

# Multi-biometric Fake Detection System using Image Quality based Liveness Detection

Asmita A. Patil, Prof. S.A.Dhole

Department of ECE, BV's College of Engineering for Women, Pune , Savitribai Phule Pune University, Pune, India

**Abstract**— Biometric systems mostly popular in all over the world because of its user friendly and credible nature in security. In spite of this advantages, many attacks that done through synthetic , self manufactured, fake, reconstructed samples affected on the performance and accuracy of biometric system which becomes major problem in biometrics. Hence, new effective measures have to be taken to protect the biometric systems. In this paper, we propose novel software based multi-biometric fake detection system to detect various types of attacks. The main moto of this system is to enhance security level of biometric recognition systems through Image Quality Assessment (IQA) which is one of the liveness detection method. 25 image quality measures calculated from test image which used to classify between real and fake trait using Linear Discriminative Analysis(LDA) classifier. The experimental results is done on the database of 2D face and fingerprint modalities, shows the proposed system is ease in implementation in real time application as complexities is very less because of one input image. Also this system is fast, user-friendly, non-intrusive which is more competitive with any other state of the art approaches, classifies between real and fake traits.

**Keyword**—Biometrics, Image quality Assessment (IQA), liveness detection method, linear discriminative analysis(LDA) classifier.

## I. INTRODUCTION

Security became basic need of human kind to distinguish between known and unknown persons as population increases day by day which makes difficult to recognize authorized person. As we talk about security, first name comes in mind is “Biometrics” as biometrics plays very vital role in last few decades in the field of security and many creations has been developed to enhance the performance and security of biometric systems[1][2]. In spite of these popularity of biometric systems, main problem facing by these systems is spoofing attacks.

These attacks make biometric systems more vulnerable and the performance of systems decreases automatically. These attacks are in the form of synthetic , self manufactured , reconstructed biometric samples(e.g.face, fingerprint, iris, vein, hand geometry) while other attacks are in the form of mimicry of behavior of genuine

user(e.g. signature, gait) whose main aim to fraudulently access the biometric system.

Hence, there are many researches have been taking place in various organization of this specific area which focus on this problem. All these spoofing attacks are performed in analog domain so any digital protection techniques such as encryption, watermarking, digital signature show less effectiveness on it.

After previous works and other analogue studies, it is cleared that there is need to propose and develop a specific method which can protect biometric systems against these attacks [3][4]. A main aim of researchers are to design a proper method that make biometric system to distinguish between real and fake samples which enhance the security levels of the systems.

There are various anti-spoofing techniques (hardware or software) available but researchers are more interested in liveness detection, has ability to discriminate the different physiological features which use to distinguish between real and fake traits. This liveness assessment techniques satisfy certain demanding requirements which represents challenging engineering problems: 1) user-friendly; 2)non-invasive, means techniques should not provide harm to users or not comes contact with use; 3)fast, results have to produce with very reduced interval; 4)low cost, overall cost should be affordable to user so that the system can publically used; 5)performance, along all these requirement, performance should check so that false rejection should not degrade[5]

Mostly, these liveness detection methods have divided into two groups: 1) hardware based techniques, where some specific devices detect fake samples by using the particular properties of living traits and 2) software based techniques, where, classification between real and fake traits is done by using features extracted from the samples which acquired with standard sensors[5]. Individually, these two techniques have some drawbacks. If we combine them together, then security level of biometric systems get increases. But, software based technique is more reliable as it is less expensive, less intrusive, easily embedded in feature extractor module so that it potentially capable to detect illegal attempt which don't come under in spoofing attacks. Also, software based technique can resist the fake, self manufactured, synthetic

sample to enter into communication channel between the feature extractor and the sensors [5].

In software based liveness detection method, many work has been done in the field of spoof detection and they are succeed to reduce spoofing attacks, But one challengeable work has to be done i.e. removal of direct attacks in this field. Most presented anti-spoofing techniques suffered with lack of generality [5], also their performance is good while detecting particular spoofs, but efficiency drops drastically when it comes in contact with synthetic generated traits. Error rates goes vary continuously when other database introduced. To remove all these drawbacks, new software based technique proposed in liveness detection method is Image Quality Assessment(IQA). IQA works on the principle that fake image acquired in the spoofing attacks will have different quality than the real image taken from sensors[5]. The proposed system is described in following section: Previous work had to be done given in section II. Proposed working mechanism is given in section III. Experimental results discussed in section IV and conclusion and future scope given in section V.

