International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 01 | Apr-2015 www.irjet.net p-ISSN: 2395-0072

GAUSSIAN FILTER BASED BIOMETRIC SYSTEM SECURITY ENHANCEMENT

M.Selvi[1], Mr. T. Manickam[2], Dr.C.N.Marimuthu[3]

[1]PG student, Applied Electronics,Nandha Engineering College, Tamil Nadu, India
[2]Associate Professor / ECE, Nandha Engineering College, Tamil Nadu, India
[3]Dean / ECE, Nandha Engineering College, Tamil Nadu, India

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

The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. Multi-biometric and Multi-attack protection method which targets to overcome part of these limitations through the use of Image Quality Assessment (IQA).

Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake, non-intrusive; user-friendly (transparent to the user), cheap and easy to embed in already functional systems and no hardware is required).

Key Words: *Gaussian filter, Fake detection, Biometric security, Image quality assessment*

1. INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research. Among the different threats analyzed, the direct or spoofingattacks have motivated the biometriccommunity to study thevulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As these types of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective.

The above mentioned works and other analogue studies, have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems. Besides other anti-spoofing approaches such as the use of multi-biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detectiontechniques, which use different physiological properties to distinguish between real and fake traits.

Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements

(i) Non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user
(ii) User friendly, people should not be reluctant to use it
(iii) Fast results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time

(iv) Low cost, a wide use cannot be expected if the cost is excessively high
(v) Performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

2. LITERATURE SURVEY

Anna Geomi George and A. KethsyPrabavathy (2013) proposed a method Image quality assessment means estimating the quality of an image and it is used for many image processing applications. Image quality can be measured in two ways, subjective and objective method. Objective method is more preferable than subjective because most of the time the original image is not available for the comparison and it is not that much expensive like the subjective method. These methods are used to predict the visual quality by comparing a distorted image against a reference image. In this paper we are comparing the different approaches of image quality assessment.

Soweon Yoon, Jianjiang Feng and Anil K. Jain (2012) Proposed a method wide spread deploymentof Automated Fingerprint Identification Systems (AFIS) in law enforcement and border control applications has heightened the need for ensuring that these systems are not compromised. While several issues related to fingerprint system security have been investigated, including the use of fake fingerprints for masquerading identity, the problem of fingerprint alteration or obfuscation has received very little attention. Fingerprint obfuscation refers to the deliberate alteration of the fingerprint pattern by an individual for the purpose of masking his identity.
Several cases of fingerprint obfuscation have been reported in the press. Fingerprint image quality assessment software (e.g., NFIQ) cannot always detect altered fingerprints since the implicit image quality due to alteration may not change significantly. The main contributions of this paper are: 1) compiling case studies of incidents where individuals were found to have altered their fingerprints for circumventing AFIS, 2) investigating the impact of fingerprint alteration on the accuracy of a commercial fingerprint matcher, 3) classifying the alterations into three major categories and suggesting possible countermeasures, 4) developing a technique to automatically detect altered fingerprints based on analyzing orientation field and minutiae distribution, and 5) evaluating the proposed technique and the NFIQ algorithm on a large database of altered fingerprints provided by a law enforcement agency. Experimental results show the feasibility of the proposed approach in detecting altered fingerprints and highlight the need to further pursue this problem.
Javier Galbally, Fernando Alonso-Fernandez and Julian Fierrez (2012) Proposed a method new software-based liveness detection approach using a novel fingerprint parameterization based on quality related features is proposed. The system is tested on a highly challenging database comprising over 10,500 real and fake images acquired with five sensors of different technologies and covering a wide range of direct attack scenarios in terms of materials and procedures followed to generate the gummy fingers. The proposed solution proves to be robust to the multi-scenario dataset, and presents an overall rate of 90% correctly classified samples. Furthermore, the liveness detection method presented has the added advantage over previously studied techniques of needing just one image from a finger to decide whether it is real or fake. This last characteristic provides the method with very valuable features as it makes it less intrusive, more user friendly, faster and reduces its implementation costs.

