International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.07,Issue.05,
June-2015,
Pages:0747-0754

www.ijatir.org

Assessment of Attacks to Fingerprint, Iris and Face Recognition Verification Systems

MULANI IRPAN AJAM[1], DR. MD. ATEEQ UR RAHMAN[2]

[1]PG Scholar, Dept of CSE, Shadan College of Engineering & Technology, Hyderabad, TS, India.
[2]Professor, Dept of CSE, Shadan College of Engineering & Technology, Hyderabad, TS, India.

Abstract: In this paper, we propose a novel system with the help of java is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment, which measures structure loss based on statistical moments, i.e., the mean and variance, represents mainly the luminance change of pixels rather than describing the spatial distribution. However, the human visual system (HVS) is highly adapted to extract structures with regular spatial distributions. In this paper, we employ a self-similarity based procedure to describe the spatial distribution of image structures. Then, combining with the statistical characters, we improve the structural similarity based quality metric. 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 (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples..The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

Keywords: Image Quality Assessment, Biometrics, Security, Attacks, Countermeasure.

I. INTRODUCTION

As a mathematical technology of the human behaviors in image quality evaluation, objective image quality assessment (IQA) metric has been widely used in various image processing application, e.g., compression, transmission and restoration[1]. The simplest and most common quality metrics are the mean square error (MSE) and the peak signal-to-noise ratio(PSNR), which directly compute the differences between the reference and distorted images. But both metrics do NOT accord with the human visual perception well, since the signal error is not equivalent to the degradation of visual quality in the human visual system (HVS). Considering the perceptual characteristic of the HVS, Wang et al. introduced a structural similarity (SSIM) based quality metric [4]. The SSIM metric is under the assumption that the HVS is highly adapted to extract structural information from an input scene. In the SSIM metric, the image structure is represented by statistical characters, e.g., the mean and variance, and image quality is measured based on the similarity between these statistical characters. This metric imitates the human perception on image structure and returns a better assessment result (be more consistent with the HVS) than MSE and PSNR. Furthermore, Wang et al. improved the SSIM metric by taking the variations of the viewing conditions into account, and introduced a multi-scale structural similarity (MS-SSIM) based quality metric [2]. As an extension of the single scale SSIM metric, the MS-SSIM metric further promotes the performance on image quality assessment. In [3], Li and Bovik segmented the image into three types of region, i.e., plain, edge, and texture, and gave different weights to the quality results (evaluated by the SSIM metric) of these regions.

In addition, the edge structure represents the major information for visual perception and plays a crucial role in the recognition for image content [1][5]. And therefore, Liu et al. [5] improved the SSIM metric by considering the edge similarity. 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 technology into practical use. Fake biometrics means by using the real images (Fig 1. Iris images captured from a printed paper and Fig 2. Fingerprint captured from a dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key.

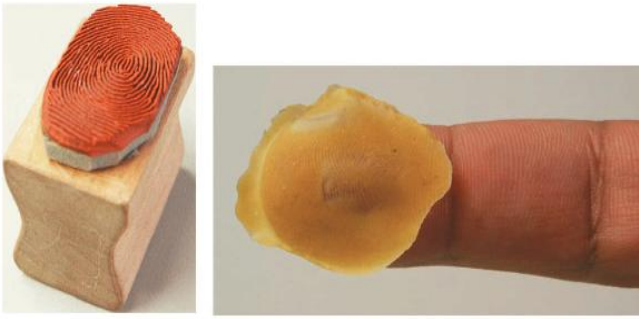
A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different type that are face recognition system, fingerprint recognition system, iris

recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioral biometric). Fig. 3 shows the type of different biometric. Multi biometric system means biometric system is used more than one biometric system for one multi-biometric system. A multi biometric system is use the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this Survey Base seminar report Image quality assessment for Liveness detection technique is used for find out the fake biometrics. Image assessment is force by supposition that it is predictable that a fake image and real sample will have different quality acquisition. Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, Fig.1 shows iris images captured from a printed paper are more likely to be fuzzy or out of focus due to shaky; face images captured from a mobile device will almost certainly be over-or under-discovered; and it is not rare that fingerprint images which is shows in Fig 2 captured from a dummy finger. 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, the fingerprint, the face, the signature , or even the gait and multimodal approaches .