## II. RELATED WORK

Liveness detection method in biometric systems become most popular because of its solutions provided in engineering problems as mentioned above. In this technique, many work has been done in particular forensic area for image manipulation system and steganalysis [7]. As software based liveness detection system is more generous than hardware based liveness detection system, many liveness detection method have been proposed which based on software. One of these methods for fingerprint is skin perspiration pattern where periodicity of sweat and sweat diffusion pattern is considered to detect fake fingerprints by using ridge signal algorithm. To improve the performance of this system ,wavelet transform is introduced which gave detection rate up to 90% .In this work ,many new techniques have been added to remove the noises in samples[10].

Work proposed by A. Antonelli et.al[11] is mostly depend on the three fingerprint regions: 1) inner region where pressure of finger has not allow any elastic deformation, 2) external region where the skin follows finger's movement as pressure is light, 3) intermediate region which used for combine inner and external region smoothly using skin stretching and compression. Same detection system has proposed on corporal odour [15].

In 2D face based liveness detection system, different techniques have been used. Liveness detection system based on frequency and texture analysis is presented by Kim.et.al.[12] to distinguish between real and synthetic face samples. Another system is developed by

J.Maatta.et.al [8]. which based on Local Binary Pattern(LBP) to analyze the textures of given face samples. Another face based liveness detection system is proposed by Lin Sun et.al.[13] based on blinking eyes mechanism.

These all works have some disadvantages like complexities and lack of generality which is removed in Image Quality Assessment based liveness detection system whose main aim is to classify real and fake samples using LDA classifier with the help of image quality measures calculated on the basis of image quality of an images.

## III. PROPOSED SECURITY PROTECTION METHOD

The proposed IQA based liveness detection system is based on the "quality-difference" hypothesis where Image Quality(IQ) measures are extracted doing comparison of distorted image with reference images. Fig 1 is the block diagram of proposed detection system where input image (Face or fingerprint) is filtered to remove noises using Low pass Gaussian filter (having sigma  $\sigma = 0.5$  and Gaussian kernel size  $3 \times 3$ ) by adding blur effect. Filtered image is compared with reference image to calculate Full Reference (FR) IQA and No Reference (NR) IQA is determined predicting the information about reference image. This IQ measures is extracted using simple classifier i.e. Linear Discriminant Analysis (LDA) classifier.

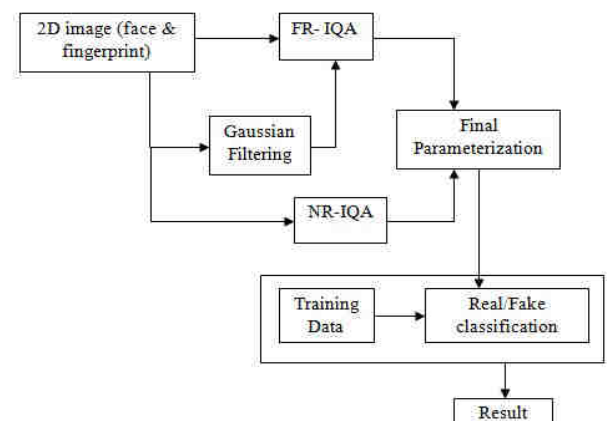


Fig.1: General Block Diagram of Proposed Security Protection Method based on Image Quality Assessment (IQA).

The classification of tested image is done based on this classifier comparing it with training database. Final result is shown on GUI is whether the sample image real or fake.

Here, 25 FR IQ measures and 4 NR IQ measures are determined. Full reference Image quality measures are determined based on the pixel difference, correlation,

edge based information, gradient based information and spectral magnitude and phase of image and so on. While No Reference (NR) IQ measures are determined on the basis of knowledge of reference image. The list of all these 21 IQ measures is given in table 1 with all descriptions whereas NR IQ measures' information are provided in references which given in table.. I is the in the case of 2D face. Because of all these properties of this system, the computation load gets reduced. Classification of image i.e. real or fake is easily done as feature vector of test image is compared with training

reference image and  $\hat{I}$  is filtered image by Gaussian filter [5].

