INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 4 ISSUE 1 – APRIL 2015 - ISSN: 2349 - 9303

An SVM based Statistical Image Quality Assessment for Fake Biometric Detection

S.Vigneshwaran[1]
PG Scholar
[1]Department of EEE
Kongu Engineering College,
Erode, India
vignesh11@yahoo.com

M.Suresh[2]
Assistant Professor
[2]Department of EEE
Kongu Engineering College,
Erode, India
onfostosuresh@gmail.com

Dr.R.Meenakumari[3]
Professor
[3]Department of EEE
Kongu Engineering College,
Erode, India
oremkay@gmail.com

Abstract

A biometric system is a computer based system and is used to identify the person on their behavioral and logical characteristics such as (for example fingerprint, face, iris, keystroke, signature, voice, etc.).A typical biometric system consists of feature extraction and matching patterns. But nowadays biometric systems are attacked by using fake biometric samples. This paper described the fingerprint biometric techniques and also introduce the attack on that system and by using Image Quality Assessment for Liveness Detection to know how to protect the system from fake biometrics and also how the multi biometric system is more secure than uni-biometric system. Support Vector Machine (SVM) classification technique is used for training and testing the fingerprint images. The testing onput fingerprint image is resulted as real and fake fingerprint image by quality score matching with the training based real and fake fingerprint samples.

Keywords: Image quality, biometrics security, support vector machine (SVM), liveness detection.

1 INTRODUCTION

On recent years the rising interest on the estimation of biometric systems security has led to the Creation of plentiful and very diverse initiatives focused on this major field of research. All these initiatives clearly highlight the importance given by all parties involved on the development of the systems security to bring this rapidly emerging technology onto practical use. Currently used for identity, confirmation and forensic purposes, biometric technologies can be broadly grouped onto four areas with several techniques on each:

1. Hands;
2. Heads and face;
3. Other physical characteristics; and
4. Behavioral characteristics.

The first three categories are physiological and are based on measurement of physical characteristics. Apart from on the case of a severe tragedy or operation, this biometrics is generally unaffected over time. Behavioral characteristics are more susceptible to change and can be

- *Author S.Vigneshwaran is currently pursuing a master's degree program on Applied electronics on Kongu Engineering College, PH-9842777847. E-mail:vigneshpsg91@gmail.com*
- *Co-Authors M.Suresh is currently working as Assistant Professor on Kongu Engineering College, India,E-mail:onfostosuresh@gmail.com and R.Meenakumari are working as a Professor on Kongu Engineering College,Ondia.Email:oremkay@gmail.com.*

Affected by age, illness, disease, tiredness and can be deliberately altered. These are therefore, less consistent as authenticators or identifiers. Along with the different threats analyze, the so-called direct or spoofing attack have forced the biometric community to study the vulnerabilities against this type of synthetically produced artifact or try to mimic the behavior of the genuine to unfairly access the biometric system. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate and also software-based techniques are on general less costly and less intrusive since their implementation is obvious to the user. The vast majority of present protection methods are based on the properties of a given trait which gives them a much reduced interoperability, since they may not be implemented on recognition systems based on other biometric modalities, or even on the same system with a dissimilar sensor.

2 LIVENESS DETECTION METHODSS

Liveness detection methods are generally classified onto two types (see Fig. 1): (I) Software-based techniques, on this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the characteristic itself);(II)Hardware-based techniques, which add some particular device to the sensor on order to detect Exacting properties of a living feature [1]. Liveness detection techniques use different physiological properties to differentiate between real and

Fake sample. Liveness detection methods represent a difficult engineering problem as they have to satisfy certain challenging requirements (I) user friendly, people should be averse to use it; (II) fast, results have to be generate on a very less time interval as the user cannot be asked to interact with the sensor for a long period of time; (III) low cost, a large use cannot be expected if the cost is very high. The two types of methods have certain advantages and disadvantages over the other and, on general, a combination of both would be the most advantageous protection approach to increase the security of biometric systems [4]. As a common comparison, hardware-based schemes generally present a higher fake detection rate, at the same time software-based techniques are on general less expensive (like no extra device is needed), and less intrusive since their implementation is clear to the user. Moreover, as they run directly on the acquired sample, software techniques may be embedded on the feature extractor module which makes them potentially accomplished of detecting other types of illegal break-on attempts not necessarily classified as spoofing attack [6]. For instance, software-based methods can protect the system against the addition of reconstructed or synthetic samples onto the communication channel between the sensor and the feature extractor [11].