Considering the perceptual characteristic of the HVS, Wang et al. introduced a structural similarity (SSIM) based quality metric. The SSIM metric is under the assumption that the HVS is highly adapted to extract structural information from an input scene. In the SSIM metric, the image structure is represented by statistical characters, e.g., the mean and variance, and image quality is measured based on the similarity between these statistical characters. This metric imitates the human perception on image structure and returns a better assessment result (be more consistent with the HVS) than MSE and PSNR. Furthermore, Wang et al. improved the SSIM metric by taking the variations of the viewing conditions into account, and introduced a multi-scale structural similarity (MS-SSIM) based quality metric. As an extension of the single scale SSIM metric, the MS-SSIM metric further promotes the performance on image quality assessment. In, Li and Bovik segmented the image into three types of region, i.e., plain, edge, and texture, and gave different weights to the quality results (evaluated by the SSIM metric) of these regions. In addition, the edge structure represents the major information for visual perception and plays a crucial role in the recognition for image content. And therefore, Liu et al. improved the SSIM metric by considering the edge similarity.

Image quality assessment is a most important topic in the image processing area. Image quality is a trait of any image usually compared with an ideal or perfect image. Digital images are subject to a large range of distortions during storage, achievement, compression, processing, transmission and reproduction, several of which may result in a degradation of visual quality. Imaging systems introduces some amount of distortion or artifacts which reduces the quality assessment. In general quality assessment is of two types one is subjective visual quality assessment and second one is objective visual qualityassessment. Objective image quality metrics can be classified on the basis of availability of an original image, with the distorted image is to be compared. Accessible approaches are known as full-reference, meaning that a complete reference image is assumed to be known. In many practical applications, however, the reference image does not exist, and a no-reference or "blind" quality assessment approach is desirable.

Fig.1. Fake iris



(a) (b)

Fig.2. fake fingerprints, a) rubber stamp made from a live scan finger print image, b) Wafer thin plastic sheet showing a replication of fingerprint

The rest of the paper is structured as follows. Liveness Detection Methods are given in Section II. Image Quality Assessment for Liveness Detection in Section III. The results for iris, fingerprint and 2D face evaluation experiments appearing Sections IV-A, IV-B, and IV-C. Conclusions are finally drawn in Section V.

II. FACTORS AFFECTS ON IQA

A. Distortion

It is an aberration that causes straight lines to curve. Distortion tends to be noticeable in low cost cameras, including cell phones (mobiles phones), and low cost DSLR lenses. It is usually very easy to see in wide angle photos. It can be corrected in software.

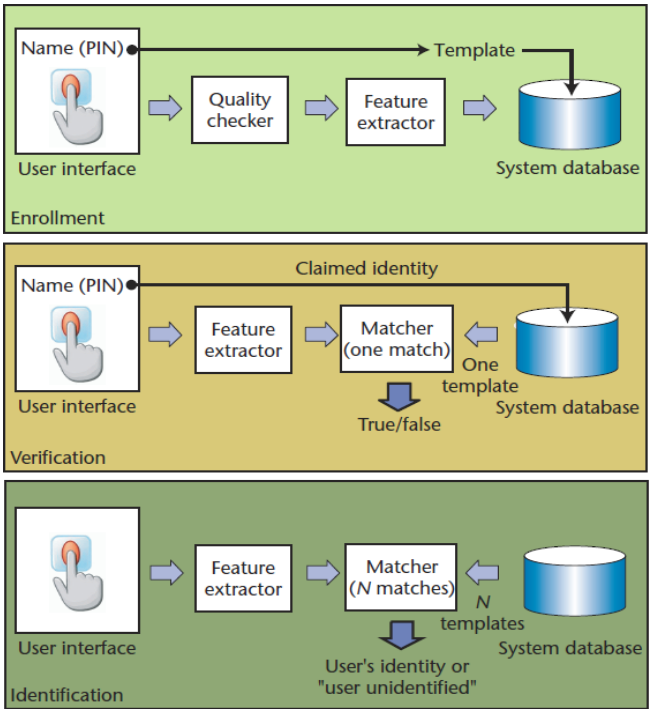


Fig.3. Different types of biometric verifications.

B. Contrast

It is also known as gamma, is the slope of the tone reproduction curve in a log-log space. High contrast usually involves loss of detail, loss of dynamic range, or clipping, in highlights or shadows.