This system keeps simplicity and generality by using only single input image (face or fingerprint image). As this system does feature extraction based on quality of image, it removes the preprocessing steps i.e. fingerprint segmentation in the case of fingerprint and face extraction feature vectors, using simple classifier i.e. LDA classifier. This implementation of our experiment is done on matlab version R2014a with the help of LDA classifier.

Table 1: Table shows the list of all Full Reference IQ measures with their formulas and descriptions where I denote for original image which take as reference and  $\hat{I}$  is filtered image via Gaussian filter.

Sr. No.	Name of IQ measures (Acronym)	Type	Descriptions
1	Mean Square Error(MSE)	FR	$MSE(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (I_{ij} - \hat{I}_{ij})^2$
2	Peak Signal to Noise Ratio(PSNR)	FR	$PSNR(I, \hat{I}) = 10 \log \left( \frac{\max(I^2)}{MSE(I, \hat{I})} \right)$
3.	Signal to Noise Ratio(SNR)	FR	$SNR(I, \hat{I}) = 10 \log \left( \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{ij})^2}{N * M * MSE(I, \hat{I})} \right)$
4.	Structural Content(SC)	FR	$SC(I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{ij})^2}{\sum_{i=1}^N \sum_{j=1}^M (\hat{I}_{ij})^2}$
5.	Maximum Difference(MD)	FR	$MD(I, \hat{I}) = \max  I_{ij} - \hat{I}_{ij} $
6.	Average Difference(AD)	FR	$AD(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (I_{ij} - \hat{I}_{ij})$
7.	Normalized Absolute Error(NAE)	FR	$NAE(I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M  I_{ij} - \hat{I}_{ij} }{\sum_{i=1}^N \sum_{j=1}^M  I_{ij} }$
8.	R-average MD (RAMD)	FR	$RAMD(I, \hat{I}, R) = \frac{1}{R} \sum_{r=1}^R \max_r  I_{ij} - \hat{I}_{ij} $
9.	Laplacian MSE(LMSE)	FR	$LMSE(I, \hat{I}) = \frac{\sum_{i=1}^{N-1} \sum_{j=1}^{M-1} (h(I_{ij}) - h(\hat{I}_{ij}))^2}{\sum_{i=1}^{N-1} \sum_{j=1}^{M-1} h(I_{ij})^2}$
10.	Normalised Cross-Correlation(NXC)	FR	$NXC(I, \hat{I}) = \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{ij} * \hat{I}_{ij})}{\sum_{i=1}^N \sum_{j=1}^M (I_{ij})^2}$
11.	Mean Angle Similarity(MAS)	FR	$MAS(I, \hat{I}) = 1 - \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (\alpha_{ij})$
12.	Mean Angle Magnitude Similarity (MAMS)	FR	$MAMS(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M \left( 1 - [1 - \alpha_{ij}] \left[ 1 - \frac{\ I_{ij} - \hat{I}_{ij}\ }{255} \right] \right)$
13.	Total Edge Difference(TED)	FR	$TED(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M  E_{ij} - \hat{E}_{ij} $
14.	Total Corner Difference(TCD)	FR	$TCD(I, \hat{I}) = \frac{ N_{cr} - \hat{N}_{cr} }{\max(N_{cr}, \hat{N}_{cr})}$

15.	Spectral Magnitude Error(SME)	FR	$SME(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M ( F_{i,j}  -  \hat{F}_{i,j} )^2$
16.	Spectral Phase Error(SPE)	FR	$SPE(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M  \arg(F_{i,j}) - \arg(\hat{F}_{i,j}) ^2$
17.	Gradient Magnitude Error (GME)	FR	$GME(\hat{F}_{i,j}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M ( G_{i,j}  -  \hat{G}_{i,j} )^2$
18.	Gradient Phase Error (GPE)	FR	$GPE(I, \hat{I}) = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M  \arg(G_{i,j}) - \arg(\hat{G}_{i,j}) ^2$
19.	Structural Similarity Index (SSIM)	FR	Description is given in reference [21][22]
20.	Visual Information Fidelity (VIF)	FR	Description is given in reference[23][22]
21.	Reduced Ref. Entropic Difference (RRED)	FR	Description is given in reference[24][22]
22.	JPEG Quality Index (JQI)	NR	Description is given in reference[25][22]
23.	High-Low Frequency Index (HLFI)	NR	Description is given in reference[26][22]
24.	Blind Image Quality Index (BIQI)	NR	Description is given in reference[27][22]
25.	Naturalness Image quality Index (NIQE)	NR	Description is given in reference[28][22]

#### IV. RESULTS AND DISCUSSION

As name indicates, proposed system is liveness detection system based on emerging new technique Image Quality Assessment (IQA), all image quality measures determined with the support of reference images provided in database. As it is multi-biometric System, two modalities i.e.1)Fingerprint and 2) face are taken which provides to presented system which detects the spoofing attacks as well as Fraudulent attacks on them. Evaluation is taken place for each modality with specific manner.