F.Alonso-Fernandez and M.Martinez-Diaz (2011**)** Proposed a method vulnerabilities of fingerprint-based recognition systems to direct attacks with and without the cooperation of the user are studied. Two different systems, one minutiae-based and one ridge feature-based, are evaluated on a database of real and fake fingerprints. Based on the fingerprint images quality and on the results achieved on different operational scenarios, we obtain a number of statistically significant observations regarding the robustness of the systems.
SiweiLyu and Hany Farid (2006) Proposed a techniques for information hiding (steganography) are becoming increasingly more sophisticated and widespread.With high-resolution digital images as carriers, detecting hidden messages is also becoming considerably more difficult.We describe a universal approach to stag analysis for detecting the presence of hidden messages embedded within digital images. We show that, within multi-scale, multi-orientation image decompositions (e.g., wavelets), first- and higher-order magnitude and phase statistics are relatively consistent across a broad range of images, but are disturbed by the presence of embedded hidden messages.We show the efficacy of our approach on a large collection of images, and on eight different steganographic embedding algorithms**.**

3. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the assumption that: "It is expected that a fakeimage captured in an attack attempt will have different qualitythan a real sample acquired in the normal operation scenariofor which the sensor was designed." Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance.

For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images. Following this "quality-difference" hypothesis, in the present research work we explore the potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing). As the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack, they may be computed on any image. This gives the proposed method a new multi-biometric dimension which is not found in previously described protection schemes.

4.SUPPORT VECTOR MACHINES

Support Vector Machines (SVM) are supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilisticbinarylinear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on.

In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.SVMs belong to a family of generalized linear classifiers and can be interpreted as an extension of the perception. They can also be considered a special case of Tikhonov regularization. A special property is that they simultaneously minimize the empirical classification error and maximize the geometric margin; hence they are also known as maximum margin classifiers.

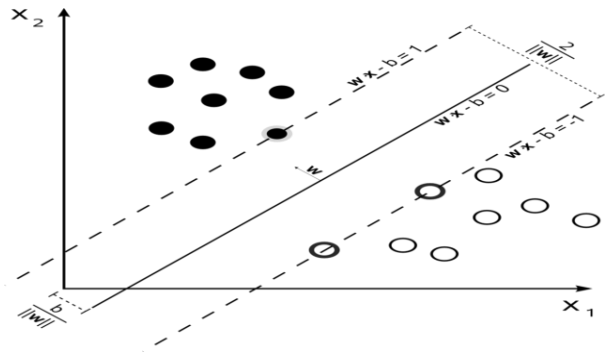

Fig -1: Maximum-margin hyper plane and margins for an SVM

Maximum-margin hyper plane and margins for an SVM trained with samples from two classes is shown in Fig -1. Samples on the margin are called the support vectors.

5. ALGORITHM FOR SVM

Training:

Step 1: Read Input Image.

Step 2: Find 25 Image Quality Measures (No Reference & Full Reference).

example: peak signal to noise ratio,average difference,maximum difference etc.

Step 3: Combine all Quality Measure as a feature.

Step 4: Create Target for SVM Training.

Step 5: Make SVM training with two classes (Fake and Real).

Testing:

Step 1: Read Test Image.

Step 2: Find 25 Image Quality Measures (No Reference & Full Reference),

example : peak signal to noise ratio, average difference ,maximum difference etc.

Step 3: Combine all Quality Measure as a feature.

Step 4: Feature compared with trained Feature using SVM.

Step 5: Final result given test image is fake or real.

5. RESULTS AND DISCUSSION

5.1 Input image

The input images used in this project is taken from a LIVDET 2009 Database. For this proposed method, two input images or required (real and fake).Input images are shown in Figure 2 and 3.

5.1.1. Real images

Fig – 2: Real finger print images

5.1.2. Fake images

Fig –3: Fake finger print images

5.2.GAUSSIAN FILTERED RESULT

5.4.TRAINING RESULTS FOR DATABASE IMAGES:

5.4.1.Real images

Traning results for real image is shown in Table 1.