C. Noise

It is a random variation of image density which is visible as grain in film and pixel level variations in digital images. Typical noise reduction (NR) software reduces the visibility of noise by smoothing the given image, excluding areas near to the contrast boundaries.

D. Sharpness

It determines the amount of detail an image can convey. System sharpness are affected by the lens design & manufacturing quality, focal length, aperture and distance from the image center and sensor. In the field, sharpness is affected by camera, focus accuracy & the atmospheric disturbances (thermal effects and aerosols).

E. Dynamic Range

It is the range of light levels a camera can capture, usually measured in f-stops, EV (exposure value), or zones (all factors of two in exposure). It is closely related to noise i.e. high noise implies low dynamic range.

F. Artifacts

Software especially operations performed during RAW conversion can cause significant visual artifacts, including data compression & transmission losses (e.g. Low quality JPEG), over sharpening "halos" and loss of fine & low contrast detail.

III. LIVENESS DETECTION METHODS FOR IMAGE QUALITY ASSESSMENT

Liveness detection methods are generally classified into two types (see Fig. 4). (I) Software-based techniques, in this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the trait itself); (ii)Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye).Liveness detection techniques, which use different physiological properties to differentiate between real and fake character Liveness assessment methods represent a difficult engineering problem as they have to satisfy certain challenging requirements (I) user friendly, people should be averse to use it; (ii) fast, results have to be generate in avery less time interval as the user cannot be asked to interact with the sensor for a long period of time; (iii) low-cost, a large use cannot be expected if the cost is very high;(iv) performance, in calculation to having a good fake detection rate, the protection system should not degrade the recognition performance (i.e., false rejection) of the biometric system.

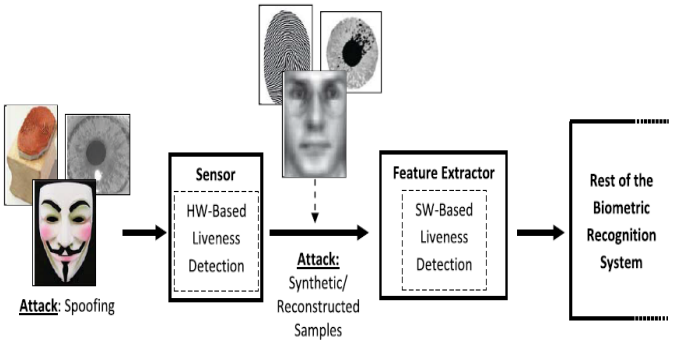


Fig.4. Types of attacks potentially detected by hardware based(spoofing) and software-based(spoofing+ reconstructed/ synthetic samples) Liveness detection techniques.

The two types of methods have certain advantages and disadvantages over the other and, in general, a combination of both would be the most advantageous protection approach to increase the security of biometric systems. As common comparison, hardware-based schemes generally present a higher fake detection rate, at the same time software-based techniques are in general less expensive(like no extra device is needed), and less intrusive since their implementation is clear to the user. moreover, as they run 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 accomplished 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 addition of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor. The use of image quality assessment for

Liveness detection is motivated by the supposition 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."Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance.

For example, iris images captured from printed paper are more likely to be unclear or out of focus due to trembling; face images captured from a mobile device will most likely be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local gaining artifacts such as spots and patches. Also, in an ultimate attack in which an unnaturally 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. The potential of general image quality assessment as protection method against different biometric attacks (with special attention to spoofing) different quality measures present diverse sensitivity to image artifacts and distortions for example, measures like the mean squared error respond additional to additive noise, while others such as the spectral phase error are extra sensitive to blur; while gradient-related features respond to distortions concentrated around edges and textures. Therefore, using alarge range of IQMs exploiting complementary image quality properties should allow detecting the aforementioned quality differences between real and fake samples expected to be found in many attack attempts (i.e., given that the technique with multi-attack protection capabilities). So consider that there is sound proof for the "quality-difference" theory and that image quality measures have the possible to achieve success in biometric protection tasks.

IV. RESULTS

The evaluation experimental protocol has been designed with a two-fold objective:

- First, evaluate the "multi-biometric" dimension of the protection method. That is, its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose three of the most extended image-based biometric modalities have been considered in the experiments: iris, fingerprints and 2D face.
- Second, evaluate the "multi-attack" dimension of the protection method. That is, its ability to detect not only spoofing attacks (such as other Liveness detectionspecificapproaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples (see Fig. 4).

