ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Statistical Image Quality Assessment for Fake Biometric Detection Based on SVM Classification: Application to Iris, and Face Recognition

R.Jayavadivel[1], B.Prabhushankar[2] , S.Rajesh[3]

Assistant Professor, Department of IT, Paavai Engineering College, Namakkal, Tamilnadu, India

Associate Professor, Department of IT, Paavai Engineering College, Namakkal, Tamilnadu, India

Assistant Professor, Department of CSE, Paavai Engineering College, Namakkal, Tamilnadu, India

ABSTRACT: Image quality assessment plays an important role in the performance of biometric system involving iris and face images. Data quality assessment is a key issue in order to broaden the applicability of iris and face biometrics to unconstrained imaging conditions. In this paper, we have proposed the quality factors of individual iris images by assessing their prominent factors by their scores. Biometric systems based on iris and face is vulnerable to direct attacks consisting on the presentation of a fake iris to the sensor. Widening a previous work, several state of- the-art iris liveness detection methods were implemented and adapted to a less-constrained scenario. The proposed method combines a feature selection step prior to the use of state-of-the art classifiers to perform the classification based upon the "best features". Support Vector Machine (SVM) classification technique is used for training and testing thE Iris and Face images. The testing input Iris and Face image is resulted as real and fake Iris and Face image by quality score matching with the training based real and fake Iris and Face samples.

KEYWORDS: Image quality, Iris and Face liveness detection biometrics security, support vector machine (SVM).

I. INTRODUCTION

Biometric systems rather identify an individual by what he is instead of based on something he knows or possesses. Considering that any piece of material or knowledge can be fraudulently acquired biometrics can offer several advantages over classical security methods. However, in spite of its advantages, biometric systems have some drawbacks, including the lack of secrecy, the fact that a biometric trait cannot be replaced and its vulnerability to external attacks which could decrease their level of security. It is necessary to keep in mind the security issues when we explore a whole new world of possibilities in this networked society of nowadays. Our mobile devices are turning into storages of personal, professional, commercial, and other kinds of information. This information is intended by the users to be kept confidential.

The necessity of controlling the access to this information opens the way to the concept of "mobile biometrics". Among the different existing biometric traits, iris has been traditionally regarded as one of the most reliable and accurate. Also the imaging properties of the handheld devices make this trait instinctive to use. Therefore the development of iris liveness detection techniques is crucial for the deployment of iris biometric applications in daily life. In a previous work we explored the use of countermeasures against spoofing attacks [1]. These attacks may consist on presenting a synthetically generated iris to the sensor so that it is recognized as the legitimate user and access is granted. The most common and simple approaches are those carried out with high quality iris printed images [2]. However, other more sophisticated threats have also been reported in the literature such as the use of contact lenses [3].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

In the present work we lean upon the previous work [1] and broaden the application of the method pursuing more unconstrained conditions. The methods for liveness detection may be hardware or software based. In the present work we use a software based approach. These countermeasures are to prevent attacks at sensor level. So, the fake irises are detected once the sample has been acquired with a standard sensor. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the sample vitality given the extracted set of features. In the previous work, the segmentation of iris was done manually; however, this is unrealistic if we are aiming a real world application. To overcome this less realistic scenario, in the present work we applied a automatic segmentation method. Therefore some of the implemented state-of-the-art methods were adapted to the non-circular contours obtained by the segmentation method. For the feature extraction, several state-of-the-art methods were implemented to perform the feature extraction that will help to discriminate between fake and real iris. Like previously, the extracted features were then included in a feature selection framework so as to determine the best cardinality and the best subset that conducts to the highest classification rate.

II.RELATED WORK

The problem of liveness detection of a biometric trait can be seen as a two class classification problem where an input trait sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the sample vitality given the extracted set of features [4]. Biometric recognition systems are vulnerable to be spoofed by fake copies [5], for instance, fake finger tips made of commonly available materials such as clay and gelatin. Iris is no exception. There are potential threats for iris-based systems, the main are [6]: Eye image: Screen image, Photograph, Paper print, Video signal.