3 IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The image quality assessment is used for the 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 methods against different biometric attack (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 on many attack attempts [1]. A novel parameterization using 25 general image quality measures. On 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 on the present work comprises 25 image quality measures for both reference and blond image quality has been successfully used on previous works for image manipulation detection and steganalysis on the forensic field. To a certain extent many spoofing attack, especially those which involve taking a picture of a facial image displayed on a 2D device (e.g., spoofing attack 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. Fingerprint 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].

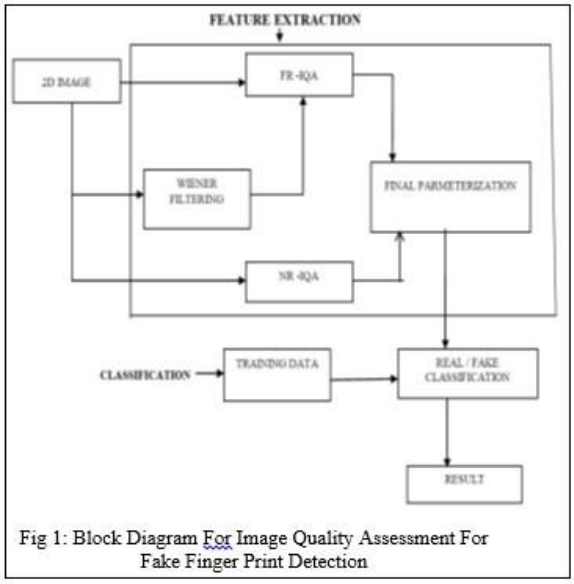


Fig 1: Block Diagram For Image Quality Assessment For Fake Finger Print Detection

3.1.2 Wiener Filtering

The input gray-scale image **I** (of size N × M) is filtered with wiener filtering on order to generate a smoothed version $\hat{\mathbf{I}}$ .The noise reduced by wiener filtered input fingerprint image is well capable for IQA technique. Because wiener filter are adaptive on nature. So wiener filtering technique is used for reducing noise on input fingerprint 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. On order to circumvent this limitation, the same strategy already successfully used for image manipulation detection on and for steganalysis is implemented here. The input gray-scale image **I** (of size N × M) filters with a wiener filter on order to generate a smoothed version $\hat{\mathbf{I}}$. Then, the quality between both images (**I** and $\hat{\mathbf{I}}$) 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].

3.1.4 No-Reference IQ Measures

Unlike the objective reference IQA methods, on 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, on 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 onto one of three trends [14].

4 FINGERPRONTS

Fingerprint analysis, also known on the Unites States as dactylographic, is the discipline of using fingerprints to recognize an individual. Fingerprint recognition is well recognized and a mature science. Palms and the soles of feet also have distinguishing epidermal patterns. Even identical twins will have contradictory fingerprints patterns. No two persons have been found to have the same prints. There are three basic categories of fingerprint: Visible prints, such as those made on oil, ink or blood. Latent prints which are unseen under normal viewing conditions. And plastic prints which are left on soft surfaces such as new paint. There are now over forty methods available for collecting prints including powders, use of chemicals such as iodine, digital imaging, dye strains, and fumes. Lasers are also used.

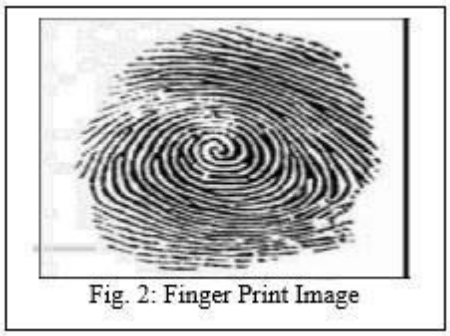


Fig. 2: Finger Print Image

5 FINGERPRONT RECOGNITION AND ATTACK ON SYSTEM

Every fingerprint of each person is considered to be unique, Even the twins also contain different fingerprint. Fingerprint recognition is the most accepted biometric recognition methods. Fingerprints have been used from a long time for identifying individuals [5]. Fingerprints consist of ridges and furrows on the surface of a fingertip.

