FAKE BIOMETRIC DETECTION USING IMAGE QUALITY ASSESSMENT

Linsha Luvis
M-Tech Embedded Systems, Dept. of ECE
Sahrdaya College of engineering and technology, Kodakara
Thrissur, India
Linshaluvis96@gmail.com

Dr.G.R. Gnana King
Assoc.Professor, Dept of ECE
Sahrdaya College of engineering and technology, Kodakara
Thrissur, India
Kings.326@gmail.com

***Abstract*— Biometric system plays important role in everyone's life as security. Biometric system is a security system which provides conditional ways after scanning for unique physical characteristics for authentication. But fake, artificially constructed sample is a main issue in the process of biometric validation. These biometric security systems are more flexible to several types of attacks such as some of artificially manufactured artifact (eg: fake fingerprints, photo print of iris image or face mask). Hence new and effective protection actions developed in hardware and software to resist these attacks. Image quality assessment is one of the techniques used to decide whether the biometric input is real or synthetic .this paper deals with full reference and no reference measures used to evaluates the quality value of an image.25 image quality features are takeout using mathematical expressions. In this paper we introduce the hardware implementation of the biometric system based on Image quality assessment.**

Keywords—image quality assessment, biometrics, security.

I INTRODUCTION

BIOMETRIC authentication has been getting much relevance over the last years due to the growth of demand for automatic person identification. The term biometric mention here to automatic identification of a person based on behavioral and /or physiological properties (eg: fingerprint, face, iris, voice, signature, etc.) which cannot be taken, lost or copied. As the use of a biometric system in many security purposes, the attacks have also increased. The researchers mainly concentrated on the evaluation of multiple biometric weaknesses, a suggestion of new security methods and the acquisition of datasets. All these clearly focused attention on the significance given by them to the enhancement of the systems security to make this technology into practical use as more efficient. Among the various attacks evaluated the direct and spoofing attacks have motivated to examine the vulnerabilities towards this type of fraudulent actions.As this type of fraud actions are execute in analog domain and the interactions with the device is done following the regular protocol, the usual digital security mechanisms (eg: encryption, digital signature or watermarking) are not useful. So researches focused on the outline of particular methods to find the fake samples and reject them thus enhance security level of the system.

Liveness detection methods are usually two types: (i) hardware-based methods, used to detect properties of a living trait (e.g. fingerprint sweat, blood pressure, or specific reflection properties of the eye); (ii) software-based methods, the fake sample is identified once the sample has been got with a standard sensor.[1] The combination of these two methods is used to increase security in biometric recognition. One of the disadvantages of protection measures is the lack of generality. The current protection measures are based on the measurement of certain specific properties of a given trait; they may not be executed in recognition systems based on other biometric techniques. In the present work, we deal with both software-based multibiometric and multi-attack security method and also the hardware implementation. Image quality assessment is an extremely good method for person identification process. We have created a model from the input samples. Then we put the test image in order to check accuracy of that model. In this model we use a camera and raspberry pi in the hardware section. The software approach has advantages of fast, user friendly, cheap etc. and we add additional advantages as less complexity and protection for any kind of attacks.

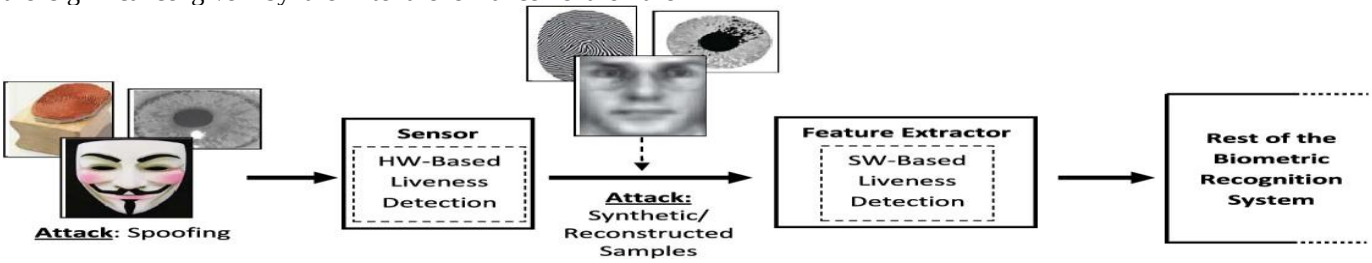


Fig 1 Hardware and software based spoofing detrction techniques

II RELATED WORKS

Some of the techniques are based on the skin properties for this; Li et al. [2] propose a technique to detect the spoofing attack. The live face detection has done by analyses of Fourier spectra of the single face image. When compare to real faces, the photographs are a normally smaller size and they would contain less high-frequency components. The results showed that these methods have an encouraging performance.