Several liveness detection methods have been presented through the past recent years. In fact, anti-spoofing techniques were presented that use physiological properties to distinguish between real and fake biometric traits. This is done in order to improve the robustness of the system against direct attacks and to increase the security level offered to the final user. Iris liveness detection approaches can broadly be divided into: i) software-based techniques, in which the fake irises are detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake eyes are extracted from the iris image, and not from the eye itself), and ii) hardware-based techniques, in which some specific device is added to the sensor in order to detect particular properties of a living iris such as the eye hippos' (which is the permanent oscillation that the eye pupil presents even under uniform lighting conditions) or the pupil response to a sudden lighting event (e.g., switching on a diode) [4]. According to this author, even though hardware based approaches usually present a higher detection rate, the software-based techniques have the advantage of being less expensive (as no extra device in needed), and less intrusive for the user (very important characteristic for a practical liveness detection solution). In general, a combination of both type of anti-spoofing schemes would be the most desirable approach to increase the security level of biometric systems. [4] In this work we focus on software based techniques since these are more easily and affordable applicable in real-world applications. In the literature we found that the methods of liveness detection may be classified into four categories based on the physical features of biometric and liveness data and the timing of measurement [9]. In this framework, the biometric data are used in the iris recognition and the liveness data are used in the liveness detection.

We can itemize the four categories:

1. Perfect matching model: Both biometric and liveness data are simultaneously obtained from the same physical feature.
2. Simultaneous measuring model: Biometric and liveness data are simultaneously obtained from different physical features.
3. Same biometric measuring model: Biometric and liveness data are obtained from the same physical feature with different timings.
4. Independent measuring model: Biometric and liveness data are obtained from different features with different timings.

A strategy based on the combination of several quality related features has also been used for spoofing detection in fingerprint based recognition systems [12] as well as in iris liveness detection [4]. In this latter work, a set of quality

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

measures are used as iris liveness detection features to aid the classification of fake or real iris images included in a framework of feature selection.

We find in literature that works concerning the quality of iris images are often the starting point to iris liveness detection techniques. One example is the assessment of the iris image quality based on measures like occlusion, contrast, focus and angular deformation [13], other is the use of texture analysis of the iris [14], among others like, for example, the analysis of frequency distribution rates of some specific regions of iris [15]. The way forward seems to be the development of techniques for iris liveness detection that work well independently of the particular characteristics of the databases available nowadays. It is required to develop and improve methods as well as to construct new databases in less constrained conditions.

III. FACE LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the fingerprint images acquired from a gummy finger present local gaining artifacts such as spots and patches. The potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing) [6].Different quality measures present diverse sensitivity to image artifacts and distortions. For example, measures like the mean squared error respond additional to additive noise, although 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 a large 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 [1]. A novel parameterization using 25 general image quality measures. In order to keep its generality and simplicity, the system requires one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes).Once the feature vector has been generated the sample is classified as real or fake using SVM classifier [13].The parameterization proposed in the present work comprises 25 image quality measures for both reference and blind. Image quality has been successfully used in previous works for image manipulation detection and steganalysis 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 [8]. Fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches [3].

3.1 Block Diagram Description

3.1.1 Input Image

The input image captured from the sensor should be 2D image. Finger print is captured from the flat optical sensor for the real and fake classification. Biometric images like face, iris and palm print also be used for the input image for image quality assessment technique [1].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

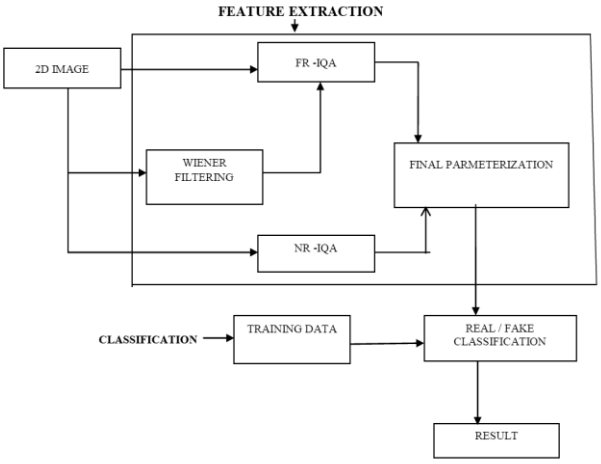

Figure 1: Block Diagram - Image Quality Assessment for Fake Finger Print Detection

3.1.2 Wiener Filtering

The input grey-scale image **I** (of size N × M) is filtered with wiener filtering in order to generate a smoothed version ˆ**I** .The noise reduced by wiener filtered input finger print image is good capable for IQA technique. Because wiener filter are adaptive in nature. So wiener filtering technique is used for reducing noise in input finger print image [3].