##### A. FINGERPRINT

As mentioned, fingerprint is one of the modality used in this proposed system, the database of real and fake fingerprint is taken from 23 persons where fake fingerprints is synthesized using material fevicol which is scanned with fingerprint sensor r305.

All IQ measures are determined on the training database whose training vector is created using matlab which compared with feature vector of test samples and depending upon it, the result shown in message box that image is real or fake.



(a)



(b)

Fig.2: (a) Fingerprint sensor r305 photo, (b) Synthetic fingerprint is generated using material Fevicol.



(a)



(b)

Fig.3: (a)Original fingerprint image, (b)Fake Fingerprint image of same person.

A. FACE

Other than fingerprint, 2D face is taken as an input in this system where reference image is captured using high definition camera while fake image is captured via USB camera module with the help of photo print of same persons.

Some of IQ measures are listed in table 2 whose values for real and fake images are given.

Ranges of values give the difference between real and fake images which lies in same range , difficult to separate out, hence LDA classifier is used to classify. All IQ measures are plotted via graph where no. of real and fake images is on X axis and ranges of feature values is on plotted on Y axis. Fig 4 and 5 shows the graph of one of IQ measures i.e. MSE for fingerprint and face.

The accuracy is calculated by computing FGR,FRR and HTER where False Genuine rate(FGR) is no. of samples which are fake but classified as real.

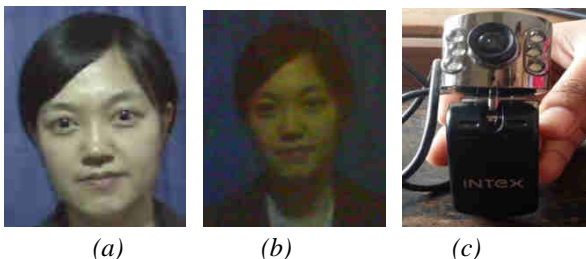


Fig.4: (a) real image taken as reference image,(b) photoprint used in spoofing attacks, (c) intex camera module used to capture photos.

Table 2: shows the some of IQ measures that values are calculated for real and fake input samples from feature vector

IQ measures	Fingerprint		2D face	
	Real	Fake	Real	Fake
MSE	32.72-42.61	22.88-43.83	1-10	1-3.5
PSNR	31.17-34.25	31.74-34.43	38-46	44-46
SC	1.0083-1.0297	1.0090-0.0177	1.0037-1.0066	1.0048-1.0066
AD	0.24-0.3726	0.2436-0.33	0.0982-0.1691	0.082-0.1199
MD	61-64	61-63	17-57	26-30

False Fake Rate (FRR) is a no. of real sample which give result as a fake and HTER is Half Total Error Rate which computed as  $HTER = (FGR + FFR) / 2$ . In the case of fingerprint modality, the FFR, FGR and HTER are shows in table 3:

Where, the accuracy for the fingerprint database is:

$$Accuracy = \frac{(74 + 66)}{166}$$

Accuracy = 84.33%

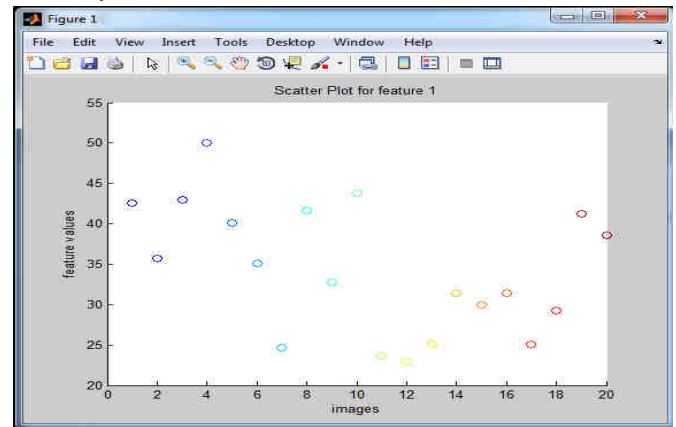


Fig.4: graph plot of MSE for 20 real and fake fingerprint images

Table 3: Table shows the values of FGR, FFR and HTER for fingerprint database.

