International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Fake Biometric Detection by Using Image Processing: Application to Iris, Fingerprint, and Face Recognition

T. Vino[1], G. Jegan[2]

Assistant Professor, Sathyabama Institute of Science and Technology, Chennai, India

Abstract: ***To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. 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: IRIS, Finger print, Face recognition, Bio metric

1. Introduction

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research. A biometric measurement is a physical or behavioral trait. The field of biometrics aims to verify personal identity using such features. These traits are of interest because they are not easily changed or imitated, and they cannot be forgotten as is the case for passwords, nor can they be lost in the same manner as identification cards. Many biometric modes have been examined to date, with the research community and industry centering around a short list of biometric modalities that have exhibited particularly promising results. Recent focus has shifted towards the face and the iris as biometric modes, and a large corpus of past publications and current research activity has emerged in recent years.

The detailed visual texture of the human iris yields accurate and reliable recognition, making it an ideal biometric mode. Commercial iris recognition systems have been in use for some time, and iris biometric systems have piqued the interest of government agencies around the world. A small scale iris biometrics system was used as part of the Clear program in US Airports. The US Department of Homeland Security uses iris biometrics as part of the VISITS program as well. The national government of India is currently using iris biometrics as part of their Unique ID project which is to date the largest proposed biometrics system in the world

The face is another area of the human body with proven performance in large scale biometrics systems. The US Department of Justice and law enforcement organizations around the country use automated face biometrics systems to identify criminals Face recognition is also being used as part of the Unique ID project of India.

While biometrics research has made much progress in recent years, and is nearing perfect recognition rates under ideal circumstances, further research is still necessary. One method of improving recognition rates is to verify that the collected data is of sufficient quality for matching. My research involves analysis of the current quality metrics used in a variety of commercial systems as well as the development of new quality metrics for biometrics.

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 . 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 mult ibiometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements : (i) non-invasive, the technique

should in no case be harmful for the individual or require an excessive contact with the user; (i i) user friendly, people should not be reluctant to use it; (i i i) fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) 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.

2. Basic Iris Recognition Algorithm

The first accurate algorithm for iris biometrics was introduced in 1993 by John Daugman Daugman provides an algorithm to locate the iris region in an image, segment it, and produce a template that can be used for comparisons to quickly and accurately determine identity. Since its introduction, Daugman has made numerous improvements to the original algorithm, and to this date Daugman's system remains the basis of almost all deployed iris biometric systems.

Iris recognition systems based on the original Daugman paper generally detect the iris boundaries by searching for circles, using an integro-differential operator. However, since the boundaries are not perfectly circular, alternative techniques have been implemented to segment the iris region based on ellipses or active contours.

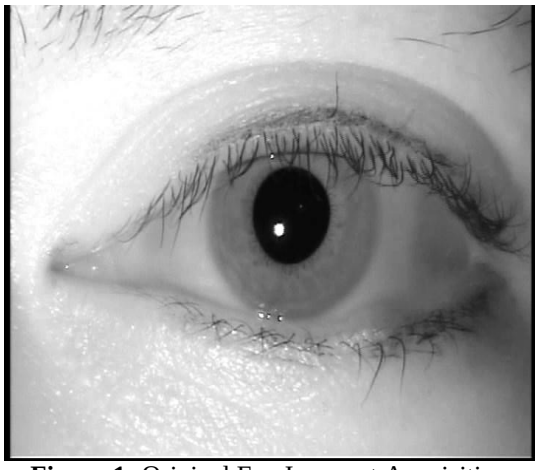

Figure 1: Original Eye Image at Acquisition

After segmentation, the iris region is "unwrapped", changing the geometry from that of an annulus to that of a rectangle. The unwrapped iris region is then sampled a set number of times such that each (x,y) sample is translated to a polar coordinate, (r,θ). This sampling interpolates the original iris segment, and forces the output to be of known dimensions. This process of "unwrapping" the iris accounts for differences in pupil dilation so that each image is translated to equal-sized bands. After acquisition, segmentation, and normalization, iris texture features are extracted through the use of a complex filter. Daugman suggests a two-dimensional log-Gabor filter, which maps each pixel in the unwrapped image to a coordinate location in the complex plane. The quadrant of the complex plane that each pixel falls into is used to produce a binary iris code. Pixles that were masked out in the segmentation step are not included in the filter response. Other filters have been suggested; more information can be found.