With these goals in mind, and in order to achieve producible results, we have only used in the experimental validation publicly available databases with well described evaluation protocols. This has allowed us to compare, in an objective and fair way, the performance of the proposed system with other existing state-of-the-art Liveness detection solutions. The task in all the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples. As explained, for this purpose we build a 25-dimensional simple classifier based on generalIQMs. Therefore, in all cases, results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; and the False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed aster = (FGR + FFR)/2.

Fig.5. 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.

For the iris modality the protection method is tested undertow different attack scenarios, namely: I) spoofing attack indie) 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 I) 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. The database used in this spoofing scenario is the ATVS-Fir DB which may be obtained from the Biometric Recognition Group-ATVS. The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the BioSecbaseline corpus. It follows the same structure as the originalBoise 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 IrisAccessEOU3000 sensor with infrared illumination which capturesbmp grey-scale images of size 640 × 480 pixels. In Fig.5 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and the I corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other50 eyes available in the dataset. The Liveness detection results achieved by the proposed approach under this scenario appear in the first row of Table I, 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 (extract the features and classify) each sample of the two considered databases. This time was measured on a standard 64-bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b.

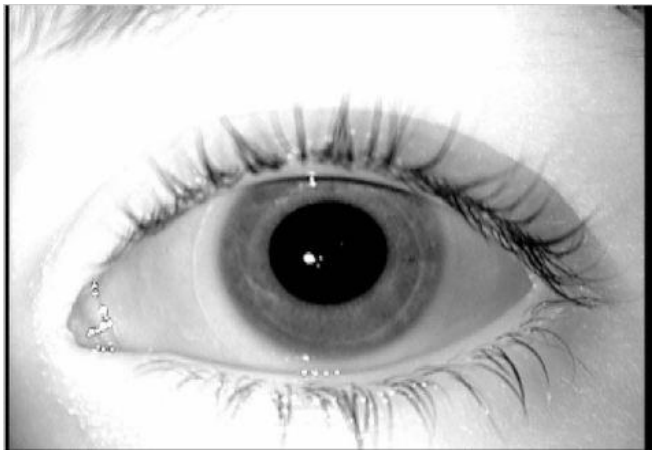


Fig.6. Typical real iris images

As no other iris Liveness detection method has yet been reported on the public ATVS-Fir DB, for comparison, the second row of Table I reports the results obtained on this database by a self-implementation of the anti-spoofing method proposed. 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.

- 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 self developed CASIA close-up camera and are stored in bmpformat.
- Synthetic database: WVU-Synthetic Iris DB. Being 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, which has two stages. In the first stage, a Markov Random Field model trained on theCASIA-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, collarets and crypts are generated and embedded in the texture field. Following theCASIA-IrisV1 DB, these synthetic database includes7 grey-scale 320×280 bmp images of 1,000 different subjects (eyes). In Fig.6 we show some typical real and fake iris images that may be found in the CASIA-IrisV1 DB and in thieve-Synthetic Iris DB. It may be observe that, as a consequence of the training process carried out on theCASIA-IrisV1 DB, the synthetic samples are visually very similar to those of the real dataset, which makes themespeciallysuitable for the considered attacking scenario.

TABLE I

	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

The table I shows the results (in percentage) obtained by the proposed biometric protection method based on aqua for the two attacking scenarios considered in the iris modality: spoofing (top row) and synthetic (bottom row). For comparison, the middle row reports the results obtained by a self-implementation of the anti-spoofing method presented. the last column indicates, in seconds, the average execution time to process each sample Some typical examples of the images that can be found in this database are shown in Fig.7, where the material used for the generation of the fake iris is specified (silicone,gelatine orplayboyh).The train and test sets selected for the evaluation experiment son this database are the same as the ones used in theLivet 2009 competition, so that the results obtained byte 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.