J.Maatta et al [3] present an efficient method for face recognition from single face images by applying microtexture analysis. In this, for liveness detection, they make use of multi-scale local binary pattern (LBP). Then it classified to real or fake by support vector machine (SVM) classifier. In this, they are using a publically available database (NUAA photograph Imposter Database). In this method, the differences between real and fake printed faces are the main concern. The main differences between them are the reflection of light and the quality difference that can be detected with micro-texture patterns. By using local binary patterns, it describes its micro-textures and their spatial information. Then the feature vector fed to SVM classifier which classifies whether it's real or fake. Main advantages are robustness and computationally fast.

Pan et al [4] propose a blinking based method. It uses a generic camera and based on the eye blink it classified in to real or fake. It does not require the extra hardware and it can finish in a non-intrusive manner. Kollreider et al [5] describe a approch based on the face motion estimation. It based model based local Gabor feature extraction and SVM classification. To detect a face part, estimated optical flow (OFL) pattern matching and classify using the model based Gabor classification. It is a quick method and robust. Bao et al [6] also used optical flow for motion estimation. One main concern of these optical flow techniques are that users required to be highly cooperative and it take more time for detection, which will make users uncomfortable.

Tan et al [7] propose a method to detect the spoofing with photograph and video based on the analysis of the Lambertian model. In this paper, they formulate the task of detecting photograph spoof as a binary classification problem. The method extracts latent reflectance features of samples by a variational retinex technique and difference-of-Gaussians (DoG) method. Then these are used for the classification process. There is no extra hardware required.

S.A. Dhole et al [8] proposes face identification using curvelet transform method. Using the curvelet transform the features are extracted. The curvelet coefficients create a feature vector for classification. These coefficients set then used to train gradient decent back propagation neural network (NN). Zhang et al [9] present multispectral face liveness detection method. The Lambertian model, examine multispectral features of human skin versus non-skin. To form training set the reflectance data of real and synthetic faces at multi-distances are selected for classification. SVM classifier is used for the classification process.

Wieclaw et al [10] propose a minutiae-based fingerprint identification and verification. It consists of two procedures, minutia extraction and matching. Depends on the accuracy of the minutia extraction procedure the performance is determined. Crossing Number (CN) concept is the technique used in minutiae extraction. The main concern is the image quality of the fingerprint. When the quality of images decreased, increase the number of false minutiae point.

Drahansky et al [11] propose method is based on the detection of optical characteristics of the finger surface (skin). In this paper detect motion of papillary lines by two methods based on optical principles. One is based on the close-up view of the fingertip by CCD camera; the second one is the distance measurement with a laser sensor. The fingerprint liveness detection has several methods: the wavelet analysis of the fingertip texture [12], the curvelet analysis of the fingertip texture [13], and the combination of local ridge frequencies and multiresolution texture analysis [14]

Li et al [15] describe new feature descriptors are defined by a multiscale directional transform (shearlet transform) for both face liveness detection and recognition. In this, they are using the CASIA Face Anti-Spoofing Database for evaluation. Chen et al [16] propose iris recognition based on a wavelet quality measure. It has the ability to deliver good special adaptively and deals with local quality measures of the iris image. Proenca et al [17] propose a method to get the quality of VW iris samples takes in unconstrained conditions. Focus, motion, angle, pupillary dilation, and levels of iris pigmentation are the factors that determine the quality of iris image. Zuo et al [18] describe a methodology which suitable for any biometric. Three methods to increase the properties of biometric matches are described. Quality of sample (QS) and confidence in matching scores (CS) are the first two methods and the third method only use for discrimination between real and fake matching scores.