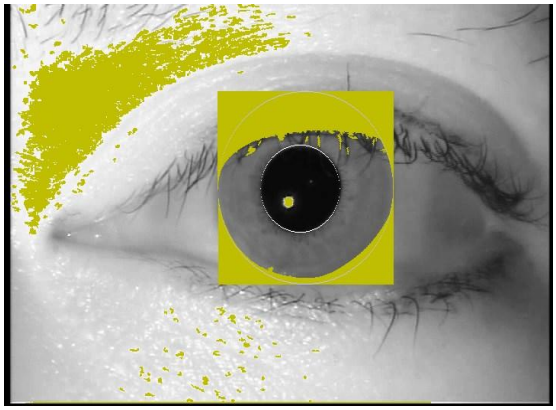

Figure 2: Fully segmented image with all eyelash and eyelid occlusion masked.

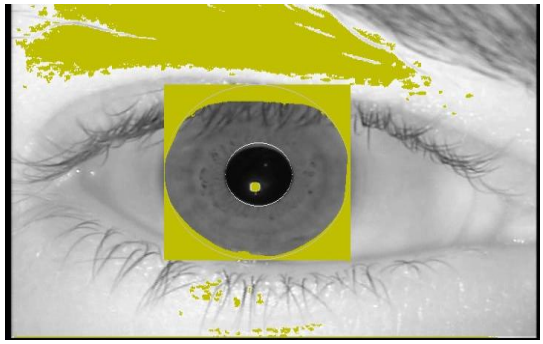

Figure 3: Segmented image with some eyelash and eyelid occlusion still unmasked.

Above figures shows Examples of segmented images with and without properly masked eyelash and eyelid occlusion and the unwrapped normalized iris image.

After all processing is completed, an iris image is defined by its iris code and a corresponding mask, and is ready for matching. In matching two iris codes, Daugman's approach computes a fractional Hamming distance between iris codes as given by the following formula:

$$HD_{raw} = \frac{||(\text{code A} \oplus \text{code B}) \cap \text{mask A} \cap \text{mask B}||}{||\text{mask A} \cap \text{mask B}||}$$

The above equation does not take into account the number of masked bits in the comparison. Comparisons with a large number of occluded bits have a higher probability of resulting in an artificially low match score. Therefore, the fractional Hamming distance is sometimes normalized using the following formula, where n is the number of bits compared:

$$HD_{norm} = 0.5 - (0.5 - HD_{raw})\sqrt{\frac{n}{900}}$$

Hamming distances represent the fraction of differing bits between two iris codes, and can range between zero and one, where zero represents no differing bits (a perfect match), and one meaning all bits differed (a perfect non-match). Two iris codes that are non-matches are expected to have a raw Hamming distance of 0.5, as each binary comparison has a 50% chance of matching in value. However, to account for eye rotation about the optical axis, iris matching algorithms rotate the iris codes by a few shifts, considering all

comparisons, and reporting the lowest score, which can artificially lower the reported average raw Hamming distance for non-matches to slightly less than 0.5. Different samples of the same iris are not generally identical, but have many more common bits than samples of different irises; a perfect raw match score of zero is thus not expected. After normalization, it is possible to achieve normalized Hamming distances that are negative.

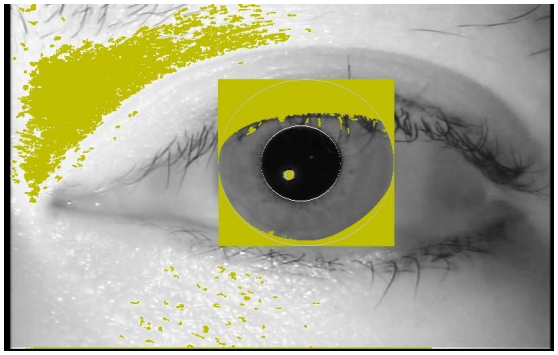

Figure 4: Image with the segmented iris and eyelid and eyelash occlusion masked

A different approach to iris segmentation is described by Wildes Instead of an integro-differential operator for circular boundary detection, a binary edge map is calculated and a Hough transform is utilized to detect the circular pupillary and limbic boundaries. Instead of log-Gabor filters, a Laplacian of a Gaussian filter is applied to the normalized image to produce an iris template. Comparisons are done using normalized correlation, yielding similarity measures instead of Hamming distances. Information on Wildes' algorithm can be found