3.1.3 Full-Reference IQ Measures

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in and for steganalysis is implemented here.

3.1.4 No-Reference IQ Measures

Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image. Following this same principle, automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference. Presently, NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models. Depending on the images used to train this model and on the a priori knowledge required, the methods are coarsely divided into one of three trends [14]. smoothed version ˆ**I**. Then, the quality between both images (**I** and ˆ**I**) is computed according to the corresponding full-reference IQA metric. This approach assumes that the loss of quality produced by Wiener filtering differs between real and fake biometric samples [1].

IV. SVM CLASSIFICATION

Support vector machines (SVM) are supervised learning models with associated learning algorithms that analyze data and used to classify the pattern. An SVM training algorithm builds a model that assigns new examples into one category or the other and it is based on the non-probabilistic binary linear classifier [13].

4.1. Algorithm For SVM Classification

4.1.1 Training Algorithm:

Step 1: Read the iris or face Input training Images from the database.
Step 2: Find 25 Image Quality Assessment Measures (No Reference & Full Reference) for the iris or face training images.
Step 3: Combine all Quality Measure as a image quality assessment feature .
Step 4: Create Target for Svm classification Training.
Step 5: Make Svm classifier traning with two classes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

4.1.2 Testing Algorithm:

Step 1: Read the iris or face Test Image from the database.
Step 2: Find 25 Image Quality Measures (No Reference & Full Reference) for the iris or face testing image.
example : peak signal to noise ratio,average difference ,maximum differencre .... and other quality features.
Step 3: Combine all Quality Measure as a feature.
Step 4: Feature Compared with trained Feature using svm classification
Step 5: Final result Given test image is fake or real iris and face image.

V. RESULTS AND DISCUSSION

The following message box appears after finding 25 image quality assessment parameters for training the finger print image in SVM classifier.

The following message box appears after finding 25 image quality assessment parameters for testing the finger print image in SVM classifier.

Iris Database Image

- Typical real iris image are taken from CASIA-IrisV1 and fake samples are made by blurring technique.
- The databases are available at http://biometrics.idealtest.org http://www.citer.wvu.edu/.

Figure 2. Real Irish Images

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Table I
Real Irish Image Quality Feature