Y. Kim et al [19] describe the behavior of reflectance in real and fake images. The sensor classifies using Fisher's linear discriminant, and they achieved 97.78 accuracies. Fierrez et al [20] review the existing methods for quality computation of fingerprint image. They are using the MCYT database which including 9000 fingerprint images. A lot of papers were told about the biometric security attacks and its protection methods. The image quality assessment technique is different from that because of its good performance under different multi biometric systems. Image quality assessment is based on the quality difference. It is a protection method for different biometrics from different kind of attacks.

III IMAGE QUALITY ASSESSMENT

The use of image quality assessment assumes that: "it is expected that a fake image will have a different quality than a real sample". In the proposed system the input samples are classified into one of two classes: real or fake. The proposed biometric system classified as real or fake based on the quality

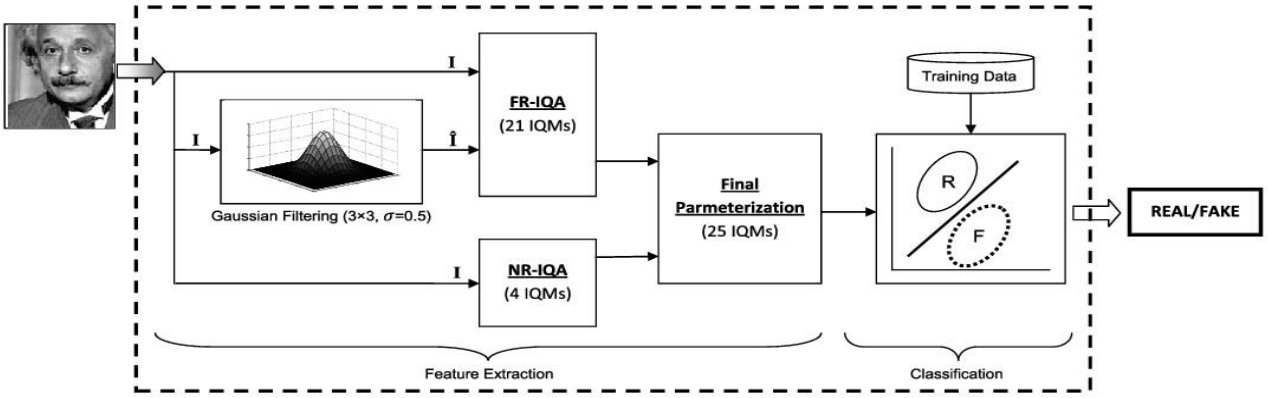


Fig 2 block diagram of biometric protection method

difference hypothesis.we expect that artificially produced samples has low quality and the real ones has high quality. In specific, our software experiments implemented in OpenCV in c++ language of the support vector machine classifiers and hardware experiments implemented in python language. Feature extraction is the method which takes out the desired features from the pre-processed images. The system uses 25 quality features for feature extraction.these features are extracted using mathematical expressions.

A.FULL REFERENCE IQ MEASURES

In full reference, IQ measures the comparison between input and reference image and the features extracted using mathematical functions. Full reference means there is a clean undistorted reference image is given then the input sample is compare with this image. Then evaluates its quality difference then classified into real or fake. The fake image has low quality when it compared with the real ones. The input image is filtered using low pass gaussian kernel for smoothening process. Then the smoothed image is compared with the original image and computed the quality difference. The full reference measures are classified into 3 main categories. They are

- Error sensitivity measures
  - a)Pixel difference measures,
  - b)Correlation-based measures,
  - c)Edge-based measures,
  - d)Spectral distance measures and
  - e)Gradient-based measures.
- Structural similarity measures,
- Information theoretic measures.

1)error sensitivity measures: error sensitivity measures are based on measuring the errors between the distorted and reference images.

- Pixel Difference measures: it calculates the distortion between two samples based on the pixel value difference. Here we consider Mean Squared Error (MSE)[21], Signal to Noise ratio (SNR)[22] Peak Signal to Noise Ratio (PSNR)[23],Maximum Difference(MD)[24], Structural Content (SC)[24], Average Difference (AD)[24], Normalized Absolute Error (NAE)[24] ,R-Averaged Maximum Difference (RAMD)[21] and Laplacian Mean Squared Error (LMSE).[24]
- Correlation-based measures: it considers the similarity between two digital images. This includes Normalised Cross Correlation (NXC)[24], Mean Angle Similarity (MAS)[21] and Mean Angle Magnitude similarity (MAMS)[21]
- Edge-based measures: the edges are the most informative parts of an image we consider two edge related measures. Total edge difference (TED)[25], and Total corner difference (TCD)[25] edges are detected by Sobel operator and corners are detected by the Harris corner detector
- Spectral distance measures: in this, we applying Fourier transform for image quality assessment. In this, we consider Spectral Magnitude Error (SME)[26] and Spectral phase Error (SPE).[26]
- Gradient-based measures: in this structural and contrast changes are considered. We consider Gradient Magnitude Error (GME)[27],and Gradient Phase Error (GPE)[27].