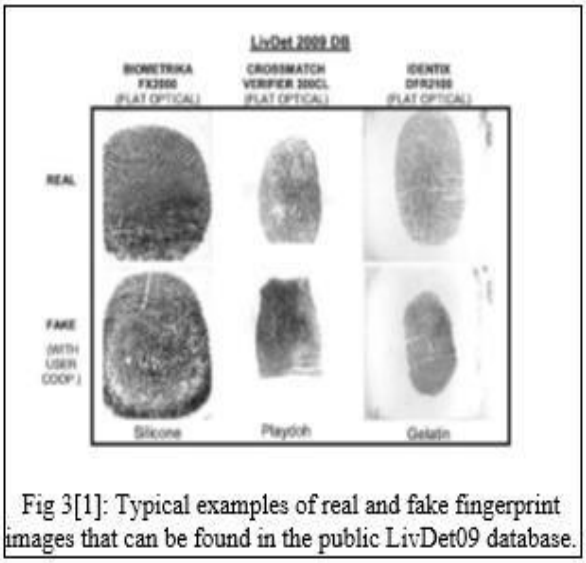


Fig 3[1]: Typical examples of real and fake fingerprint images that can be found in the public LivDet09 database.

6 SVM CLASSIFICATION

Support vector machine's (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 onto one category or the other and it is based on the non-probabilistic binary linear classifier [13].

6.1. Algorithm For SVM Classification

6.1.1 Training Algorithm

Step 1: Read the fingerprint Input training Images from the database.

Step 2: Fond 25 Image Quality Assessment Measures (No Reference & Full Reference) for the fingerprint training images.

Example: peak signal to noise ratio, average difference, maximum difference and other quality features.

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 training with two classes (Fake and Real).

6.1.2 Testing Algorithm

Step 1: Read the finger print Test Image from the database.

Step 2: Fond 25 Image Quality Measures (No Reference
& Full Reference) for the fingerprint test image.

Example: peak signal to noise ratio, average difference, maximum difference 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 finger print image.

7 THE SECURITY PROTECTION METHODS

The difficulty of fake biometric detection can be seen as a two-class categorization problem where an input biometric model has to be assigned to one of two classes: real or fake. The solution point of the methods is to fond a set of discriminate features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. The four selection criteria are:

1. Performance. Only widely used image quality approaches which have been consistently tested showing well performance for different applications have been considered.
2. Complementarity. On order to generate a system as general as possible on terms of attack detected and biometric modalities supported, we have given priority to IQMs based on complementary properties of the image
3. Complexity. On order to keep the simplicity of the methods, low complexity features have been preferred over those which require a high computational load.
4. Speed. This is, on general, closely related to the previous complexity. To assure a user-friendly non-intrusive application, users should not be kept waiting for a response from the recognition system. For this reason, big importance has been given to the feature extraction time, which has a very big impact on the overall speed of the fake detection algorithm.

8 RESULTS AND DISCUSSION

A Number of unique subjects on training and testing, as well as the average number of images. It should also be noted that Identic, Cross match and biometric were collected by multiple persons (Table I). [3]

Table I
Number of unique subjects in training and testing

Scanners	Training Subjects	Testing Subjects	Aver Images / subject
Identix	35	125	18.75
Crossmatch	63	191	15.75
Biometrika	13	37	40.0

8.1 GAUSSIAN FILTERED FINGERPRONT IMAGE

The onput gray-scale image **I** (of size N × M) is filtered with a low-pass Gaussian kernel (σ = 0.5 and size 3 × 3) on order to generate a smoothed version ˆ**I** . Then, the quality between both images (**I** and ˆ**I**) is computed according to the corresponding full-reference IQA metric.

Fig 4. Gaussian Filtered Finger Print Image

The PSNR value obtained for Gaussian filtered input fingerprint image is only 22.5231.The noise reduced by Gaussian filtered input fingerprint image is not capable for IQA technique So wiener filtering is also used for reducing noise on input fingerprint image.

8.2 WIENER FILTERED FINGER PRINT IMAGE

The onput gray-scale image **I** (of size N × M) is filtered with wiener filtering on order to generate a smoothed version ˆ**I** . Then, the quality between both images (**I** and ˆ**I**) is computed according to the corresponding full-reference IQA metric.