PARAMETER	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6	IMAGE 7	IMAGE 8	IMAGE 9	IMAGE 10	IMAGE 11	IMAGE 12
MSE(e^+2)	1.74	1.43	1.4	1.9	1.77	1.43	1.63	1.3	1.37	1.44	1.27	1.06
PSNR(e^+1)	2.57	2.65	2.66	2.55	2.56	2.65	2.68	2.59	2.69	2.67	3.7	3.78
SNR(e^+1)	2.33	2.45	2.42	2.25	2.31	2.42	2.44	2.23	2.39	2.31	2.58	2.74
SC(e^+0)	1.1	1.13	1.14	1.16	1.12	1.1	1.18	1.02	1.04	1.05	1.17	1.04
MD	86	82	91	85	94	81	91	87	84	89	88	95
AD(e^+1)	2.33	2.45	2.42	2.25	2.32	2.42	2.44	2.23	2.29	2.31	2.58	2.74
NAE(e^-2)	5.18	4.23	4.35	5.81	4.96	4.34	4.07	5.94	5.55	5.43	3.77	2.99
RAMD	8.6	8.2	9.1	8.5	9.4	8.1	9.1	8.7	8.4	8.9	8.8	9.5
LMSE(e^+1)	8.12	9.45	7.43	8.04	8.44	6.34	5.87	7.89	5.98	8.34	8.56	7.43
NXC(e^-1)	9.9	9.91	9.93	9.87	9.89	9.95	9.78	9.71	9.34	9.81	9.56	9.76
MAS(e^-2)	4.12	4.23	5.78	6.32	4.98	5.89	4.87	5.32	5.87	4.67	4.29	4.56
MAMS(e^+6)	24.4	22.5	21.8	22.9	24.6	23.8	26.8	22.6	23.4	25.6	23.9	25.5
TED(e^2)	10.2	9.31	8.94	7.21	11.2	8.98	10.4	11.8	12.5	10.8	9.34	11.8
TCD(e^-1)	15.3	12.5	11.8	13.2	17.3	12.4	11.5	12.8	13.8	15.8	14.9	13.1
SME(e^-3)	2.33	3.44	4.89	2.44	3.89	4.76	2.43	3.97	5.34	4.12	3.23	4.21
SPE(e^-7)	10.3	11.7	13.5	12.8	13.9	9.32	10.9	12.3	14.2	8.34	10.2	9.34
GME(e^4)	5.22	6.34	7.32	5.54	4.22	5.23	6.22	7.23	5.89	4.12	5.32	7.44
GPE(e^2)	3.12	3.56	4.12	5.23	6.23	4.23	7.34	5.34	6.39	5.23	3.45	5.32
SSIM(e^-1)	8.21	8.45	8.87	8.64	8.91	8.02	8.23	8.75	8.5	8.98	8.12	8.04
VIF	84	87	98	78	94	74	81	96	82	93	83	91
RRED	123	134	164	173	183	153	182	172	133	152	132	143
JQI(e^+1)	1.43	2.54	2.12	3.19	4.21	1.01	1.32	1.54	2.09	2.89	3.23	1.02
HLFI(e^-2)	7.23	6.34	7.45	8.56	8.67	9.34	8.34	7.03	6.92	8.44	7.87	7.94
BIQI(e^-1)	2.87	3.29	1.34	2.8	1.87	2.21	3.84	1.09	2.82	1.07	3.98	3.98
NIQE(e^+1)	9.01	8.87	7.18	7.34	9.23	8.12	9.5	6.33	7.22	8.32	5.88	2.98

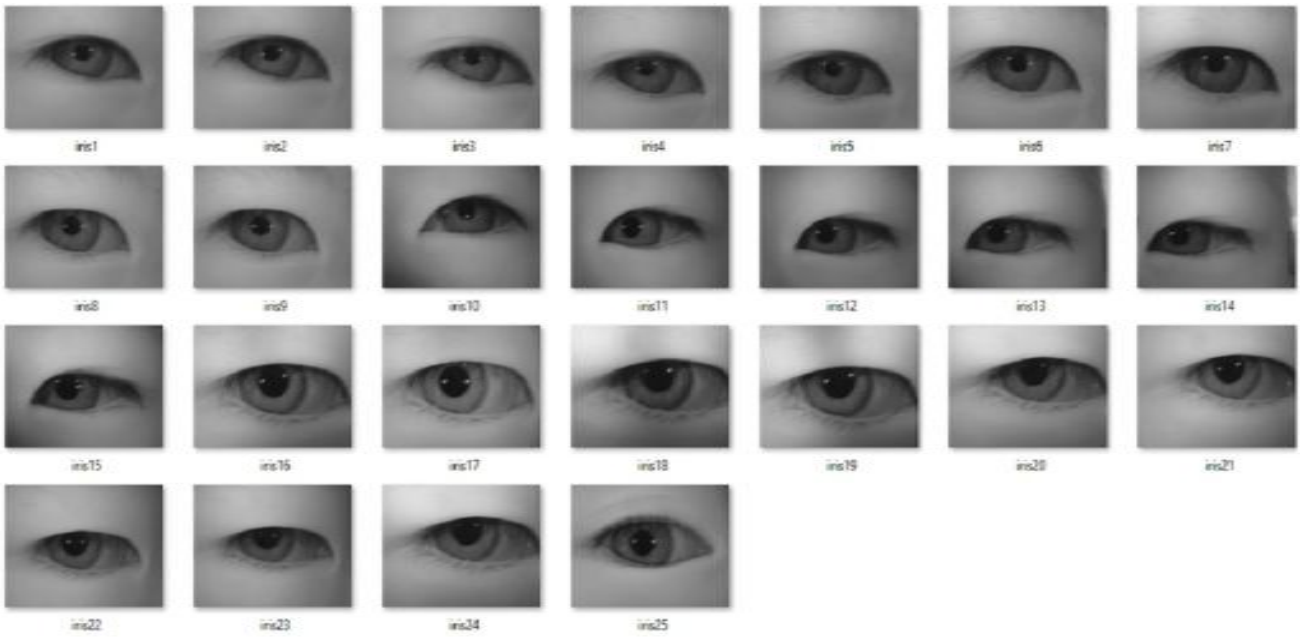

Figure 3. Fake Irish Images

Face Database Image

- Typical examples of real face image can be found in the public REPLAY-ATTACK DB and fake samples are made by blurring technique. The database is available at https://www.idiap.ch/dataset/replayattack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Table II
Fake Iris Image Quality Features