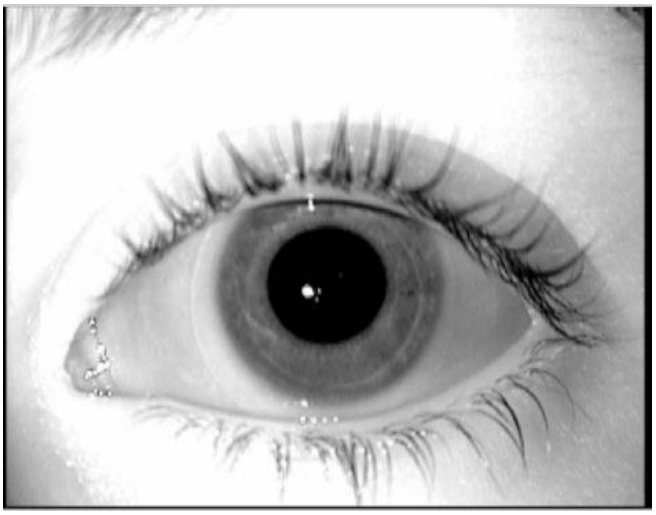


Fig.7. Input image after filtering.

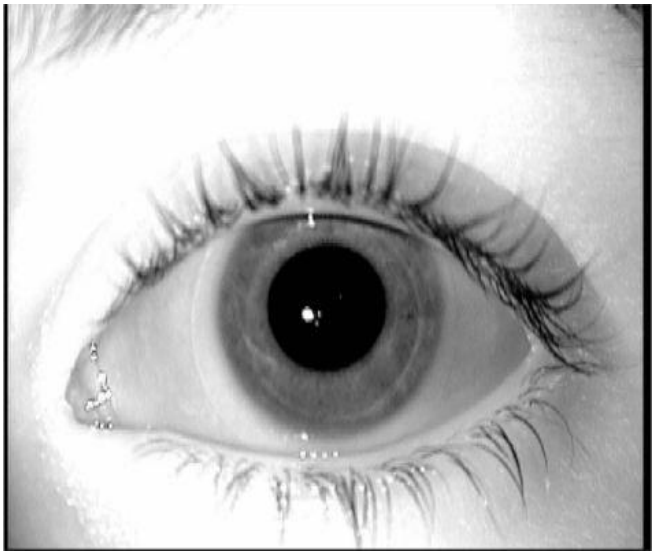


Fig.8. Harris corner detection for input image.

Fig.9. Harris corner detected for input image.

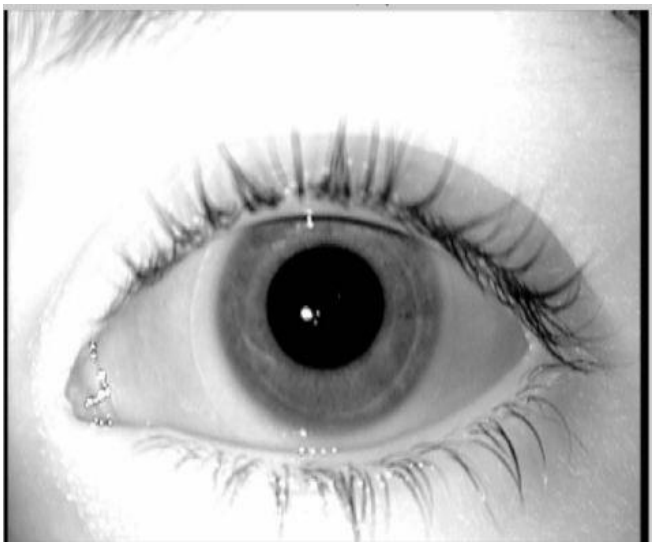


Fig.10. Harris corner detection for Reference image.

Fig.11. Harris corner detected for Reference image.

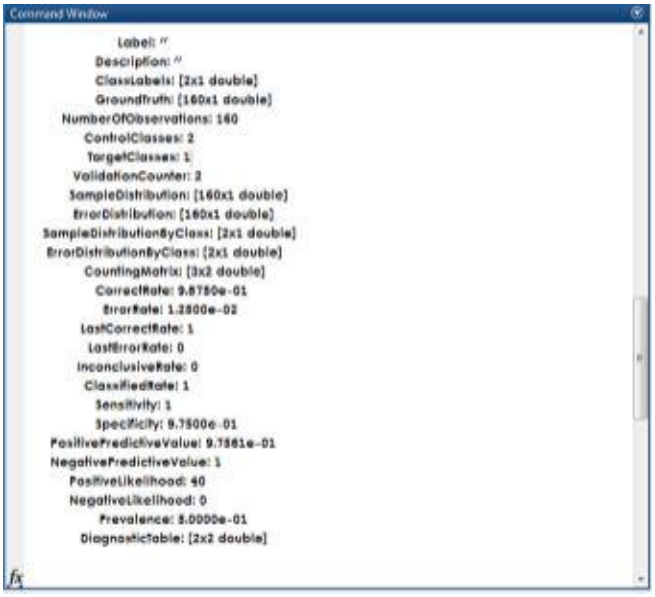


Fig.12. Trained Classifier result.

