Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fake Biometric Detection to Iris, Fingerprint Using Image Quality Assessment

R. Radhika[1], D. Sanjana[2], C. Anuradha[3]
[1, 2] Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India
[3]Assistant Professor, Dept. of C.S.E., Bharath University, Chennai, India

Abstract: ***To make sure the actual presence of a true legitimate attribute in distinction to a faux self-manufactured artificial or reconstructed sample may be a significant drawback in biometric identification, which needs the event of recent and efficient protection measures. During this paper, we have a tendency to gift a unique software-based faux discover technique which will be employed in multiple biometric systems to detect differing types of deceitful access tries. The target of the planned system is to boost the safety of biometric recognition frameworks, by adding animate ness assessment during a quick, easy, and non-intrusive manner, through the utilization of image quality assessment. The planned approach presents a really low degree of complexness, that makes it appropriate for time period applications, mistreatment twenty five general image quality options extracted from one image (i.e., constant non heritable for authentication purposes) to tell apart between legitimate and pseud samples. The experimental results, obtained on publically accessible information sets of fingerprint, iris, and 2nd face, show that the planned technique extremely terribly competitive compared with different progressive approaches which the analysis of the final image quality of real biometric samples reveals highly valuable data that will be very efficiently wont to discriminate them from faux traits.***

Keywords: Image quality assessment, security for biometric attacks, countermeasures.

I. INTRODUCTION

IN RECENT years, the increasing interest within the analysis of biometric systems security has crystal rectifier to the creation various} and really diverse initiatives targeted on this major field of analysis: the publication of the many analysis works revealing and evaluating totally different biometric vulnerabilities, the proposal of latest protection strategies, connected book the publication of many standards within the space and the dedication of specific tracks As this kind of attacks are performed within the analog domain and therefore the interaction with the device is completed following the regular protocol, the same old digital protection mechanisms (e.g., encryption, digital signature or watermarking) aren't effective.

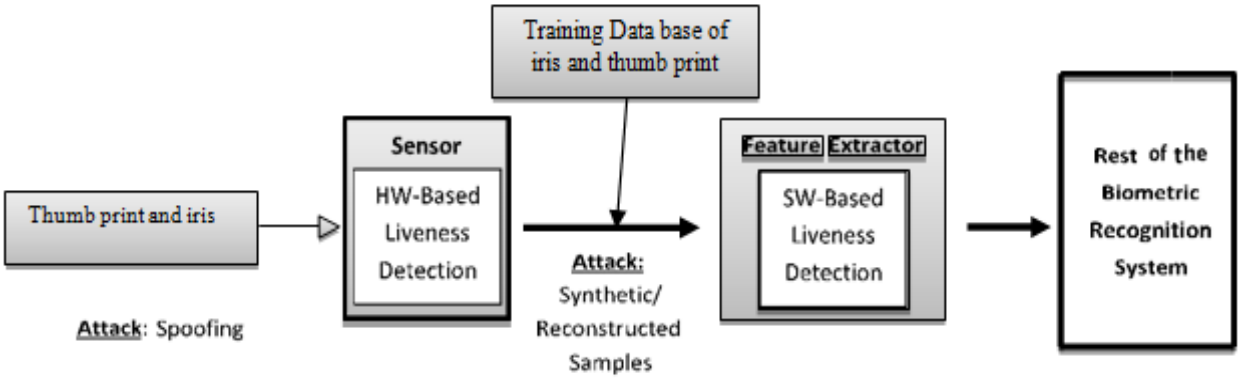

Fig.1.Typesofattackspotentiallydetectedbyhardware-based(spoofing)andsoftware-based (spoofing+reconstructed/syntheticsamples)livenessdetectiontechniques.