Results in this thesis are taken from three systems: one system using Daugman's method (with some modifications) of iris recognition that reports match scores as fractional Hamming distances, IrisBEE ; as well as two commercially available algorithms, Neuro Technology VeriEye; and MIRLIN reports fractional Hamming distances, much like in the Daugman algorithm, but uses a product-of-sums approach. VeriEye reports similarity scores between 0 and 3,235, where 3,235 is a perfect match and zero is reported if software is confident that the images are non-matches.

3. Basic Face Recognition Algorithm

Methods for detecting a face in a sample fall into three main categories: feature invariant, template matching, and appearance-based. In feature invariant face detection, cues in the image (such as facial features or skin tone) are used to locate possible faces. Template matching techniques search the sample for regions that match a given generic face template. Most appearance-based face detection uses machine learning techniques, such as support vector machines or hidden Markov models , to identify faces. for a sample image and a face region identified using the Haar cascades provided with the Open CV computer
Vision library.

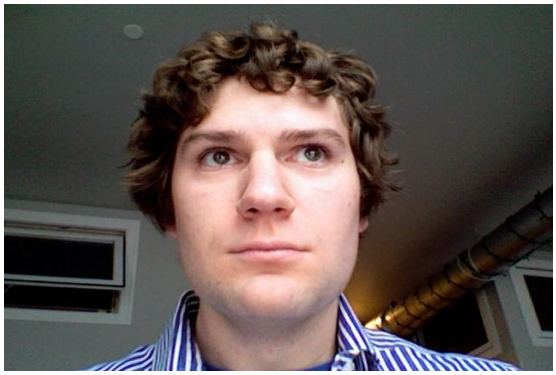

Figure 5: Face Original imageat Acquisition

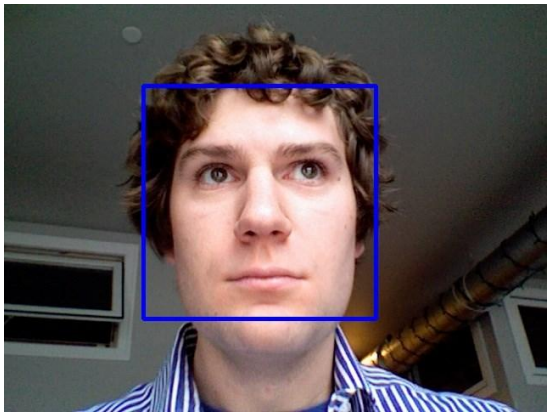

Figure 6: Face Image with Detected Face Marked by Colored Square

Once a face is identified, the raw sample data needs to be turned into a template suitable for matching. Multiple methods exist for transforming the sample data, including holistic approaches, feature-based approaches, model-based approaches and classifier-based approaches. Holistic approaches use the entire face as input, as it appears in the detected face region, and then perform some conversion on the data as a whole to produce a template. Feature-based approaches extract local feature information from the face region to build a template. Using features with low variance can help counter some effects of expression. Model-based approaches use fundamentals of reflection to generate a 3D face template from the 2D sample data. Classifier-based approaches use machine-learning techniques to classify regions of the image as either face or non-face.

4. Fingerprints

Fingerprint analysis, also known in the US as dactylography, is the science of using fingerprints to identify a person. Fingerprints are the most commonly used biometric and have been used for identification since the 1890's.

In 1901, Sir Edward Henry introduced the Henry Classification System for fingerprints which is widely recognised, even today, in anglophone countries. In South American countries a system devised by Dr. Juan Vucetich in 1892 is widely used. These manual classification systems are, however, being replaced by other techniques which are more suitable for large scale electronic storage and analysis.

Fingerprint identification is well established and a mature science. It has also been extensively tested in various legal

systems and is accepted as an international standard for identification. Although law enforcement agencies are principal users of fingerprints, various electronic readers are now commonly available and are used for authentication purposes, mainly in access control applications.