PARAMETER=	IMAGE-1=	IMAGE-2=	IMAGE-3=	IMAGE-4=	IMAGE-5=	IMAGE-6=	IMAGE-7=	IMAGE-8=	IMAGE-9=	IMAGE-10=	IMAGE-11=	IMAGE-12=
MSE(e^+2)=	1.14=	1.1=	1.16=	1.12=	1.1=	1.04=	1.03=	1.17=	1.04=	1.18=	1.02=	1.15=
PSNR(e^+1)=	2.45=	2.52=	2.23=	2.65=	2.98=	2.43=	2.91=	2.34=	2.78=	2.12=	3.94=	3.63=
SNR(e^+1)=	2.02=	2.12=	2.34=	2.21=	2.39=	2.46=	2.42=	2.21=	2.35=	2.01=	2.87=	2.92=
SC(e^+0)=	1.74=	1.43=	1.4=	1.9=	1.77=	1.23=	1.03=	1.78=	1.14=	1.2=	1.19=	1.93=
MD=	81=	87=	86=	91=	89=	75=	83=	72=	93=	82=	74=	81=
AD(e^+1)=	3.32=	4.55=	4.21=	5.21=	2.99=	3.99=	4.32=	3.24=	3.22=	2.42=	2.53=	2.67=
NAE(e^-2)=	2.18=	7.23=	5.34=	2.31=	7.32=	2.94=	1.07=	3.94=	2.42=	4.31=	5.7=	6.95=
RAMD=	8.1=	8.7=	8.6=	9.1=	8.9=	7.5=	8.3=	7.2=	9.3=	8.2=	7.4=	8.1=
LMSE(e^+1)=	2.12=	5.45=	3.43=	1.04=	2.44=	3.34=	1.87=	3.89=	4.98=	3.34=	2.56=	5.43=
NXC(e^-1)=	9.43=	9.21=	9.56=	9.87=	9.01=	9.03=	9.16=	9.26=	9.65=	8.61=	9.01=	9.34=
MAS(e^-2)=	7.12=	2.21=	1.78=	8.3=	2.82=	1.92=	5.31=	4.19=	7.32=	2.73=	5.29=	4.56=
MAMS(e^+6)=	19.4=	17.5=	16.3=	27.9=	19.6=	18.8=	21.8=	17.6=	16.4=	31.6=	28.9=	19.5=
TED(e^2)=	10.2=	9.31=	8.94=	7.21=	11.2=	8.98=	10.4=	11.8=	12.5=	10.8=	9.34=	11.8=
TCD(e^-1)=	15.3=	12.5=	11.8=	13.2=	17.3=	12.4=	11.3=	12.8=	13.8=	15.8=	14.9=	13.1=
SME(e^-3)=	2.43=	3.23=	4.45=	2.12=	3.56=	4.54=	2.64=	3.12=	5.65=	4.63=	3.97=	4.2=
SPE(e^-7)=	2.35=	6.27=	8.53=	2.81=	6.79=	4.3=	5.19=	7.73=	9.22=	2.36=	4.22=	4.21=
GME(e^4)=	2.02=	1.43=	4.12=	7.24=	6.32=	1.32=	3.24=	5.21=	8.12=	5.65=	2.42=	6.12=
GPE(e^2)=	3.45=	3.16=	3.56=	5.43=	6.07=	4.34=	7.07=	4.13=	7.33=	5.53=	3.78=	4.34=
SSIM(e^-1)=	12.3=	4.45=	9.87=	3.64=	5.91=	12.2=	4.23=	5.75=	8.5=	4.98=	2.32=	11.4=
VIF=	78=	93=	82=	74=	64=	70=	84=	87=	92=	78=	77=	82=
RRED=	134=	111=	131=	119=	136=	165=	132=	176=	123=	185=	123=	156=
JQI(e^+1)=	4.31=	5.42=	1.42=	8.19=	6.45=	2.01=	6.32=	2.54=	5.09=	2.89=	7.21=	3.01=
HLFI(e^-2)=	5.34=	2.45=	1.12=	4.32=	5.67=	2.3=	2.59=	3.45=	2.54=	3.12=	4.32=	2.94=
BIQI(e^-1)=	1.34=	7.33=	6.32=	5.83=	5.54=	7.43=	6.32=	6.23=	8.82=	7.23=	9.23=	5.23=
NIQE(e^+1)=	8.01=	5.87=	6.18=	6.34=	2.23=	4.12=	3.5=	9.33=	5.22=	7.32=	4.88=	7.98=