The said works and different analogue studies, have clearly shown the need to propose and develop specific protection strategies against this threat. This way, researchers have targeted on the look of specific countermeasures that modify biometric systems to find faux samples and reject them, up this manner the strength and security level of the systems. physiological property assessment strategies represent a difficult engineering downside as they need to satisfy sure strict needs : (i) non-invasive, the technique ought to in no case be harmful for the individual or need associate degree excessive contact with the user; (ii) user friendly, folks mustn't be reluctant to use it; (iii) quick, results ought to be created in a very reduced interval because the user cannot be asked to act with the detector for a protracted amount of time(iv) Low price, a large use cannot be expected if the value is too high; (v) performance, additionally to having a decent pretend detection rate, the protection theme mustn't degrade the popularity performance (i.e., false rejection) of

the biometric system. aliveness detection ways are typically classified into one in every of 2 teams: Hardware-based techniques, that add some specific device to the detector so as to sight explicit properties of a living attribute (e.g., fingerprint sweat, pressure, or specific reflection properties of the eye); (ii) Software-based techniques, during this case the pretend attribute is detected once the sample has been nonheritable with a typical detector (i.e., options accustomed distinguish between real and pretend traits are extracted from the biometric sample, and not from the attribute itself).

The 2 kinds of ways gift sure benefits and downsides over the opposite and, in general, a mixture of each would be the foremost fascinating protection approach to extend the protection of biometric systems. As a rough comparison, hardware-based schemes typically gift a better pretend detection rate, whereas software-based techniques are normally less costly (as no further device is needed), and fewer intrusive since their implementation is clear to the user. what is more, as they operate directly on the nonheritable sample (and not on the biometric attribute itself), software-based techniques is also embedded within the feature extractor module that makes them probably capable of police work alternative kinds of illegitimate breaking and entering makes an attempt not essentially classified as spoofing attacks. For example, software-based ways will shield the system against the injection of reconstructed or artificial samples into the channel between the detector and also the feature extractor.

Although, as shown on top of, an excellent quantity of labour has been tired the field of spoofing detection and lots of advances are reached, the assaultive methodologies have additionally evolved and become additional and additional refined. As a consequence, there area unit still massive challenges to be two-faced within the detection of direct attacks. one amongst the standard shortcomings of most anti-spoofing methods is their lack of generality. it's not rare to find that the planned approaches gift are awfully high performance detecting sure sort of spoofs (i.e., viscid fingers created out of silicone), however their efficiency drastically drops once they area unit bestowed with a distinct sort of artificial attribute. This way, their error rates vary greatly once the testing conditions area unit modified or if the analysis information is changed. Moreover, the overwhelming majority of current protection ways area unit supported the activity of sure specific properties of a given attribute (e.g., the frequency of ridges and valleys in fingerprints or the pupil dilation of the eye) which provides them are awfully reduced ability, as they'll not be enforced in recognition systems supported alternative biometric modalities (e.g., face), or perhaps on a similar system with a distinct detector. Within the gift work we tend to propose a completely unique software-based multi-biometric and multi-attack protection technique that targets to beat a part of these limitations through the utilization of image quality assessment (IQA). It's not solely capable of operational with are awfully sensible performance underneath completely different biometric systems (multi-biometric). The remainder of the paper is structured as follows. Some key ideas concerning image quality assessment and also the explanation behind its use for biometric protection is given in Section II. The projected methodology is delineate in Section III. The results for iris, fingerprint and 2nd face analysis experiments seem in Sections IV-A, IV-B, and IV-C. Conclusions area unit finally drawn in Section V.

II. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The utilization of image quality assessment for aliveness detection is intended by the belief that: "It associate that a faux image captured in an attack try can have completely different quality than a true sample nonheritable within the traditional operation situation that the sensing element was designed." Because the enforced options don't judge any specific property of a given biometric modality or of a specific attack, they'll be computed on any image. This provides the projected methodology a brand new multi-biometric dimension that isn't found in represented protection schemes. Within the current progressive, the explanation behind the utilization of IQA options for aliveness detection is supported by 3 factors:

• Image quality has been with success employed in previous works for image manipulation detection and steganalysis within the rhetorical field. To an explicit extent, several spoofing attacks, particularly those that involve taking an image of a facial image displayed in a very 2nd device (e.g., spoofing attacks with written iris or face images), is also thought to be a sort of image manipulation which might be effectively detected, as shown within the gift analysis work, by the utilization of various quality options.