Results achieved on this database are shown in the figures. For clarity, In this work, comparative results were reported with particular implementations (from the authors) of the techniques proposed based on the wavelet analysis of the finger tip texture, based on the Curve let analysis of the finger tip texture; and based on the combination of local ridge frequencies and multi-resolution texture analysis. We also present these results so that they may be compared with our proposed IQA-based method(row one). In the bottom row we show the average execution time in seconds needed to process (extract the features and classify) each sample of the three datasets. This time was measured on a standard 64-bit Windows7-PC withal 3.4 GHz processor and 16 GB RAM memory, runningMATLAB R2012b. Due to the high simplicity of the method, the computational cost of processing an image depends almost exclusively on the size of the sample.

TABLE II

	Comparative Results: Fingerprints-LivDet09								
	Biometrika			CrossMatch			Identix		
	FFR	FGR	HTER	FFR	FGR	HTER	FFR	FGR	HTER
IQA-based	14.0	**11.6**	12.8	8.6	12.8	10.7	**1.1**	**1.4**	**1.2**
Best LivDet09 [10]	15.6	20.7	18.2	**7.4**	**11.4**	**9.4**	2.7	2.8	2.8
Marasco et al. [53]	**12.2**	13.0	**12.6**	17.4	12.9	15.2	8.3	11.0	9.7
Moon et al. [54] reported in [53]	20.8	25.0	23.0	27.4	19.6	23.5	74.7	1.6	38.2
Nikam et al. [55] reported in [53]	14.3	42.3	28.3	19.0	18.4	18.7	23.7	37.0	30.3
Abhyankar et al. [56] reported in [53]	24.2	39.2	31.7	39.7	23.3	31.5	48.4	46.0	47.2
Av. Exec. (s)	0.169			0.231			0.368		

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. The general structure of the protocol is specified. The database is also released with face detection data. These data was used to crop and normalize all the faces to a 64×64bounding box prior to the anti-spoofing experiments. This way the final classification results are ensured to be totally unbiased and not dependent on contextual-specific artifacts such as: unwanted changes in the background; different sizes of the heads (we can see in Fig.8 that fake faces are in general slightly bigger than the ones in real images); a black frame due to an imperfect fitting of the attack media on the capturing device screen, etc.

In the grand test experiments (also defined in the associated protocol) the protection method is trained using data from the print, mobile and higher scenarios, and tested also on samples from the three types of attacks. This is probably the most realistic attack case, as, in general, we cannot know priori the type of artifact (paper, mobile phone or tablet) that the attacker will use to try to break into the system. The performance shown by the proposed algorithm in the face-based evaluation confirms the conclusions extracted from the iris and fingerprint experiments: the IQA-based protection method is able to adapt to different modalities, databases and attacks performing consistently well in all of them. In different LBP-based anti-spoofing techniques(partially based on the study presented) were tested following the exact same protocol used in the present work. Results were only reported on the grandest scenario considering all types of supports (hand and fixed). A comparison between both protection approaches (IQA-based and LBPbased)appears. The error rates of all methods are very similar; however, the IQA-based has the advantage obits simplicity and generality.

In the 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks 2011 [12] there were several important differences with the protocol followed in the present work's) only the print subset was used (considering both hand and fixed supports); ii) faces were not necessarily cropped and normalized (which, as mentioned before, may lead to optimistically biased results); and iii) classification was carried out on a video-basis and not frame-by-frame as in our experiments (i.e., systems in the competition exploited both spatial and temporal information). Therefore, a fully fair comparison between the competition and the present work is not possible. However, for reference, we present the results obtained by the different participants in the competition compared to the performance of our method without doing the cropping and normalization of the videos. We can observe that, even though many of the contestants were using sequence of frames to classify each video (with the complexity and speed decrease that this entails), our proposed IQA-based method performs similarly to the top rankedsystems. Furthermore, several of the algorithms presented to the competition are based on motion-detection of the face and, therefore, their ability to detect fake access attempts carried outwit replayed motion videos (mobile and higher scenarios)would be at least under question.