2) Structural Similarity Measures: it considers there is a variation in lightning contrast or brightness is different in the structural image compared to the distorted image. Structural similarity index measure (SSIM)[28] has used in practical applications.

3) Information Theoretic measures: In these two features are considered the Visual information Fidelity (VIF)[29] and the reduced reference entropic difference index (RRED)[30]

B.NO REFERENCE IQ MEASURES

The no reference measures are adopting the human visual system. The human visual system does not require the reference image to determine its quality level. No reference method also does not require a reference image. Three approaches are there Distortion specific approaches, training

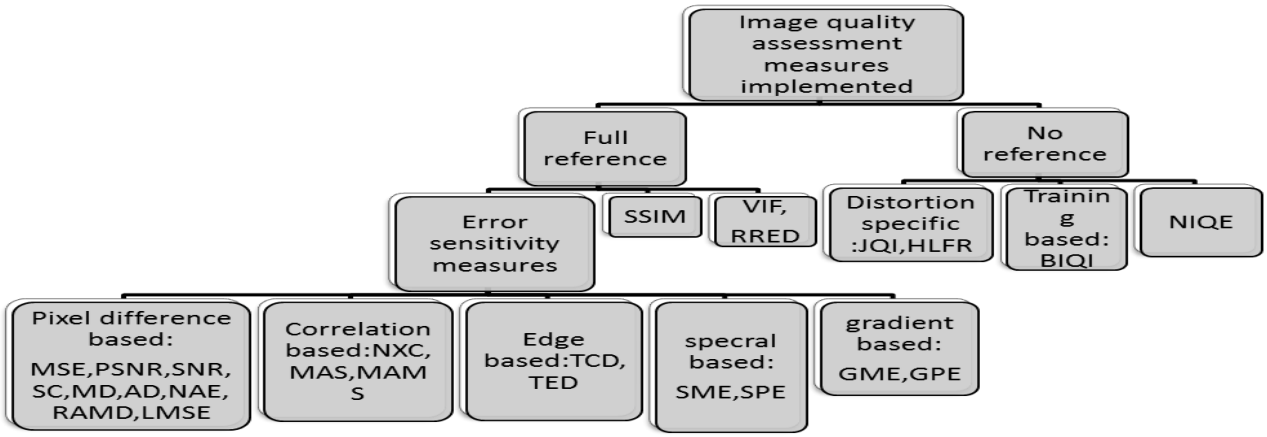


Fig 3 25 image quality measures classified into full reference and no reference measures.

based approaches natural scene static approaches. The no reference method is more complex than full reference method. The test image is compare with pre trained statistical models

Distortion specific approaches: it contains the JPEG Quality Index (JQI)[31].JPEG is a block DCT based lossy image coding technique it evaluates the quality of image the usual block artifacts. The High low-Frequency Index (HLFI)[32] using the upper and lower frequency of the Fourier spectrum the sharpness of the image is computed.

Training based approaches: the model is trained using real and fake samples. Then the quality score computed based on the number of features extracted.

Natural scene static approaches: in this, we are using natural quality evaluator (NIQE)[33]. It is a blind quality analyzer (BIQI)[34] based on the collection of statistical quality features.

IV ARTIFICICIAL INTELIGENCE

Our project was done using the artificial inteligence technology. In computer science the artificial inteligence is an emerging technology and it also called the machine inteligence. By using mechine learning the computer systems can perform specific tasks without using explicit instructions.

Machine learning algorthm creates a mathematical model using the traing data. and verify that using testing data. Maching learning algorithums are used in many applications. The one of the application is the computer vision , it is that computer can made decisions from digital images and videos. It include the acquiring of high quality image or video,processing, analysing and produce numeric or symbolic information as decisions

V SVM CLASSIFICATION

Support vector machine classification is supervised learning, which the input images are mapped into either one of the two categories as real or fake. It is used only when the training set of correctly identified observation available. The given training examples are mapped to different categories are divided by a clear wide gap. Then the new samples are classified into any one of the category.then evaluates its accuracy.