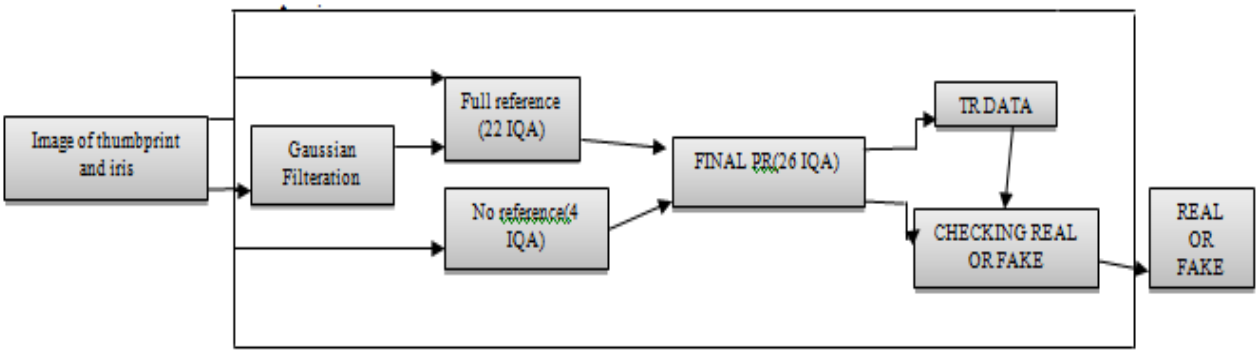

Fig.2.Generaldiagramofthebiometricprotectionmethodbasedon ImageQualityAssessment(IQA)proposedinthepresentwork. IQMstandsforImageQualityMeasure,FRforFull-Reference,andNRforNo-

Reference.SeeFig.3forageneralclassificationofthe25IQMsimplemented.SeeTableIforthecompletelistandformaldefinitionsofthe25IQMs.SeeSectionIIIforamoredetaileddescriptionofeachIQM.

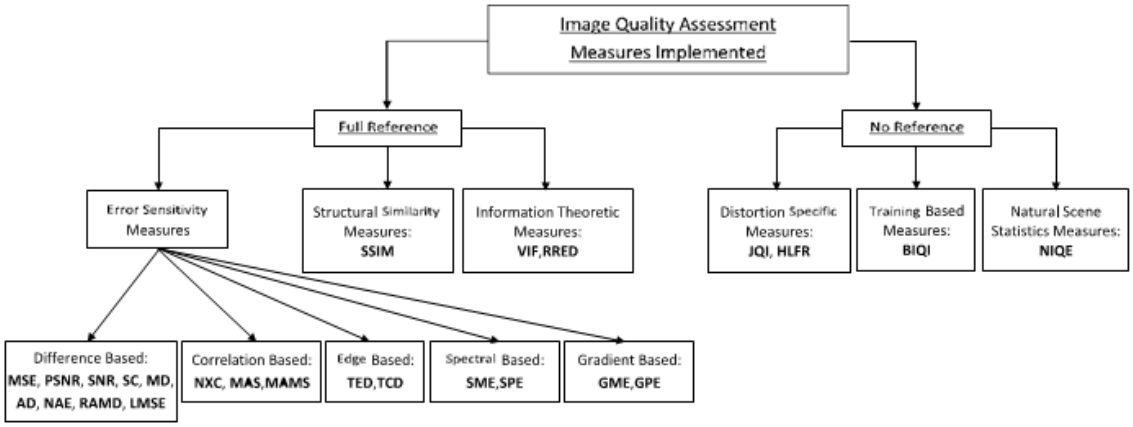

Fig.3.Classificationofthe25imagequalitymeasuresimplementedinthework.Acronyms(inbold)ofthedifferentmeasuresareexplainedinTableIandSectionIII.