Figure 4.Real Irish Image

The above diagram and data values representing real Irish image with minimum errors.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Table III Real Face image quality features

PARAMETER	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	IMAGE 6	IMAGE 7	IMAGE 8	IMAGE 9	IMAGE 10	IMAGE 11	IMAGE 12
MSE(e^+2)	1.74	1.43	1.4	1.9	1.77	1.43	1.63	1.3	1.37	1.44	1.27	1.06
PSNR(e^+1)	2.57	2.65	2.66	2.55	2.56	2.65	2.68	2.59	2.69	2.67	3.7	3.78
SNR(e^+1)	2.33	2.45	2.42	2.25	2.31	2.42	2.44	2.23	2.39	2.31	2.58	2.74
SC(e^+0)	1.1	1.13	1.14	1.16	1.12	1.1	1.18	1.02	1.04	1.05	1.17	1.04
MD	86	82	91	85	94	81	91	87	84	89	88	95
AD(e^+1)	2.33	2.45	2.42	2.25	2.31	2.42	2.44	2.23	2.29	2.31	2.58	2.74
NAE(e^-2)	5.18	4.23	4.35	5.81	4.96	4.34	4.07	5.94	5.55	5.43	3.77	2.99
RAMD	8.6	8.2	9.1	8.5	9.4	8.1	9.1	8.7	8.4	8.9	8.8	9.5
LMSE(e^+1)	8.12	9.45	7.43	8.04	8.44	6.34	5.87	7.89	5.98	8.34	8.56	7.43
NXC(e^-1)	9.9	9.91	9.93	9.87	9.89	9.95	9.78	9.71	9.34	9.81	9.86	9.76
MAS(e^-2)	4.12	4.23	5.78	6.32	4.98	5.89	4.87	5.32	5.87	4.67	4.29	4.86
MAMS(e^+6)	24.4	22.5	21.8	22.9	24.6	23.8	26.8	22.6	23.4	25.6	23.9	25.5
TED(e^2)	10.2	9.31	8.94	7.21	11.2	8.98	10.4	11.8	12.5	10.8	9.34	11.8
TCD(e^-1)	15.3	12.5	11.8	13.2	17.3	12.4	11.5	12.8	13.8	15.8	14.9	13.1
SME(e^-3)	2.33	3.44	4.89	2.44	3.89	4.76	2.43	3.97	5.34	4.12	3.23	4.21
SPE(e^-7)	10.3	11.7	13.5	12.8	13.9	9.32	10.9	12.3	14.2	8.34	10.2	9.34
GME(e^4)	5.22	6.34	7.32	5.54	4.22	5.23	6.22	7.23	5.89	4.12	5.32	7.44
GPE(e^2)	3.12	3.56	4.12	5.23	6.23	4.23	7.34	5.34	6.39	5.23	3.45	5.32
SSIM(e^-1)	8.21	8.45	8.87	8.64	8.91	8.02	8.23	8.75	8.5	8.98	8.12	8.04
VIF	84	87	98	78	94	74	81	96	82	93	83	91
RRED	123	134	164	173	183	153	182	172	133	152	132	143
JQI(e^+1)	1.43	2.54	2.12	3.19	4.21	1.01	1.32	1.54	2.09	2.89	3.23	1.02
HLFI(e^-2)	7.23	6.34	7.45	8.56	8.67	9.34	8.34	7.03	6.92	8.44	7.87	7.94
BIQI(e^-1)	2.87	3.29	1.34	2.8	1.87	2.21	3.84	1.09	2.82	1.07	3.98	3.98
NIQE(e^+1)	9.01	8.87	7.18	7.34	9.23	8.12	9.5	6.33	7.22	8.32	5.88	2.98