Training algorithm

1)Read the sample images from the database for training
2)acquire the image quality features by full reference and no-reference measures
3)Combine all the feature and form a feature vector, which contains a number of features that are descriptive of the object
4)construct a target for SVM classification
5)SVM classifier trained with two categories as real or fake

Testing algorithm

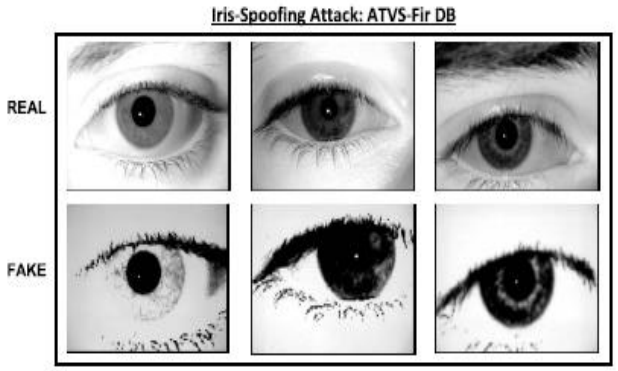
1)Read the test images
2)Acquire the image quality features from the test image
3)Collect all the features and form a feature vector
4)The feature vector is now compared with the trained feature values using SVM classifier
5)Finally, the test image is classified as real or fake.

VI EXPERIMENTAL SETUP

In this system,we need to achive good perfomance under different biometrics :iris, fingerprint, face. we use 25 quality features for feature extraction and SVM classifier for classification. 25 image quality features are takeout using mathematical expressions The results are expressed in terms of False Genuine rate (FGR), number of false samples which classified as real; and False Fake rate (FFR), number of genuine samples which are considered as fake. The Half Total Error Rate (HTER) computed as

$$HTER=(FGR+FFR)/2$$

A.RESULTS: IRIS



. Fig 4 typical real and fake iris samples used in spoofing attacks

For Iris spoofing the database used for evaluation is from AVTS-Flr DB which acquired from the biometric recognition group –AVTS (http://atvs.ii.uam.es/). For the iris we considering two types of attacks, namely:1) spoofing attack and 2) attack with synthetic samples. The databases are divided into two sections one for training and next for testing. The train set used for training the classifier, and test set used for checking the performance of the system.

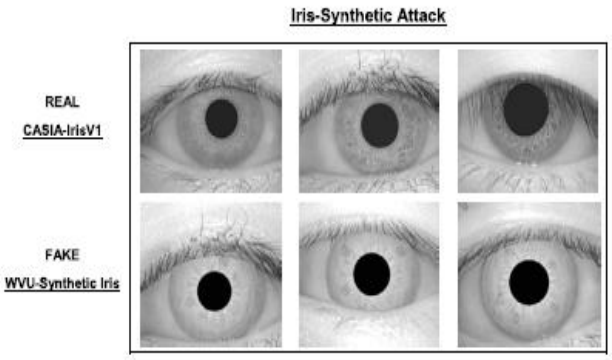


Fig 5 typical real and fake iris samples used in synthetic attacks.

Typical fake and real iris images used for synthetic experiments are may be found in WVU synthetic Iris DB (http://www.citer.wvu.edu/) and CASIA-Iris VI(http://biometrics.idealtest.org)

	Results:iris			
	FFR	FGR	HTER	Av.Exec.(s)
Iris spoof	4.2	0.25	2.2	0.328
Iris spoof[35]	1.3	4.9	3.1	2.563
Iris synthetic	3.4	0.8	2.1	0.356

Table I results obtained for iris by using IQA method

The classifier used for the two analysis is support vector machine classification. This result is obtained using standard 64-bit windows 10 PC which has 2 GHz processor and 8 GB RAM memory, running in qt creator using OpenCV library. The table shows the results obtained by image quality assessment method. The top and bottom row for spoofing and synthetic modality. For comparison the middle row shows the results obtained in anti spoofing method disscussed in [35]. The last column indicates the avarage execution time to process the sample.