Table –1: Training results for real image

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

The following Figures 4 and 5 shows the Gaussian Filtered Result and the Weiner Filtered Results

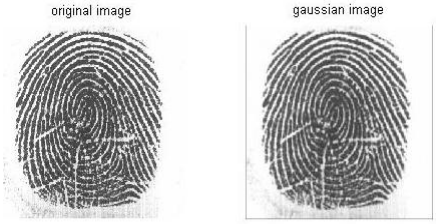

Fig –4: Gaussian filter output

5.3.WEINER FILTERED RESULT

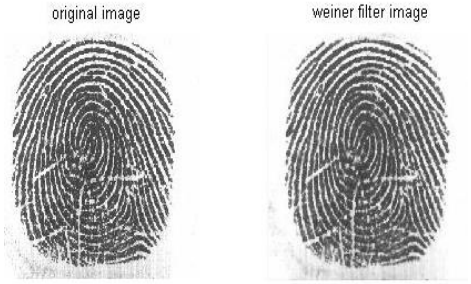

Fig – 5: Weiner filter output

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

5.4.2.Fake images

Training results for fake image is shown in Table 2.

Table –2: Training results for fake image

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 Images, R1-R12-Real Image

5.5.TESTING RESULTS FOR DATABASE IMAGE:

5.5.1. Real finger print image

The Table 3. represents the value of real

Table - 3: Testing results – real finger print image

PARAMETER	INPUT 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

5.5.2.Fake fingerprint image

The Table 4. represent the value of fake finger print image.The Table 5. shows the different analysis of real and fake finger print.

Table –4: Testing results – fake finger print image

PARAMETER	INPUT 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

5.6.OVERALL RESULTS

FEATURE	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

Table – 5: Overall results – Real & Fake image

6. CONCLUSIONS

This paper develops a new framework to consistently perform at a high level for different biometric traits. The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection. The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios. The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions. In addition to its very competitive performance and to its "multi-biometric"and"multi-attack"characteristics. The proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system. It has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks and validation of a new biometric protection method. Reproducible evaluation on multiple biometric traits based on publicly available databases. Comparative results with other previously proposed protection solutions.

REFERENCES

[1] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofin"', *in Proc. IEEE Int. Conf. Biometric. Special Interest Group*, 2012

[2] J. Daugman, "How Iris Recognition Works",*IEEETransactions onCircuits and Systems for Video Technology*, vol.14, No.1, pp. 21 – 30, 2004

[3] J. Daugman, "New Methods in Iris Recognition", *IEEE Transactions onSystems,* Man, and Cybernetics B, Vol. 37, No.5 , pp. 1167 – 1175, 2007

[4] R. Derakhshani, S.A. Schuckers,L.A.Hornak, and L. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in finger print scanners",*Pattern Recognition,* Vol. 36, no. 2, pp.383-396, 2005

[5] ElhamTabassi, L. Charles Wilson Craig,"Watson Fingerprint Image Quality" , NISTIR 7151, *National Institute of Standards and Technology, Gaithersburg, 2004.*

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

[7] J. Galbally, J. Fierrez, F. Alonso-Fernandez and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems", *J. Telecommun. Syst.*, Vol. 47, No.3-4, pp. 243–254,2011.

[8] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks", *Pattern Recognit.,* Vol. 43, No. 3, pp.1027–1038, 2010.

[9] B. Geller, J.Almog, P. Margot, and E. Springer, "A chronological review of fingerprint forgery"*J. Forensic Sci.,* Vol.44, No.5, pp. 963-968, 1999.

[10] A. K. Jain, K.Nandakumar and A. Nagar, "Biometric template security", *J. Adv. Signal Process.,* Vol. 2008, pp.113–129, 2008.

[11] A. Liu,W. Lin and M. Narwaria, "Image quality assessment based on gradient similarity" ,*IEEE Trans. Image Process.,* Vol. 21, No. 4, pp.1500–1511, 2012.

[12] E. Marascoand C. Sansone,"Combining perspiration-and morphology based static features for fingerprint liveness detection", *Pattern Recognit.Lett.,* Vol. 33, No. 9, pp.1148–1156, 2012.

[13] 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, 2013.

[14] 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, 2010.

[15] D.W. Osten, H.MCarim, M.R. Arneson, andB.L. Blan, "Biometric, personal authentication system", *United States Patent* 5719950, 1998.

[16] M. Pons, J. Malo, J.M. Artigas, and P. Capilla, quality metric based on multidimensional contrast perception models', *Displays,* Vol. 20, No. 2, pp. 93–110, 1999.

[17] S.A. Schuckers, "Spoofing and Anti-Spoofing Measures",*Information Security Technical Report,* Vol. 7, No. 4, pp.56 – 62, 2002.