III. THESAFETYPROTECTIONMETHOD

The safety protection methodology downside the matter biometric detection are often seen as a 2-class classification problem wherever Associate in Nursing input biometric sample must be appointed to 1 of two classes: real or fake. The key purpose of the method is to find a group of discriminant options which allows to create Associate in Nursing applicable classifier which supplies the chance of the image "realism" given the extracted set of options. Within the gift work we have a tendency to propose a unique parameterization mistreatment twenty five general image quality measures. A general diagram of the protection approach planned during this work is shown in Fig. 2. So as to stay its generality and ease, the system wants only 1 input: the biometric sample to be classified as real or faux (i.e., identical image non heritable for biometric recognition purposes). Moreover, because the methodology operates on the entire image while not searching for any trait-specific properties, it doesn't needany preprocessing steps (e.g., fingerprint segmentation, iris detection or face extraction) before the computation of the intelligence quotient options. This characteristic minimizes its procedure load. Once the feature vector has been generated the sample is classified as real (generated by a real trait) or faux (synthetically produced), mistreatment some easy classifiers. Particularly, for our experiments we've thought of standardic language implementations in Matlab of the Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers.The parameterization projected within the gift work comprises twenty five image quality measures each reference and blind because it would be unworkable to hide all the vast vary of strategies, approaches and views projected within the literature for IQA, the initial feature choice method to work out the set of twenty five IQMs has been allotted per four general criteria, that intend that the final methodology complies to the best potential extent with the fascinating needs set for aliveness detection systems. These four choice criteria are:

• Complementarity: So as to come up with a system as general as potential in terms of attacks detected and biometric modalities supported, we've given priority to IQMs supported complementary properties of the image (e.g., sharpness, entropy or structure)

• Complexness: So as to stay the simplicity of the strategy, low complexness options are most well-liked over those that need a high machine load.Unknown, because the detection system solely has access to the input sample. So as to avoid this limitation, an equivalent strategy already with success used for image manipulation detection in and for steganalysis in is enforced here.

A. Full Reference –IQMeasures:

Many of those metrics are enclosed within the 26-feature parameterization planned within the gift work. For clarity, these options are classified here into five totally different categories consistent with the image property measured: Picture element distinction measures. These options calculate the distortion between 2 pictures on the idea of their pixel wise variations. Here we have a tendency to include: Mean square Error (MSE), Peak Signal to Noise quantitative relation (PSNR), Signal to Noise quantitative relation (SNR), Structural Content (SC), most distinction (MD), Average distinction (AD), Normalized Absolute Error (NAE), R-Averaged most distinction (RAMD) and Laplacian Mean square Error (LMSE). The formal into the HIV definitions for every of those options area unit given in Table I. within the RAMD entry in Table I, max is defined because the r-highest picture element distinction between 2 pictures. For this implementation, R =10. within the LMSE entry in Table I, $h(I_{i,j}) = I_{i+1,j} + I_{i-1,j} + I_{i,j+1} + I_{i,j-1} - 4I_{i,j}$. The VIF live comes from the magnitude relation of 2 mutual data quantities: the mutual data between the input and also the output of the HVS channel once no distortion channel is gift and also the mutual information between the input of the distortion channel and also the output of the HVS channel for the check image. Therefore, to reckon the VIF metric, the whole reference image is needed as quality is assessed on a worldwide basis. On the opposite hand, the RRED metric approaches the problem space vehicle of QA from the angle of measurement the quantity of native data distinction between the reference image and also the projection of the distorted image onto the house of natural pictures, for a given sub band of the wave domain.

• Performance: Solely wide used image quality approaches that are systematically tested showing sensible performance for various applications are thought of attack detects.

In essence, the RRED formula computes the typical distinction between scaled native entropies of wave coefficients of reference and projected distorted pictures in a very distributed fashion. This way, contrary to the VIF feature, for the RRED it's not necessary to own access the whole reference image however solely to a reduced a part of its data. This needed data will even be reduced to only 1 single scalar just in case all the scaled entropy terms within the elect wave sub band square measure thought-about in one single block.