B.RESULTS: FINGERPRINTS

In fingerprint evaluated using LivDet 2009 DB*. Using three different optical sensor the real and fake datasets are constructed 1)Biometric FX2000 (569 dpi)2)CrossMatch Verifier 300CL (500 dpi) 3)Identix DFR2100 (686 dpi) . The gummy fingers are made by silicone, gelatine or playdoh materials. The database images are divided for training and testing. The classifier used here is support vector machine classifier. It classifies the given input into real or fake.

	LivDet 2009 DB			
	Training(real/fake)		Testing(real/fake)	
	Finger	samples	fingers	samples
crossmatch	35/35	1000/1000 (344g+ 346p+310s)	100/35	3000/3000 (1036g+1034p+ 930s)
biometrica	13/13	520/520s	39/13	1473/1480s
Identix	63/35	750/750(250 g+250p+ 250s)	100/35	2250/2250 (750g+750p+ 750s)

Table II Structure of LivDet 2009 DB

The general distribution of the database is expressed in Table II. The fake samples are given in terms of the materials used:g for gelatin, p for playdoh and s for silicon In Table III reported the results from different methods and from that we can compare the results. the Marasco et al introduces a novel fingerprint liveness method using perspiration and morphological features and in this they used LivDet 09 database for evaluvation.the moon et al used wavelet analysis of the finger tip texture, Nikam et al based on the curvelet analysis of the finger tip texture and abhyankar et al used the combination of local ridge frequencies and multiresolution texture analysis. And these methods are compared with the image quality assessment method. The last row shows the avarage execution time of image quality assessment method to process each sample.
This result is obtained using standard 64-bit windows 10 PC which has 2 GHz processor and 8 GB RAM memory, running in qt creator using OpenCV library

	Comparative results:fingerprints-livDet 09

	Crossmatch			Biometika			Identix		
	FFR	FGR	HTER	FFR	FGR	HTER	FFR	FGR	HTER
IQA based	8.6	12.8	10.7	14.0	11.6	12.8	1.1	1.4	1.2
Best livDet09[37]	7.4	11.4	9.4	15.6	20.7	18.2	2.7	2.8	2.8
Marasco et al[38]	17.4	12.9	15.2	12.2	13.0	12.6	8.3	11.0	9.7
Moon et al [12]	27.4	19.6	23.5	20.8	25.0	23.0	74.7	1.6	38.2
Nikam et al[13]	19.0	18.4	18.7	14.3	42.3	28.3	23.7	37.0	30.3
Abhyankar et al[14]	39.7	23.3	31.5	24.2	39.2	31.7	48.4	46.0	47.2
Av.exec.(s)	0.231			0.169			0.368		