No. of finger image	(FGR)	(FFR)	(HTER)
166	17	9	13

Similarly, if we provide face image as an input to the proposed method, FER is zero as no fake samples are classified as real.FFR is 20 in this case. Hence, HTER is given in table 4 below:

Table 4: Table shows the values of FGR,FFR and HTER for face database.

No of Face image	FGR	FFR	HTER
140	0	20	10

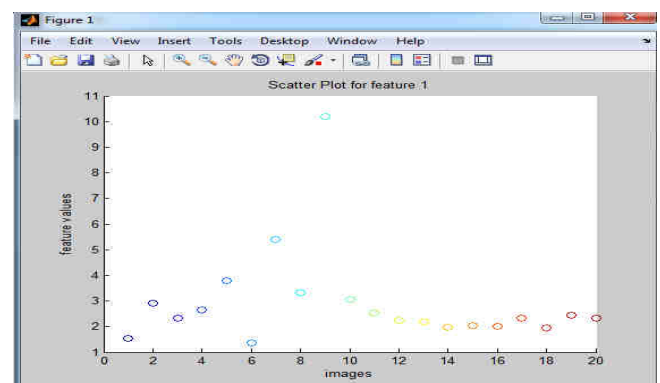


Fig. 5: Graph plot of MSE for 20 real and fake face images

The accuracy is calculated on testing database where both real and fake database is kept. The classification is done on the basis of testing vector of test image, training features and training labels where 1 is denoted for real and 2 for fake classification. The message box is displayed on window to show the result is real or fake.

The result of this proposed system is varies as the modalities keep changing. The result of both modalities are above 80%.If we compare both the results then fingerprint based security system is more vulnerable to different types of attacks as it is very difficult to find out the real one and fake one. In case of face based security method, it is not that tough to recognize real and fake samples. The accuracy and performance of the proposed method is varying by changing the types of input. This system can be used for any type of biometric Modalities. Hence this system is more advantageous than previous work.

Table 5: Table shows the performance of the system after executing the operation result on real and fake samples and execution time is denoted.

Face	Fingerprint	Ground Truth	Output	Accuracy result	Execution Time(s)
R1	R1	Real	Real	1	8
R2	R2	Real	Real	1	8.1
R3	R3	Real	Real	1	8
F1	F1	Fake	Fake	1	8.24
F2	F2	Fake	Fake	1	8.29
F3	F3	Fake	Fake	1	7.54

#### IV. CONCLUSION

The main motivation given to propose this system is vulnerability of available biometric systems to various spoofing and direct attacks that driven by intruder to access the system fraudulently. Here, the proposed liveness detection system based on “image quality hypothesis which works on the image quality of input image and extracted the 25 IQ measures that helps to classify between real and fake samples. From the results obtained by proposed system, the system is very effective in following manner:1)the Accuracy is above 95% which is most important achievement in this biometric system, 2) Error rate is very less so that the performance is constant, 3)Different types of attacks can be stopped using this system hence we can say that it fallows “multi-attack” property 4)Various type of modalities can be applied as an input i.e.it is “Multi-biometric” in nature .5) cost is very less as it is software based method ,6) It is user-friendly and main advantages are 7) It is more generous to user and 8) very less complex in nature.

Also, after comparing the result based on the input modalities to proposed system, conclusion derived is that the face biometric modality has more accuracy and performance than fingerprint modalities as more spoofing can be done in the case of fingerprint and it is difficult to classify.

Future scope of this system is that we can give video as an input so that the any fraudulent activity happened can be stopped. Also this work can be applied new type of biometric modalities like finger vein, hand geometry and many more.