All digits (fingers, thumbs and toes) have epidermal ridges, furrows and patterns. Palms and the soles of feet also have distinctive epidermal patterns. These patterns are widely believed to provide a friction surface to assist in gripping and handling objects and for walking Fingerprints are formed in the third and fourth month of foetal development and are unique. Even identical twins will have differing fingerprint patterns. In the many years fingerprinting has been used by law enforcement agencies, no two individuals have been found to have identical prints.

The skin excretes oils and perspiration through sweat glands, flowing along the tops of the ridges. When a surface is touched the fingerprint is transferred. Smooth, clean surfaces record better quality fingerprints but fingerprints can also be found on irregular surfaces such as paper. There are three basic categories of fingerprint:

- Visible prints (also called patent), such as those made in oil, ink or blood
- Latent prints which are invisible under normal viewing conditions; and
- Plastic prints which are left in soft surfaces such as new paint.

Figure 7: Fingerprints shown on irregular surfaces

There are now over forty methods available for collecting prints including powders, use of chemicals such as iodine, ninhydrin, and silver nitrate, digital imaging, dye stains and fumes. Some are powders and chemicals are coloured to contrast with the background or to fluoresce or illuminate under alternative light sources. Lasers are also used. Generally the least destructive method is used first.

Henry Classification System

As the Inspector General of Police for Bengal Province in India, Sir Edward Henry (1850 -1931) developed a classification system which was officially adopted by British India in 1897. The British Association for the Advancement of Science heard of Henry's success in India and in 1900 he presented a paper entitled "Fingerprints and the Detection of Crime in India. Shortly after, Henry's book "The Classification and Uses of Finger Prints" was published.

In December 1900, Britain's Belper Committee recommended that the fingerprints of criminals be taken and classified by the Indian System. In 1901, Henry was called back to England and given the post of Assistant Commissioner of Police in charge of Criminal Identification at New Scotland Yard. In 1903, Henry became Commissioner of Police.

The Henry Classification System organises ten-print fingerprint records by pattern type. Finger ridges and patterns can be continuous, interrupted, forked, and other formations. Fingerprints are classified and identified by the relationship of these formations, described as minutiae. These patterns are divided into five basic groups, with various subgroups.

- Arch: a ridge that runs across the fingertip and curves up in the middle. Tented arches have a spiked effect.
- Whorl: an oval formation, often making a spiral pattern around a central point. Principal types are a plain whorl and a central pocket loop whorl
- Loops: These have a stronger curve than arches, and they exit and enter the print on the same side. Radial loops slant toward the thumb and ulnar loops away from the thumb. "Composites" are a mix of other patterns; "Accidentals" form an irregular pattern that's not classifiable as an Arch, Loop or Whorl.

Figure 8: Patterns of fingerprints

Several other characteristics can be present within fingerprint patterns. These are minutiae or interruptions to the smooth flow of ridges, and are the basis for most fingerprint identification. Codified in the late 1800's as Galton features, minutiae are at their most rudimentary ridge endings, the points at which a ridge stops, bifurcations, the point at which one ridge divides into two, and dots or small ridges.

Many types of minutiae are categorised and in addition to ridge endings, bifurcation and dots, include:

- Islands (ridges slightly longer than dots, occupying space between two temporarily divergent ridges);
- Ponds or lakes (empty spaces between two temporarily divergent ridges);
- Spurs (a notch protruding from a ridge);
- Bridges (small ridges joining two longer adjacent ridges); and
- Crossovers (two ridges which cross each other).

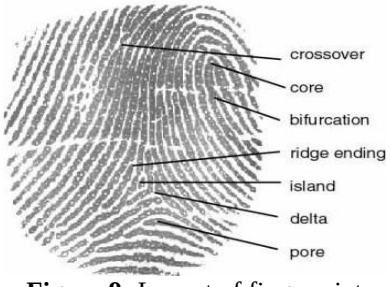

Figure 9: Layout of fingerprint

For the fingerprint modality, the performance of the proposed protection method is evaluated using the LivDet 2009 DB 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).

5. Parameters for Software Implementation

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 and stegan alysis 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. 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-theart. 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 on one specific modality and, in many cases, also to detect one specific type of spoofing attack.
- Human observers very often refer to the "different appearance" 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 artifacts 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.

1) FR-IQMs: Error *Sensitivity Measures:* Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features.