Table III Comparative results:fingerprints-livDet 09

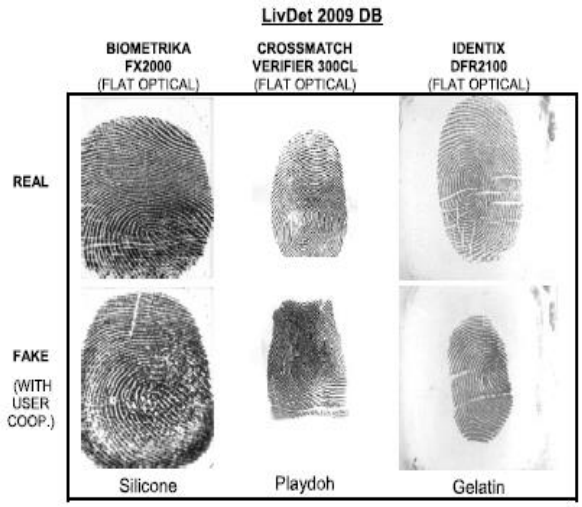


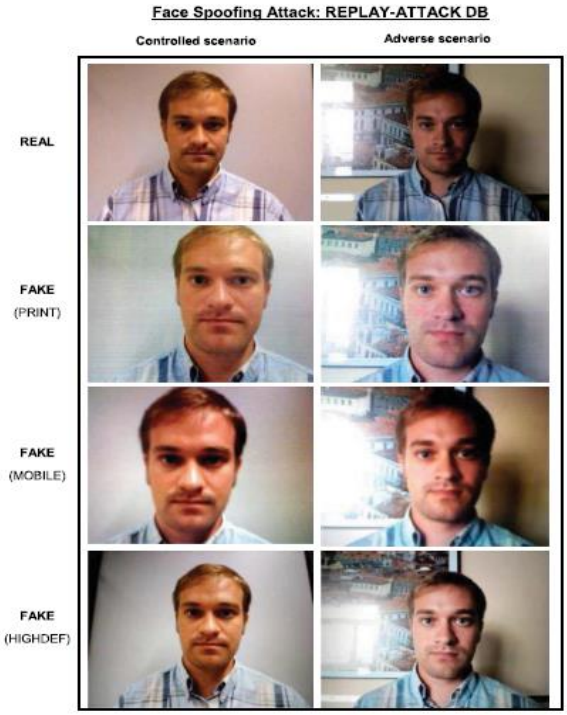
Fig 6 examples of real and fake fingerprint images

C.RESULTS: FACE

In 2D face we consider different types of attacks 1) print, high-resolution digital photographs, 2) mobile, photos captured by iPhone using iPhone screen 3) high def., the photos are displayed using resolution 1024×768

	Comparative :Replay.-ATT.DB(print)		
	FFR	FGR	HTER
IQA based(svm)	0.0	0.0	0.0
IQAbased	0.0	1.0	0.5
AMILAB[36]	0.0	1.2	0.6
CASIA[36]	0.0	0.0	0.0
IDIAP[36]	0.0	0.0	0.0
SIANI[36]	0.0	21.2	10.6
UNICAMP[36]	1.2	0.0	0.6
UOULU[36]	0.0	0.0	0.0

Table IV Comparison of results,obtained on the print subscorpus of the replay attack.



.

Fig 7 examples of real and fake(print, mobile, and high-def) face images.

In this, we capture sufficient quality face images using web camera and these face images are proceed for feature extraction.then the base of training samples the SVM classifier classifies these images to either real or fakeThis result is obtained using standard 64-bit windows 10 PC with 2 GHz processor and 8 GB RAM memory, running in qt creator using OpenCV library

D.HARDWARE IMPLEMENTATION

For hardware implementation we are using a raspberry pi as its main part. It is a 1.4 GHz 64-bit quad core processor, and it has dual band wireless LAN, Bluetooth 4.2/BLE, faster Ethernet and power over Ethernet support.it is programmed using the python language and classify using SVM classifier. The high quality image captured using pc web camera and.the the main drawback is the execution time.

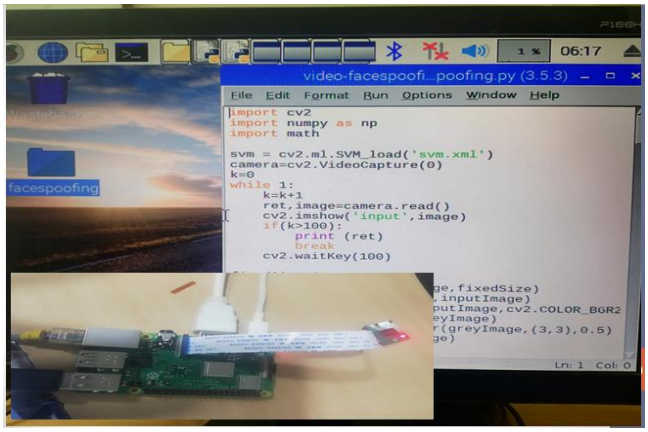


Fig 8 Hardware Implementation

VII CONCLUSION AND FUTURE SCOPE

In this paper, we have introduced a method for biometric detection using image quality assessment and SVM classification. In this method, we are considering the quality variations between real and fake biometric traits. We consider 25 quality features integrate with a simple classifier to identify real and fake traits. The most common drawback anti-spoofing method is the absence of generality. The present work is a software base multi-biometric and multi-attack protection with high performance. The main advantage of this approach: fast, non-intrusive, user-friendly, cheap and easy to embed in already functional systems. It has also an added advantage is its speed and very low complexity.it has been verified by publically available databases of iris, fingerprint, and 2D face. There are also possibilities to future work including the extension of quality features, and can extend this application other image-based protection methods (e.g., hand geometry, vain, palm print, etc.).Video attacks can be also detected using video quality measures.