Fig 5.Wiener Filtered Finger Print Image

PSNR value obtained for wiener filtered onput fingerprint image is 26.9805.The noise reduced by wiener filtered onput fingerprint image is well capable for IQA technique. Because wiener filter are adaptive on nature. So wiener filtering technique is used for reducing noise on onput fingerprint image.

The following message box appears after finding 25 image quality assessment parameters for training the fingerprint image on SVM classifier.

The following message box appears after finding 25 image quality assessment parameters for testing the fingerprint image on SVM classifier.

8.3 TRAINING RESULTS FOR FINGERPRONT IMAGES:

8.3.1 Real Fingerpront Images

Table II. Training Results For Real Fingerpront Images

PARAMETER	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12
MSE(e^+2)	1.74	1.43	1.40	1.90	1.77	1.43	1.63	1.30	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	3.70	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)	1.10	1.13	1.14	1.16	1.12	1.10	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)	9.90	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	8.50	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	2.80	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

R1-R12-Real Image

8.3.2 FAKE FINGERPRONT IMAGES

Table III Training Results For Fake fingerprint Images

PARAMETER	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12
MSE(e^+2)	1.14	1.10	1.16	1.12	1.10	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	1.40	1.90	1.77	1.23	1.05	1.78	1.14	1.20	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	5.70	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	8.30	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	4.20
SPE(e^-7)	2.35	6.27	8.53	2.81	6.79	4.30	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	8.50	4.98	2.12	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	2.30	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

F1-F12-Fake

8.4 TESTING RESULTS FOR FINGERPRONT IMAGE

8.4.1 Real fingerprint Image

Table IV. Testing Results For Real fingerprint Image

PARAMETER	ONPUT IMAGE (REAL)
MSE(e^+2)	1.63
PSNR(e^+1)	2.57
SNR(e^+1)	2.21
SC(e^+0)	1.08
MD	75
AD(e^+1)	7.32
NAE(e^-2)	5.18
RAMD	7.5
LMSE(e^+1)	8.12
NXC(e^-1)	9.60
MAS(e^-2)	2.12
MAMS(e^+6)	19.4
TED(e^2)	3.24
TCD(e^-1)	8.33
SME(e^-3)	2.21
SPE(e^-7)	2.53
GME(e^4)	12.3
GPE(e^2)	3.02
SSIM(e^-1)	8.02
VIF	81
RRED	174
JQI(e^+1)	5.21
HLFI(e^-2)	2.74
BIQI(e^-1)	2.73
NIQE(e^+1)	9.43

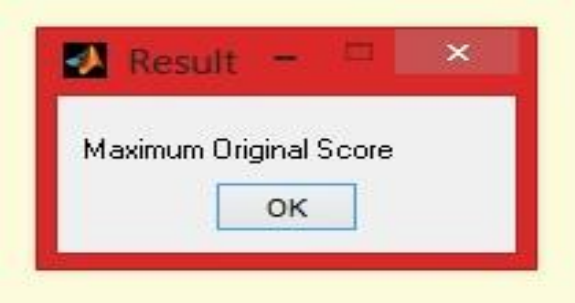
8.4.2 Fake fingerprint Image

Table V.Testing Results for Fake fingerprint Image

PARAMETER	ONPUT IMAGE(FAKE)
MSE(e^+2)	7.43
PSNR(e^+1)	5.21
SNR(e^+1)	6.06
SC(e^+0)	3.32
MD	84
AD(e^+1)	3.42
NAE(e^-2)	5.18
RAMD	8.4
LMSE(e^+1)	2.32
NXC(e^-1)	2.54
MAS(e^-2)	7.32
MAMS(e^+6)	19.14
TED(e^2)	10.89
TCD(e^-1)	15.01
SME(e^-3)	7.02
SPE(e^-7)	2.39
GME(e^4)	2.23
GPE(e^2)	8.32
SSIM(e^-1)	2.43
VIF	65
RRED	154
JQI(e^+1)	4.02
HLFI(e^-2)	5.93
BIQI(e^-1)	7.48
NIQE(e^+1)	2.10

8.5 Matlab Results

The following result shows that tested fingerprint image is Original.



The following result shows that tested fingerprint image is fake.