B. No-Reference IQ Measures

Unlike the target reference IQA ways, normally the human sensory system doesn't need of a reference sample to work out the standard level of a picture. Following this same principle, automatic no-reference image quality assessment (NR-IQA) algorithms try and handle the terribly complicated and difficult downside of assessing the visual quality of pictures, within the absence of a reference. Presently, NR-IQA ways usually estimate the standard of the check image in step with some pre-trained applied mathematics models. Counting on the photographs accustomed train this model and on the a priori knowledge needed, the ways square measure coarsely divided into one in all 3 trends:

• Distortion-specific approaches: The final quality live is computed in line with a model trained on clean pictures and on pictures full of this explicit distortion. 2 of those measures are enclosed within the biometric protection technique projected within the gift work. The JPEG Quality Index (JQI), that evaluates the standard in pictures full of the standard block artifacts found in several compression algorithms running at low bit rates like the JPEG. Within the current implementation, il =ih =0.15N and jl = jh = zero.15M.

• Training-based approaches: During this variety of techniques a model is trained mistreatment clean and distorted pictures. Then, the standard score is computed supported variety of options extracted from the check image and associated with the final model.. This is the case of the Blind Image Quality Index (BIQI) de lineated in, that is an element of the twenty five feature set employed in this work. The BIQI follows a two-stage framework during which the individual measures of various distortion-specific consultants area unit combined to get one world quality score.

• Natural Scene datum approaches. These blind IQA techniques use a priori knowledge taken from natural scene distortion-free pictures to coach the initial model. The explanation behind this trend depends on the hypothesis that artless pictures of the flora and fauna gift bound regular properties that fall at intervals a precise topological space of all attainable pictures. The NIQE may be a fully blind image quality instrument supported the development of a top quality aware assortment of applied mathematics options associated with a multi chance variable mathematician natural scene applied mathematics model.

Table I

Listofthe26imagequalitymeasures(iqms)implementedinthepresentworkandusedforbiometricprotection.allthefeatureswereeitherdirectlytakenoradaptedfromthereferencesgiven.inthetable:frdenotesfull-referenceandnrno-reference;idenotesthereferencecleanimage(ofsizen×m)andithesmoothedversionofthereferenceimage.forothernotationspecifications andundefinedvariablesorfunctionswereferthereadertothedescriptionofeachparticularfeatureinsectioniii.givenreferences

#	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]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
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]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-\lambda_1-\alpha_{i,j})[1-\frac{\lvert\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert\rvert}{255}]\}$
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]

IV. EXPERIMENTSANDRESULTS

A. Results: Iris

For the iris modality the protection technique is tested below 2 completely different attack eventualities, namely: i) spoofing attack and ii) attack with artificial samples.For each of the eventualities a specific combine of real-fake databases is employed. Databases area unit divided into all freelance (in terms of users): toy, wont to train the classifier; and take a look at set, wont to evaluate the performance of the projected protection technique.In all cases the final results (shown in Table II) area unit obtained applying two-fold cross validation.The classifier used for the 2 eventualities is predicated on Quadratic Discriminant Analysis (QDA) because it showed a rather higher performance than Linear Discriminant Analysis (LDA), which can be employed in the face-related experiments, whereas keeping the simplicity of full system.

1) Results: Iris-Spoofing: The info employed in this spoofing situation is that the ATVS-FIR decibel which can be obtained from the Biometric Recognition Group-ATVS. The info includes real and faux iris pictures of fifty users indiscriminately selected from the Bio sec baseline corpus. It follows an equivalent structure because the original Bio sec dataset, therefore, it includes fifty users × two eyes × four pictures × two sessions = 800 faux iris pictures and its corresponding original samples. The acquisition of each real and faux samples was dispensed victimisation the LG IrisAccess EOU3000 detector with infrared illumination that captures bmp grey-scale pictures of size 640 ×480 pixels.In Fig. four we tend to show some typical real and faux iris pictures which will be found within the dataset.As mentioned higher than, for the experiments the info is split into a: toy, comprising four hundred real pictures and their corresponding faux samples eyes; and a take a look at set with the remaining four hundred real and faux samples returning from the opposite 50 eyes accessible within the dataset.