References

[1] Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez vol. 23, no. 2, February 2014

[2] J. Li, Y. Wang, T. Tan, and A. K. Jain.(2004.) "Live face detection based on the analysis of fourier spectra". In Biometric Technology for Human Identification, pages 296303

[3] J. Maatta, A. Hadid,and M. Pietikainen, (2011)"Face Spoofing Detection From Single Images Using Micro-Texture Analysis", IEEE Transaction of Image processing,

[4] 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

[5] K. Kollreider, H. Fronthaler, and J. Bigun. Non-intrusive liveness detection by face images. Image and Vision Computing, 27:233–244, 2009.

[6] W. Bao, H. Li, N. Li, and W. Jiang. A liveness detection method for face recognition based on optical flow field. In 2009 International Conference on Image Analysis and Signal Processing, pages 233–236. IEEE, 2009

[7] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In Proceedings of the 11th European conference on Computer vision: Part VI, ECCV'10, pages 504–517, Berlin, Heidelberg, 2010. Springer-Verlag

[8] Mrs.Dhole S.A. Dr. Prof. Patil V.H, (2015), "Face Recognition Using Curvelet Transform", International Journal of Applied Engineering Research, Volume 10, No. 14 pp.33949-33954, August 2015(Impact factor0.166),Scopus indexing

[9] Zhiwei Zhang, Dong Yi, Zhen Lei, Stan Z. Li "Face Liveness Detection by Learning Multispectral Reflectance Distributions" Chinese National Natural Science Foundation Project #61070146, National Science and Technology Support Program Project #2009BAK43B26

[10] Łukasz Więcław (2009)"A Minutiae-Based Matching Algorithms In Fingerprint Recognition Systems" Journal Of Medical Informatics & Technologies Vol. 13/, ISSN 1642-6037

[11]] Martin Drahansky, Dana Lodrova,(2008) "Liveness Detection for Biometric Systems Based on Papillary Lines "International Journal of Security and Its Applications Vol. 2, No. 4, October

[12] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," Electron. Lett., vol. 41, no. 20, pp. 1112–1113, 2005

[13] S. Nikam and S. Argawal, "Curvelet-based fingerprint anti-spoofing," Signal, Image Video Process., vol. 4, no. 1, pp. 75–87, 2010.

[14] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques," in Proc. IEEE ICIP, Oct. 2006, pp. 321–324.

[15] Yuming Li, Lai-Man Po "Face Liveness Detection And Recognition Using Shearlet Based Feature Descriptors" IEEE ICASSP 874978-1-4799-9988-0/16 ©2016

[16] Y Chen, S Dass, A Jain, "Localized iris image quality using 2-D wavelets,Advances in Biometrics," Lecture Notes in Computer Science, vol. 3832.(Springer, Berlin Heidelberg), pp. 373381

[17] H Proena, (2011) "Quality assessment of degraded iris images acquired in the visible wavelength". IEEE Trans. Inf. Forensics Secur. 6(1), 8295

[18]] Yingbo Zhou, Ajay Kumar, "Contactless Palm Vein Identification using Multiple Representations, Department of Computing," The Hong Kong Polytechnic University

[19] Y. Kim, J. Na, S. Yoon, and J. Yi, (2009.) "Masked fake face detection using radiance measurements," Journal of the Optical Society of America A, vol. 26, no. 4, pp. 760–766

[20] Fernando Alonso-Fernandez, Julian Fierrez-Aguilar, Javier Ortega-Garcia (2005)"A Review Of Schemes For Fingerprint Image Quality Computation" European Co-Operation in the Field of Scientific and Technical Research

[21] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.

[22] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," Electron. Lett., vol. 44, no. 13,pp. 800–801, 2008.

[23] S. Yao, W. Lin, E. Ong, and Z. Lu, "Contrast signal-to-noise ratio for image quality assessment," in Proc. IEEE ICIP, Sep. 2005, pp. 397–400.

[24] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," IEEE Trans. Commun., vol. 43, no. 12, pp. 2959–2965, Dec. 1995.

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

[26] 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.

[27] 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, Apr. 2012.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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

[33] 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.

[34] 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.

[35] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB,Mar./Apr. 2012, pp. 271–276.

[36] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks,"in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

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

[38] E. Marasco and C. Sansone, "Combining perspiration-and morphologybased static features for fingerprint liveness detection," Pattern Recognit. Lett., vol. 33, no. 9, pp. 1148–1156, 2012.