#### REFERENCES

- [1] S. Prabhakar, S. Pankanti, and A. K. Jain, Biometric recognition:Security and privacy concerns ,IEEE Security Privacy, vol. 1, no. 2,pp. 3342, Mar./Apr. 2003.
- [2] K. A. Nixon, V. Aimale, and R. K. Rowe, Spoof detection schemes,Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008,pp. 403423.
- [3] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu,et al., First international fingerprint liveness detection competition LivDet 2009, in Press. IAPR ICIAAP, Springer LNCS-5716. 2009, pp. 1223.
- [4] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,et al., Competition on countermeasures to 2D facial spoofing attacks, in Press. IEEE IJCB, Oct. 2011, pp. 16.
- [5] J. Galbally, S. Marcel, and J. Fierrez, 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
- [6] G. Pan, Z.Wu, and L. Sun. Liveness detection for face recognition. In K. Delac, M. Grgic, and M. S. Bartlett, editors, Recent Advances in Face Recognition, page Chapter 9. INTECH,2008.
- [7] R. Derakhshani, S. Schuckers, L. Hornak, L. OGorman, "Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners", Pattern Recognition 36 (2003) 383396.
- [8] J. Maatta, A. Hadid,and M. Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis", IEEE Transaction of Image processing, 2011
- [9] Mrs. Dhole S.A. Dr. Prof. Patil V.H, Face Recognition Using CurveletTransform, International Journal of Applied Engineering Research, Volume 10, No. 14 (2015), pp.33949-33954, August 2015(Impact factor- 0.166),Scopus indexing
- [10] B. DeCann, B. Tan, S. Schuckers, A novel region based liveness detection approach for fingerprint scanners, in press. IAPR/IEEE Int. Conf. on Biometrics, in: LNCS, vol. 5558, Springer, 2009, pp. 627636.
- [11] A. Antonelli, R. Capelli, D. Maio, D. Maltoni, "Fake finger detection by skin distortion analysis", IEEE

- Transactions on Information Forensics and Security 1 (2006) 360373.
- [12] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, "Face liveness detection based on texture and frequency analyses", 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67- 72, March 2012
- [13] H. K. Jee, S. U. Jung, and J. H. Yoo, "Liveness detection for embedded face recognition system, International Journal of Biological and Medical Sciences", vol. 1(4), pp. 235-238, 2006.
- [14] Lin Sun, Gang Pan, Zhaohui Wu, Shihong Lao, "Blinking-Based Live Face Detection Using Conditional Random Fields", ICB 2007, Seoul, Korea, International Conference, on pages 252-260, August 27-29, 2007.
- [15] D. Baldiserra, A. Franco, D. Maio, D. Maltoni, "Fake fingerprint detection by odor analysis", IAPR Int. Conf. on Biometrics (ICB), in: LNCS, vol. 3832, Springer, 2006, pp. 265272.
- [16] Z. Wang, H. R. Sheikh, and A. C. Bovik, No-reference perceptual quality assessment of JPEG compressed images, IEEE ICIP, Sep. 2002, pp. 477480.
- [17] A. K. Moorthy and A. C. Bovik, A two-step framework for constructing blind image quality indices, IEEE Signal Process. Lett., vol. 17, no. 5, pp. 513516, May 2010.
- [18] S.F. Bahgat, S. Ghoniemy, M. Alotaibi, "Proposed multi-modal palm veins-face biometric Authentication", International Journal of Advanced Computer Science and application (IJACSA), Vol. 4, No. 6., 2013
- [19] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
- [20] 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.
- [21] (2012). *LIVE* [Online]. Available: <http://live.ece.utexas.edu/research/Quality/index.htm>
- [22] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Trans. Image Process.*, vol. 15, no. 2, pp. 430–444, Feb. 2006.
- [23] R. Soundararajan and A. C. Bovik, "RRED indices: Reduced reference entropic differencing for image quality assessment," *IEEE Trans. Image Process.*, vol. 21, no. 2, pp. 517–526, Feb. 2012.
- [24] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," in *Proc. IEEE ICIP*, Sep. 2002, pp. 477–480.
- [25] X. Zhu, P. Milanfar, "A no-reference sharpness metric sensitive to blur and noise," in *Proc. Int. Workshop Qual. Multimedia Exper.*, 2009, pp. 64–69.
- [26] A. K. Moorthy and A. C. Bovik, "A two-step framework for constructing blind image quality indices," *IEEE Signal Process. Lett.*, vol. 17, no. 5, pp. 513–516, May 2010.
- [27] A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a 'completely blind' image quality analyzer," *IEEE Signal Process. Lett.*, vol. 20, no. 3, pp. 209–212, Mar. 2013.