Fig.4. Typicalrealirisimages(toprow)andtheircorresponding fakesamples(bottomrow)thatmaybefoundintheATVS-FIRDB(toprow)andfakesamplesfromWVU-SyntheticIris usedintheiris-spoofingexperiments.DB(bottomrow),usedintheiris-syntheticexperiments.

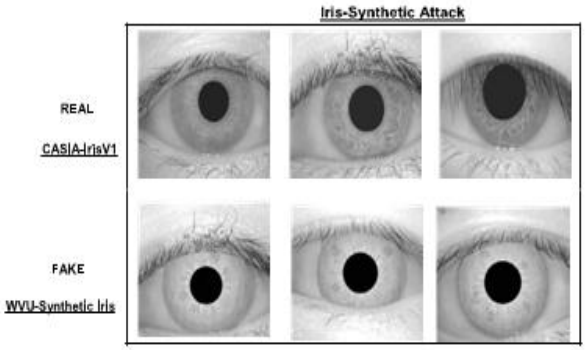

Fig.5.TypicalrealirisimagesfromCASIA-IrisV1

The aliveness detection results achieved by the projected approach below this situation seem within the first row of Table II, wherever we will see that the strategy is in a position to properly classify over ninety seven of the samples. Within the last column we tend to show the typical execution time in seconds required to method every sample of the 2 thought of databases. Now was measured on a customary 64-bit Windows7-PC with a three.4 Gc processor and sixteen GB RAM memory, running MATLAB R2012b.As no different iris aliveness detection technique has however been reported on the general public ATVS-FIR decibel, for comparison, the second row of Table II reports the results obtained on this info by a self-implementation of the anti-spoofing technique projected in [28]. It should be discovered that the projected technique not solely outperforms the progressive technique, but also, because it doesn't need any iris detection or segmentation, the time interval is around ten times quicker.

2) Results: Iris-Synthetic: During this situation attacks area unit per-formed with synthetically generated iris samples that area unit injected within the communicating between the detector and also the feature extraction module. The important and pretend databases utilized in this case are:

• Real database: CASIA-IrisV1.This dataset is publicallyout there through the Biometric Ideal take a look at (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA).2 It contains seven grey-scale 320×280 pictures of 108 eyes captured in 2 separate sessions with a self-developed CASIA close-up camera and area unit hold on in bmp format.

• Artificial database: WVU-Synthetic Iris decibel. Being a info that contains solely absolutely artificial information, it's not subjected to any legal constraints and is publically out there through the CITER centre.3The artificial irises area unit generated following the tactic delineated, that has 2 stages. Within the first stage, a Markoff Random Field model trained on the CASIA-IrisV1 decibel is employed to get a background texture representing the world iris look.

A consequence of the coaching method administered on the CASIA-IrisV1 decibel, the artificial samples area unit visually terribly almost like those of the important dataset, that makes them specially appropriate for the thought of assaultive situation.The last column indicates, in seconds, the typical execution time to method every sample.In the experiments, so as to possess balanced coaching categories(real and fake) solely fifty four artificial eyes were willy-nilly elect. This way, the matter of overfitting one category over the opposite is avoided. The take a look at set contains the remaining fifty four real eyes and 946 artificial samples.The results achieved by the projected protection methodology supported IQA on this assaultive situation area unit shown within the bottom row of Table II. In spite of the similarity of

real and pretend pictures, the world error of the algorithmic program during this situation is a pair of.1%.The experiments rumored during this Section IV-A show the power of the approach to adapt to totally different assaultive situations and to stay a high level of protection all told of them. Therefore, the results conferred in Table II confirm the "multi-attack" dimension of the projected methodology. The same QDA classifier already thought-about within the iris-related experiments is employed here.