Although their efficiency as signal fidelity measures is somewhat controversial up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system they are easy to calculate and usually have very low computational complexity.

Several of these metrics have been included in the 25-feature parameterization proposed in the present work. For clarity, these features have been classified here into five different categories according to the image property measured

- **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, $\max_r$ is defined as the r-highest pixel difference between two images. For the present implementation, $R = 10$.

In the LMSE entry in Table I, $h(\mathbf{I}_{i,j}) = \mathbf{I}_i+1_{,j} + \mathbf{I}_i-1_{,j} + \mathbf{I}i,j+1 + \mathbf{I}i,j-1 - 4\mathbf{I}i,j$.

- **Correlation-based measures** The similarity between two digital images can also be quantified in terms of the correlation function. A variant of correlationbased measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include
- **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 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 $\mathbf{I_E}$ and $\mathbf{I}\hat{}E$; *(ii)* the Harris corner detector [48] to compute the number of corners N_{cr} and $N\hat{}cr$ found in **I** and **I**ˆ.
- **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 **F**ˆ are the respective Fourier transforms of **I** and **I**ˆ), 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

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 **G**ˆ are the gradient maps of **I** and **I**ˆ defined as $\mathbf{G} = \mathbf{G}_x+i\mathbf{G}_y$, where $\mathbf{G}_x$ and $\mathbf{G}_y$ are the gradients in the x and y directions).

2) FR-IQMs: Structural Similarity Measures: Although being very convenient and widely used, the aforementioned image quality metrics based on error sensitivity present several problems which are evidenced by their mismatch (in many cases) with subjective human-based quality scoring systems In this scenario, a recent new paradigm for image quality assessment based on structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones.

Among these recent objective perceptual measures, the Structural Similarity Index Measure (**SSIM**), has the simplest formulation and has gained widespread popularity in a broad range of practical applications In view of its very attractive properties, the SSIM has been included in the 25-feature parameterization.

3) FR-IQMs: Information Theoretic Measures: The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem (rather than a signal-fidelity problem). The core idea behind these approaches is that an image source communicates to a receiver through a channel that limits the amount of information that could flow through it, thereby introducing distortions. The goal is to relate the visual quality of the test image to the amount of information shared between the test and the reference signals, or more precisely, the mutual information between them. Under this general framework, image quality measures based on information fidelity exploit the (in some cases imprecise) relationship between statistical image information and visual quality.

In the present work we consider two of these information theoretic features: the Visual Information Fidelity (**VIF**) and the Reduced Reference Entropic Difference index (**RRED**) Both metrics are based on the information theoretic perspective of IQA but each of them take either a global or a local approximation to the problem, as is explained below.

The VIF metric measures the quality fidelity as the ratio between the total information (measured in terms of entropy) ideally extracted by the brain from the whole distorted image and the total information conveyed within the complete reference image. This metric relies on the assumption that natural images of perfect quality, in the absence of any distortions, pass through the human visual system (HVS) of an observer before entering the brain, which extracts cognitive information from it. For distorted images, it is hypothesized that the reference signal has passed through another "distortion channel" before entering the HVS. The VIF measure is derived from the ratio of two mutual information quantities: the mutual information between the input and the output of the HVS channel when no distortion channel is present (i.e., reference image information) and the mutual information between the input of the distortion channel and the output of the HVS channel for the test image. Therefore, to compute the VIF metric, the entire reference image is required as quality is assessed on a global basis.

On the other hand, the RRED metric approaches the problem of QA from the perspective of measuring the amount of local information difference between the reference image and the projection of the distorted image onto the space of natural images, for a given sub band of the wavelet domain. In essence, the RRED algorithm computes the average difference between scaled local entropies of wavelet coefficients of reference and projected distorted images in a distributed fashion. This way, contrary to the VIF feature,

for the RRED it is not necessary to have access the entire reference image but only to a reduced part of its information (i.e., quality is computed locally). This required information can even be reduced to only one single scalar in case all the scaled entropy terms in the selected wavelet subband are considered in one single block.

6. Flow Chart and Results

Image quality is a trait of any image Usually compared with an ideal or perfect image. 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. In general quality assessment is of two type one is subjective visual Quality assessment and second one is objective visual quality assessment. 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.