Figure 5. Fake Irish Image

Face Database Image

- Typical examples of real face image can be found in the public REPLAY-ATTACK DB and fake samples are made by blurring technique. The database is available at https://www.idiap.ch/dataset/replayattack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Table IV
Fake Face image quality features

PARAMETER=	IMAGE-1=	IMAGE-2=	IMAGE-3=	IMAGE-4=	IMAGE-5=	IMAGE-6=	IMAGE-7=	IMAGE-8=	IMAGE-9=	IMAGE-10=	IMAGE-11=	IMAGE-12=
MSE(e^+2)=	1.14=	1.1=	1.16=	1.12=	1.1=	1.04=	1.05=	1.17=	1.04=	1.18=	1.02=	1.15=
PSNR(e^+1)=	2.45=	2.52=	2.23=	2.65=	2.98=	2.43=	2.91=	2.34=	2.78=	2.12=	3.94=	3.63=
SNR(e^+1)=	2.02=	2.12=	2.34=	2.21=	2.39=	2.46=	2.42=	2.21=	2.35=	2.01=	2.87=	2.92=
SC(e^+0)=	1.74=	1.43=	1.4=	1.9=	1.77=	1.23=	1.05=	1.78=	1.14=	1.2=	1.19=	1.93=
MD=	81=	87=	86=	91=	89=	75=	83=	72=	93=	82=	74=	81=
AD(e^+1)=	3.32=	4.55=	4.21=	5.21=	2.99=	3.99=	4.32=	1.24=	3.22=	2.42=	2.53=	2.67=
NAE(e^-2)=	2.18=	7.23=	5.34=	2.31=	7.32=	2.34=	1.07=	3.94=	2.42=	4.31=	5.7=	6.95=
RAMD=	8.1=	8.7=	8.6=	9.1=	8.9=	7.5=	8.3=	7.2=	9.3=	8.2=	7.4=	8.1=
LMSE(e^+1)=	2.12=	5.45=	3.43=	1.04=	2.44=	3.34=	1.87=	3.89=	4.98=	3.34=	2.56=	5.43=
NXC(e^-1)=	9.43=	9.21=	9.56=	9.87=	9.01=	9.03=	9.16=	9.26=	9.65=	8.61=	9.01=	9.34=
MAS(e^-2)=	7.12=	2.21=	1.78=	8.3=	2.82=	1.92=	5.81=	4.19=	7.32=	2.73=	5.29=	4.56=
MAMS(e^+6)=	19.4=	17.5=	16.8=	27.9=	19.6=	18.8=	21.8=	17.6=	16.4=	31.6=	28.9=	19.5=
TED(e^2)=	10.2=	9.31=	8.94=	7.21=	11.2=	8.98=	10.4=	11.8=	12.5=	10.8=	9.34=	11.8=
TCD(e^-1)=	15.3=	12.5=	11.8=	13.2=	17.3=	12.4=	11.5=	12.8=	13.8=	15.8=	14.9=	13.1=
SME(e^-3)=	2.43=	3.23=	4.45=	2.12=	3.56=	4.54=	2.64=	3.12=	5.65=	4.63=	3.97=	4.2=
SPE(e^-7)=	2.35=	6.27=	8.53=	2.81=	6.79=	4.3=	5.19=	7.73=	9.22=	2.36=	4.22=	4.21=
GME(e^4)=	2.02=	1.43=	4.12=	7.24=	6.32=	1.32=	3.24=	5.21=	8.12=	5.65=	2.42=	6.12=
GPE(e^2)=	3.45=	3.16=	3.56=	5.43=	6.07=	4.34=	7.07=	4.13=	7.33=	5.53=	3.78=	4.34=
SSIM(e^-1)=	12.3=	4.45=	9.87=	3.64=	5.91=	12.2=	4.23=	5.75=	8.5=	4.98=	2.12=	11.4=
VIF=	78=	93=	82=	74=	64=	70=	84=	87=	91=	78=	77=	82=
RRED=	134=	111=	131=	119=	136=	165=	132=	176=	123=	185=	123=	156=
JQI(e^+1)=	4.31=	5.42=	1.42=	8.19=	6.45=	2.01=	6.32=	2.54=	5.09=	2.89=	7.21=	3.01=
HLFI(e^-2)=	5.34=	2.45=	1.12=	4.32=	5.67=	2.3=	2.59=	3.45=	2.54=	3.22=	4.32=	2.94=
BIQI(e^-1)=	1.84=	7.33=	6.32=	5.83=	5.54=	7.43=	6.32=	6.23=	8.82=	7.23=	9.23=	5.23=
NIQE(e^+1)=	8.01=	5.87=	6.18=	6.34=	2.23=	4.12=	3.5=	9.33=	5.22=	7.32=	4.88=	7.98=