1) Results: Fingerprints-Spoofing: Within the bottom row we tend to show the common execution time in seconds required to method every sample of the 3 datasets. As within the iris and fingerprint experiments, this point was measured on a customary 64-bit Windows7-PC with a three.4 Giga cycle processor and sixteen GB RAM memory, running MATLAB R2012b. Recall that the print, mobile and high def eventualities see the kind of artefact being employed as forgery and to not the acquisition device, that is DE same for all cases.

In the grand test experiments the protection methodology is trained victimisation knowledge from the print, mobile and high def situations, and tested additionally on samples from the 3 sort of attacks. This can be in all probability the foremost realistic attack case, as, in general, we have a tendency to cannot grasp a priori the sort of object that the assaulter can use to undertake to interrupt into the system.

The performance shown by the planned algorithmic rule within the face-based analysis confirm the conclusions extracted from the iris and fingerprint experiments: the IQA-based protection methodology is ready to adapt to totally different modalities, databases and attacks performing arts systematically well altogether of them. In totally different LBP-based anti-spoofing techniques were tested following the precise same protocol utilized in the current work. Results were solely reported on the grand test situation considering all kinds of supports. The error rates of all strategies area unit terribly similar, however, the IQA-basedhas the advantage of its simplicity and generality.

The fact that several of the contestants were employing a sequence of frames to classify every video our planned IQA-based methodology performs equally to the highest hierarchal systems. Furthermore, many of the algorithms conferred to the competition area unit supported motion detection of the face and, therefore their ability to discover faux access tries distributed with replayed motion videos would be a minimum of underneath question. It ought to even be noted that in several applications there is no access to a video of the user. For these situations, several of the anti-spoofing solutions bestowed at the competition wouldn't be usable as they are not designed to figure on one static face image

V. CONCLUSION

The study of the vulnerabilities of biometric systems against differing kinds of attacks has been awfully active field of analysis in recent years. This interest has cause massive advances within the field of security-enhancing technologies for biometric-based applications. Simple visual examination of a picture of a true biometric attribute and a pretend sample of an equivalent attribute shows that the two pictures are often terribly similar and even the human eye might find it difficult to create a distinction between them when a brief examination. Yet, some disparities between the important and faux pictures might become evident once the pictures are translated into a correct feature house. These variations return from the actual fact that biometric traits, as 3D objects, have their own optical qualities, that alternative materials or synthetically made samples don't possess. What is more, biometric sensors are designed to produce smart quality samples once they act, in an exceedingly traditional operation surroundings, with a true 3D attribute. If this state of affairs is modified, or if the attribute bestowed to the scanner is sudden pretend unit, the characteristics of the captured image might significantly vary. In this context, it's cheap to assume that the image quality properties of real accesses and fallacious attacks are going to be totally different. Following this "quality-difference" hypothesis, within the gift analysis work we've got explored the potential of general image quality assessment as a protection tool against totally different biometric attacks. For this purpose we've got thought-about a feature house of twenty six complementary image quality measures that we've got combined with easy classifiers to notice real and faux access makes an attempt.

The novel protection technique has been evaluated on 3 mostly are duplicable and will be fairly compared with alternative future analogue solutions. Several conclusions is also extracted from the analysis results given within the experimental sections of the article: i) The projected methodology is ready to systematically perform at a high level totally different for various biometric traits ("multi-biometric"); ii) The projected methodology is ready to adapt to differing types of attacks providing for all of them a high level of protection ("multi-attack"); iii) The projected methodology is ready to generalize well to different databases, acquisition conditions and attack scenarios; iv) The error rates achieved by the projected protection theme are in several cases under those rumored by alternative trait-specific progressive anti-spoofing systems that are tested within the framework of various independent competitions v) additionally to its terribly competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the projected methodology presents another terribly enticing options such as: it's easy, fast, non-intrusive, easy and low-cost, all of them terribly fascinating properties in an exceedingly sensible protection system.