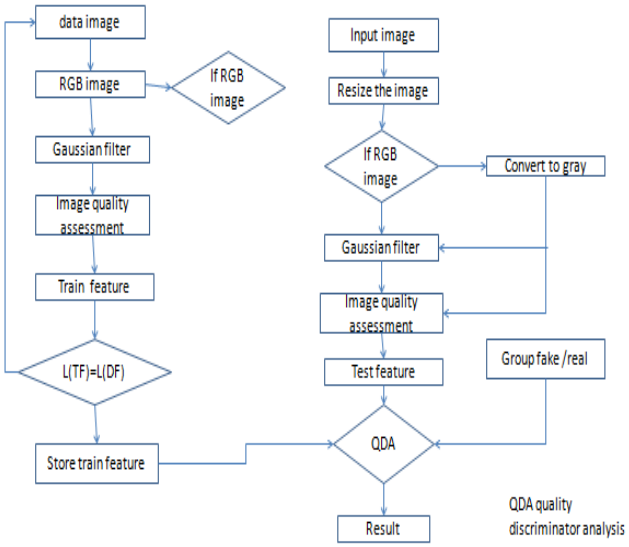

Figure 10: Flow chart for fake biometric detection outputs

IRIS:

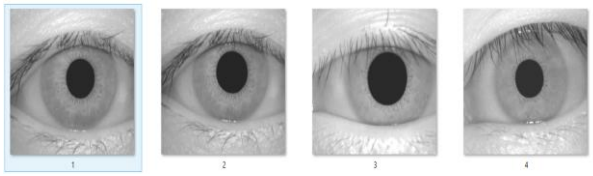

Figure 11: Database images

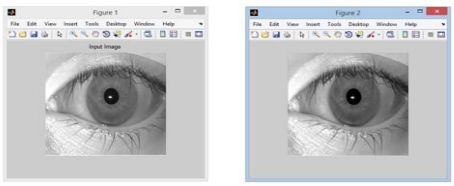

Figure 12: Output image of iris

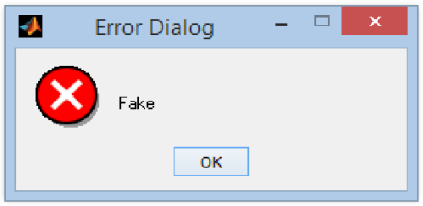

Figure 13: Dialog box showing real or fake

FACE:

Figure 14: Data base images of face

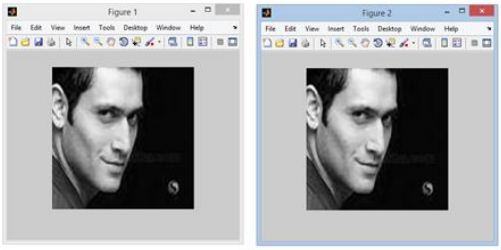

Figure 15: Output of face image

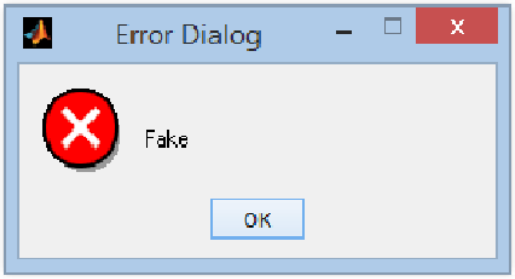

Figure 16: dialog box showing real or fake

FINGER:

Figure 17: Data base images of fingerprint

Figure 18: Output of fingerprint image

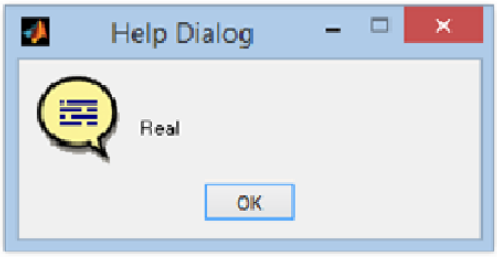

Figure 19: Dialog box showing real or fake

in every output images we are enhancing the input image with respect to the database image dimensions and removing of noise is taken place. In second step we will get the all values of image like SNR,PSNR etc. we compare the values with the database images values. if both the values are same means the dialog box shows that given input is "REAL" else it shows the "FAKE". we can use this system in multilevel security purposes.