8.6 OVERALL RESULTS

Table VI Overall Results

FINGERPRINT IMAGE	FULL REFERENCE	NO REFERENCE
REAL	MSE,PSNR,SNR,NAE, SME,SC, NXC,GPE,SSIM,VIF, RRED	BIQI, NIQI
FAKE	MD,AD,RAMD,LMSE, MAS,MAMS, TED,TCD,SPE,GME	JQI,HLFI

The most remarkable finding is that the whole group of25 quality measures is consistently selected as the best performing feature set for all the considered scenarios and traits, showing the high complementarity of the proposed metrics for the biometric security task studied on the work.

9. 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 on 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., palmpront, hand geometry, vein); III) inclusion of temporal information for those cases on 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 on biometric can be done on efficient way.

10. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of this paper. We extend our sincere thanks to all the faculty and staff members of Electrical and Electronics Engineering department of the Kongu Engineering College for their valuable suggestions and help throughout our paper work. We also thank our friends and family members for their support towards the completion of the project work.

REFERENCES

[1] Javier Galbally, Sebastian Marce, and Julian Fierrezvol, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, fingerprint, and Face Recognition.",IEEE transactions on image processing vol.23, no. 2, February 2014.

[2] Rohit Kumar Csvtu bhilai Sscet bhilai India, Vishal Moyal Csvtu bhilai scet bhilai, "Visual Image Quality Assessment Technique using FSIM", Vol.2– Issue 3, 250 - 254, 2013.

[3] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., "First international fingerprint liveness detection competition— LivDet," on Proc. IAPR ICIAP,Spronger LNCS-5716. 2009, pp. 12–23,2009..

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

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection methods based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.

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

[7]Anil K. Jaon, Michigan State. Pradnya M. Shende "Biometrics Technology for Human Recognition", International Journal of Computer Science Engineering and Technology (IJCSET) Vol 4, Issue 4,129-132, April 2014.

[8] M. M. Chaka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,et al., "Competition on counter measures to 2D facial spoofing attack," on Proc. IEEE IJCB, pp. 1–6, Oct. 2011.

[9] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martonez-Diaz, "Evaluation of direct attack to fingerprint verification systems," J. Telecomm. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

[10] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attack," on Proc. IEEE 5th Ont. Conf. BTAS, pp. 283–288, Sep. 2012.

[11] D. Maltoni, D. Maio, A. Jaon, and S. Prabhakar, "Handbook of fingerprint Recognition". New York, NY, USA: Spronger-Verlag,pp, 2009.

[12] R. Cappelli, D. Maio, A. Lumoni, and D.Maltoni,"Fingerpront image reconstruction from standard templates," IEEE Trans. Pattern Anal.Mach. Ontell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[13] J. F. Aguilar, J. O. Garcia, J. G. Rodriguez and J. Bigun, "Discriminative multimodal biometric authentication based on quality measures", *Pattern Recognition* **38** (5) 777–779, 2005.

[14] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No reference perceptual quality assessment of JPEG compressed images," on *Proc. IEEE ICIP*, pp. 477–480, Sep. 2002**.**

[15] M. G. Martoni, C. T. Hewage, and B. Villaroni, "Image quality assessment based on edge preservation," Signal Process., Image Commun., vol. 27, no. 8, pp. 875–882, 2012.

[16] N. B. Nill and B. Bouzas, "Objective image quality measure derived from digital image power spectra," Opt. Eng., vol. 31, no. 4, pp. 813–825, 1992.

[17] A. Liu, W. Lon, and M. Narwaria, "Image quality assessment based on gradient similarity," IEEE Trans. Image Process., vol. 21, no. 4, pp. 1500–1511, Apr. 2012.

[18] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[19] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," on Proc. IEEE ICIP, Sep. 2002, pp. 477–480.

[20] X. Zhu and P. Milanfar, "A no-reference sharpness metric sensitive to blur and noise," on Proc. Ont. Workshop Qual. Multimedia Exper., 2009, pp. 64–69.

[21] A. K. Moorthy and A. C. Bovik, "A two-step framework for constructing blond image quality ondices," IEEE Signal Process. Lett., vol. 17, no. 5, pp. 513–516, May 2010.

[22] A. Mittal, R. Soundararajan, and A. C. Bovik, "Makong a 'completely blond' image quality analyzer," IEEE Signal Process. Lett., vol. 20, no. 3, pp. 209–212, Mar. 2013.