All the previous results validate the "quality-difference" hypothesis. "It is predict that a pretend image captured in an attack try can have totally different quality than a true sample nonheritable within the traditional operation situation that the detector was designed.In this context, this work has created many contributions to the progressive within the field of biometric security, in particular: i) it's shown the high potential of image quality assessment for securing biometric systems against a range of attacks; ii) proposal and validation of a brand new biometric protection method; iii) duplicable analysis on multiple biometric traits supported in public on the market databases; iv) comparative results with alternative projected protection solutions. The present analysis conjointly opens new potentialities for future work, including: i) extension of the thought-about 26-feature set with new image quality measures; ii) more analysis on

alternative image-based modalities (e.g., palm print, hand pure mathematics, vein); iii) inclusion of temporal info for those cases within which it's on the market (e.g., systems operating with face videos); iv) use of video quality measures for video attacks (e.g., hot access tries thought-about within the REPLAY-ATTACK DB); v) analysis of the options individual connexion.

REFERENCES

[1] S.Prabhakar, S.Pankanti, and A.K.Jain, "Biometricrecognition: Securityandprivacyconcerns, "IEEE Security Privacy,vol.1, no.2,pp.33–42,Mar./Apr.2003.

[2] T.Matsumoto,"Artificialirises:Importanceofvulnerabilityanalysis,"inProc.AWB,2004.

[3] J.Galbally,C.McCool,J.Fierrez,S.Marcel,andJ.Ortega-Garcia,"Onthevulnerabilityoffaceverificationsystemstohill-climbingattacks,"PatternRecognit.,vol.43,no.3,pp.1027–1038,2010.

[4] A.K.Jain,K.Nandakumar,andA.Nagar,"Biometrictemplatesecurity,"EURASIPJ.Adv.SignalProcess., vol.2008,pp.113–129,Jan.2008.

[5] J.Galbally,F.Alonso-Fernandez,J.Fierrez,andJ.Ortega-Garcia,"Ahighperformancefingerprintlivenessdetectionmethodbasedonqualityrelatedfeatures,"FutureGenerat.Comput.Syst.,vol.28,no.1,pp.311–321,2012.

[6] S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network Infrastructures", International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April 2013.

[7] A.Nixon,V.Aimale,andR.K.Rowe,"Spoofdetectionschemes,"HandbookofBiometrics.NewYork,NY,USA: Springer-Verlag,2008,pp.403–423.

[8] ISO/IEC19792:2009,InformationTechnology—SecurityTechniques—SecurityEvaluationofBiometrics,ISO/IECStandard19792,2009.

[9] K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.

[10] BiometricEvaluationMethodology.v1.0,CommonCriteria,2002.

[11] K.Bowyer,T.Boult,A.Kumar,andP.Flynn,ProceedingsoftheIEEEInt.JointConf.onBiometrics. Piscataway,NJ,USA:IEEEPress,2011.

[12] G.L.Marcialis,A.Lewicke,B.Tan,P.Coli,D.Grimberg,A.Congiu,etal., Firstinternationalfingerprintlivenessdetectioncompetition—LivDet2009,"inProc.IAPRICIAP,SpringerLNCS-5716.2009,pp.12–23.

[13] K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.

[14] Ms. J.Praveena, K.G.S.Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.

[15] M.M.Chakka,A.Anjos,S.Marcel,R.Tronci,B.Muntoni,G.Fadda,etal., "Competitiononcountermeasuresto2Dfacialspoofingattacks,"inProc.IEEEIJCB,Oct.2011,pp.1–6.

[16] BiometricsInstitute,London,U.K.(2011).BiometricVulnerabilityAssessment Expert Group [Online]. Available:http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group- vaeg.html

[17] (2012).BEAT:BiometricesEvaluationandTesting[Online].Available:http://www.beat-eu.org/

[18] J.Galbally,J.Fierrez,F.Alonso-Fernandez,andM.Martinez-Diaz,"Evaluationofdirectattackstofingerprintverificationsystems,"J.Telecommun.Syst.,vol.47,nos.3–4,pp.243–254,2011.

[19] A.AnjosandS.Marcel, "Counter-measurestophotoattacksinfacerecognition: Apublicdatabaseandabaseline, "inProc. IEEEIJCB, Oct. 2011,pp.1–7.

[20] K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.