7. 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. 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. These differences come from the fact that biometric traits, as 3D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. Furthermore, biometric sensors are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact (2D, different material, etc.), the characteristics of the captured image may significantly vary. 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. All the previous results validate the "quality-difference" hypothesis formulated in Section II: "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."

In this context, the present work has made several contributions to the state-of-the-art in the field of biometric security, in particular: *i*) it has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks; *ii*) proposal and validation of a new biometric protection method; *iii*) reproducible evaluation on multiple biometric traits based on publicly available databases; *iv*) comparative results with other previously proposed protection solutions.

The present research also opens new possibilities for future work, including: *i*) extension of the considered 25-feature set with new image quality measures; *ii*) further evaluation on other image-based modalities (e.g., palmprint, hand geometry, vein); *iii*) inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos); *iv*) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB); *v*) analysis of the features individual relevance.

References

[1] Akhtar.Z, Fumera.G, Marcialis.G.L, and Roli.F, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *Proc. IEEE 5th Int. Conf. BTAS*, Sep. 2012, pp. 283–288.
[2] Anjos.A and Marcel.S, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. IEEE IJCB*, Oct.2011, pp.1–7.
[3] *Biometric Evaluation Methodology. v1.0*, Common Criteria, 2002.[Online]. Available: http://www.tabularasa-euproject.org/.
[4] Bayram.S, Avcibas.I, Sankur.B, and Memon.N, "Image manipulation detection," *J. Electron. Imag.*, vol. 15, no. 4, pp. 041102-1–041102-17, 2006.
[5] *BEAT: Biometrices Evaluation and Testing* [Online]. Available: http://www.beat-eu.org/.

[6] Bowyer.K, Boult.T, Kumar.A, and Flynn.P, *Proceedings of the IEEE Int. Joint Conf. on Biometrics*. Piscataway, NJ, USA: IEEE Press, 2011.
[7] Cappelli.R, Maio.D, Lumini.A, and Maltoni.D, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
[8] Chakka.M.M, Anjos.A, Marcel.S, Tronci.R, Muntoni.B, Fadda.*G, et al.*, "Competition on countermeasures to 2D facial spoofing attacks," *in Proc. IEEE IJCB*, Oct. 2011, pp. 1–6.
[9] Galbally.J, Alonso-Fernandez.F, Fierrez.F, and Ortega-Garcia.J, "A high performance fingerprint liveness detection method based on quality related feature*s," Future Generat. Comput. Syst.*,vol.28, no. 1, pp. 311–321, 2012.
[10] Galbally .J, Cappelli.R, Lumini.A, de Rivera.G.G, Maltoni.D, Fierrez.J, *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.
[11] Galbally.J, Fierrez.J, Alonso-Fernandez.F, and Martinez-Diaz.M, "Evaluation of direct attacks to fingerprint verification systems," *J. Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.
[12] Galbally.J, McCool.C, Fierrez.J, Marcel.S, and Ortega-Garcia.J, "On the vulnerability of face verification systems to hill-climbing attacks," *Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.
[13] Hadid.A, Ghahramani.M, Kellokumpu.V, Pietikainen.M, Bustard.J, and Nixon.M, "Can gait biometrics be spoofed?" in *Proc. IAPR ICPR*, 2012, pp. 3280–3283.
[14] Hennebert.J, Loeffel.R, Humm.A, and Ingold.R, "A new forgery scenario based on regaining dynamics of signature," in *Proc. IAPR ICB*, vol. Springer LNCS-4642. 2007, pp. 366–375.
[15] *ISO/IEC 19792:2009, Information Technology— Security Techniques— Security Evaluation of Biometrics*, ISO/IEC Standard 19792, 2009.
[16] Jain A. K, Nandakumar.K, and Nagar.A, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.
[17] Maltoni.D, Maio.D, Jain.A, and Prabhakar.S, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2009.
[18] Marcialis.G.L, Lewicke.A, Tan.B, Coli.P, Grimberg.D, Congiu.A, *et al.*, "First international fingerprint liveness detection competition— LivDet 2009," in *Proc. IAPR ICIAP*, Springer LNCS-5716. 2009, pp. 12–23.
[19] Matsumoto.T., "Artificial irises: Importance of vulnerability analysis," in *Proc. AWB*, 2004.