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 SFFSmethod is a deterministic, single-solution feature selection algorithm first proposed in, which has shown remarkable performance over other suboptimal selection schemes. In the current experimental analysis, the selection criterion to be optimized by the SFFS algorithm is the HTER achieved by the system in the test set following the experimental protocols described. In particular, the SFFS algorithm has-been used to search for the best performing feature subsets of dimensions: 5, 10, 15 and the best overall subset regardless obitssize. For the sake of argument, the results obtained for three representative scenarios of those considered in the previous sections are

- The first observation implies that other quality-related features could still be added to the proposed set in order to further improve its overall performance (until, eventually, adding new features starts decreasing its detection rates).
- For all cases, the best performing 5-feature and even10-feature subsets present around a 50% HTER, which reinforces the idea that the competitive performance of the system does not rely on the high discriminative power of certain specific features but on the diversity and complementarily of the whole set.

V. CONCLUSION

Our system for spoofing attacks to iris recognition systems. The proposed method, based on a 22 feature set of quality related parameters, was tested on an iris database which comprises 1,600 real and fake images, where it reached a

total 86% of correctly classified (robust/vulnerable) real samples, proving this waits feasibility as a strategy to prevent direct attacks tithe sensor. Vulnerability detection solutions such as the one presented in this work may become of great importance in the biometric field as they can help to reduce the effect of direct attacks, thus enhancing the level of security offered to those users that are more exposed to this type of threat.

VI. REFERENCES

[1] Javier Globally, Sebastian Marcel, Member, IEEE, and Julian Fires, "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.

[2] 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.

[3] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis,"inProc. AWB, 2004.

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

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

[6] J. Globally, F. Alonso-Fernandez, J. Fires, and J. Ortega-Garcia,"A high performance fingerprint Liveness detection method based onquality related features," Future Generat. Comput. Syst., vol. 28, no. 1,pp. 311–321, 2012.

[7] 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.

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

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

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

[11] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu,et al., "First international fingerprint Liveness detection competitionLivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009,pp. 12–23.

[12] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,et al., "Competition on countermeasures to 2D facial spoofing attacks,"inProc. IEEE IJCB, Oct. 2011, pp. 1–6.(CARDIS), 2000, pp. 289–303.

[13] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verificationsystems," Telecommunication Systems, vol. 47, pp. 243–254,2011.

[14] N. Poh, T. Bourlai, J. Kittler, L. Allano, F. Alonso-Fernandez,O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez,H. Ganster, J. Ortega-Garcia, D. Maurer, A. A. Salah, T. Sheidat,and C. Vielhauer, "Benchmarking quality-dependent andcost-sensitive score-level multimodal biometric fusion algorithms,"IEEE Trans. on Information Forensics and Security,vol. 4, pp. 849–866, 2009.

[15] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia,J. Gonzalez-Rodriguez, H. Front haler, K. Kollreider,and J. Bigun, "A comparative study of fingerprint imagequality estimation methods," IEEE Trans. on InformationForensics and Security, vol. 2, no. 4, pp. 734–743, 2008.

[16] L. Masek and P. Kovesi, "Matlab source code for a biometricidentification system based on iris patterns," The School ofComputer Science and Software Engineering, The Universityof Western Australia, Tech. Rep., 2003.

[17] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez, "Bio Sec baseline corpus: A multimodalbiometric database," Pattern Recognition, vol. 40, pp.1389–1392, 2007.

[18] Z. Wei, T. Tan, Z. Sun, and J. Cui, "Robust and fast assessmentof iris image quality," in Proc. IAPR Int. Conf. onBiometrics (ICB). Springer LNCS-3832, 2006, pp. 464–471.

[19] J. Daugman, "How iris recognition works," IEEE Trans. OnCircuits and Systems for Video Technology, vol. 14, pp. 21–30, 2004.

[20] A. Abhyankar and S. Schukers, "Iris quality assessment and bi-orthogonal wavelet based encoding for recognition," Pattern Recognition, vol. 42, pp. 1878–1894, 2009.