5.1 TESTING RESULTS FOR IRIS IMAGE

5.1.1. Real Iris Image Quality Features

Table V. Testing Results For Real Iris Image

PARAMETER	INPUT IMAGE (REAL)	INPUT IMAGE(FAKE)
MSE(e^+2)	1.63	**7.43**
PSNR(e^+1)	2.57	**5.21**
SNR(e^+1)	2.21	**6.06**
SC(e^+0)	1.08	**3.32**
MD	75	**84**
AD(e^+1)	7.32	**3.42**
NAE(e^-2)	5.18	**5.18**
RAMD	7.5	**8.4**
LMSE(e^+1)	8.12	**2.32**
NXC(e^-1)	9.6	**2.54**
MAS(e^-2)	2.12	**7.32**
MAMS(e^+6)	19.4	**19.14**
TED(e^2)	3.24	**10.89**

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

TCD(e^-1)	8.33	**15.01**
SME(e^-3)	2.21	**7.02**
SPE(e^-7)	2.53	**2.39**
GME(e^4)	12.3	**2.23**
GPE(e^2)	3.02	**8.32**
SSIM(e^-1)	8.02	**2.43**
VIF	81	**65**
RRED	174	**154**

VI. CONCLUSION

Image quality assessment for liveness detection technique is used to detect the fake biometrics. Due to Image quality measurements it is easy to find out real and fake users because fake identities always have some different features than original it always contain different color and luminance, artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. This paper 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., palm print, 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 access attempts; v)Also Real time implementation of Iris and face image application in biometric can be done in efficient way.

REFERENCES

[1] A. F. Sequeira, J. Murari, and J. S. Cardoso, "Iris liveness detection methods in mobile applications," in Proceedings of International Conference on Computer Vision Theory and Applications (VISAPP), 2014.
[2] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in Biometrics and Identity Management. Springer, 2008, pp. 181–190.
[3] Z. Wei, X. Qiu, Z. Sun, and T. Tan, "Counterfeit iris detection based on texture analysis," in ICPR 2008. 19th International Conference on Pattern Recognition. IEEE, 2008, pp. 1–4.
[4] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in 5th IAPR International Conference on Biometrics (ICB). IEEE, 2012, pp. 271– 276.
[5] J. Daugman, "Iris recognition and anti-spoofing countermeasures," in 7-th International Biometrics conference, 2004.
[6] X. He, Y. Lu, and P. Shi, "A new fake iris detection method," in Advances in Biometrics. Springer, 2009, pp. 1132–1139.
[7] J. Daugman, "Recognizing people by their iris patterns," Information Security Technical Report, vol. 3, no. 1, pp. 33–39, 1998.
[8] E. Lee, K. Park, and J. Kim, "Fake iris detection by using purkinje image," in Advances in Biometrics, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2005, vol. 3832, pp. 397–403.
[9] M. Une and Y. Tamura, "liveness detection techniques," IPSJ Magazine,vol. 47, no. 6, pp. 605–608, 2006.
[10] M. Kanematsu, H. Takano, and K. Nakamura, "Highly reliable liveness detection method for iris recognition," in SICE, 2007 Annual Conference. IEEE, 2007, pp. 361–364.
[11] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in Defense and Security. International Society for Optics and Photonics, 2004, pp. 296–303.
[12] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generation Computer Systems, vol. 28, no. 1, pp. 311–321,2012.