International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.04,Issue.46,
November-2015,
Pages:10023-10028

www.ijsetr.com

Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

K. RAKESH[1], MD. RAFEEK PASHA[2], ANIL SOORAM[3]

[1]PG Scholar, Dept of ECE, Farah Institute of Technology, Chevella, R.R. (Dt), TS, India, Email: rakeshgoud4121@gmail.com.
[2]Associate Professor, Dept of ECE, Farah Institute of Technology, Chevella, R.R. (Dt), TS, India.
[3]Associate Professor, Dept of ECE, Farah Institute of Technology, Chevella, R.R. (Dt), TS, India.

Abstract: A biometric system is a computer system .Which is used to identify the person on their behavioral and physiological characteristic (for example fingerprint, face, iris, key-stroke, signature, voice, etc). A typical biometric system consists of sensing, feature extraction, and matching modules. But now a day's biometric systems are attacked by using fake biometrics. This paper introduce three biometric techniques which are face recognition, fingerprint recognition, and iris recognition (Multi Biometric System) and also introduce the attacks on that system and by using Image Quality Assessment For Liveness Detection how to protect the system from fake biometrics. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

Keywords: Image Quality Assessment, Biometrics, Security, Attacks, And Countermeasures.

I. 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 [2]: the publication of many research works disclosing and evaluating different biometric vulnerabilities [3], [4], the proposal of new protection methods [5], [6], related book chapters [7], the publication of several standards in the area [8], [9], the dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences [10], the organization of competitions focused on vulnerability assessment [11], [12], the acquisition of specific datasets, the creation of groups and laboratories specialized in the evaluation of biometric security, or the existence of several European Projects with the biometric security topic as main research interest. Fake biometrics means by using the real images (Fig 1. Iris images captured from a printed paper and Fig 2. Fingerprint captured from a dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different type that are face recognition system, fingerprint recognition system, iris recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioral biometric). Fig. 3 shows the type of different biometric.

Multi biometric system means a biometric system is used more than one biometric system for one multi-biometric system. A multi biometric system is use the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this Survey Base seminar report Image quality assessment for Liveness detection technique is used for find out the fake biometrics. Image assessment is force by supposition that it is predictable that a fake image and real sample will have different quality acquisition. Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, Fig.1 shows iris images captured from a printed paper are more likely to be fuzzy or out of focus due to shaky; face images captured from a mobile device will almost certainly be over-or under-discovered; and it is not rare that fingerprint images which is shows in Fig 2 captured from a dummy finger. In addition in ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor,

this fake sample will most probably not have some of the properties found in natural images.

Fig.1. Fake iris.

Fig.2. fake fingerprints.

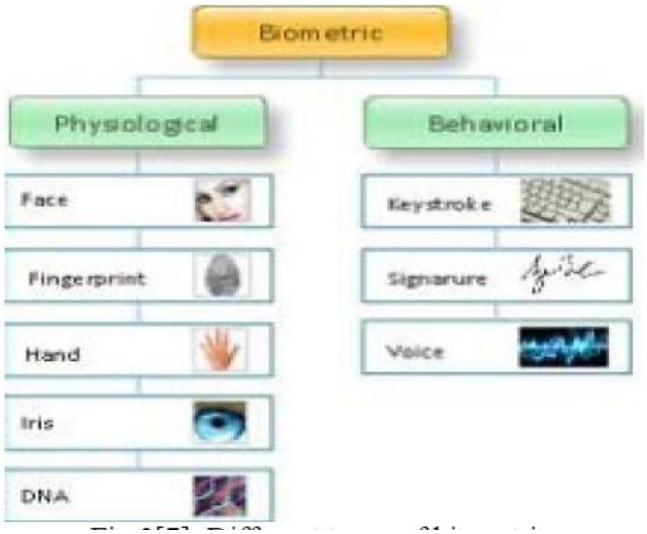

Fig.3. Different types of biometric.

Image quality assessment is a most important topic in the image processing area. Image quality is a trait of any image usually compared with an ideal or perfect image. Digital images are subject to a large range of distortions during storage, achievement, compression, processing, transmission and reproduction, several of which may result in a degradation of visual quality. Imaging systems introduces some amount of distortion or artifacts which reduces the quality assessment. In general quality assessment is of two types one is subjective visual quality assessment and second one is objective visual quality assessment. Objective image quality metrics can be classified on the basis of availability of an original image, with the distorted image is to be compared as shown in Fig.1. Accessible approaches are known as full-reference, meaning that a complete reference image is assumed to be known. In many practical applications, however, the reference image does not exist, and a no-reference or "blind" quality assessment approach is desirable. The rest of the paper is structured as follows. Liveness Detection Methods are given in Section II. Image Quality Assessment for Liveness Detection in Section III .The results for iris, fingerprint and 2D face evaluation experiments appear in Sections IV-A, IV-B, and IV-C. Conclusions are finally drawn in Section V.

II. LIVENESS DETECTION METHODS

Liveness detection methods are generally classified into two types (see Fig. 4): (i) Software-based techniques, in 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 trait itself); (ii) Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye). Liveness detection techniques, which use different physiological properties to differentiate between real and fake character Liveness assessment 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 in 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; (iv) performance, in calculation to having a good fake detection rate, the protection system should not degrade the recognition performance (i.e., false rejection) of the biometric system. The two types of methods have certain advantages and disadvantages over the other and, in general, a combination of both would be the most advantageous protection approach to increase the security of biometric systems.

As a common comparison, hardware-based schemes generally present a higher fake detection rate, at the same time software-based techniques are in 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 (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially accomplished of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system

against the addition of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor.

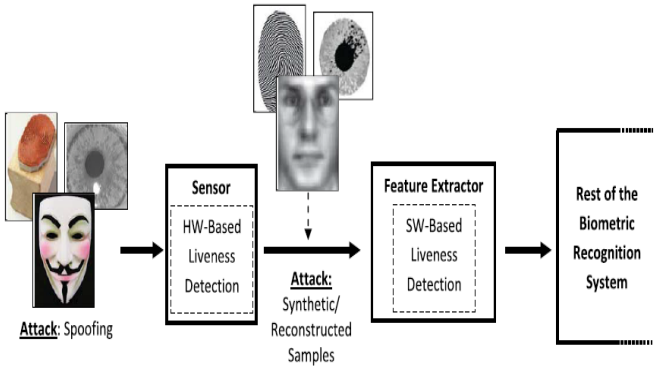

Fig.4. Types of attacks potentially detected by hardware based (spoofing) and software-based (spoofing + reconstructed/synthetic samples) Liveness detection techniques.

III. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for Liveness detection is motivated by the supposition that: "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed." Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be unclear or out of focus due to trembling; face images captured from a mobile device will most likely be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local gaining artifacts such as spots and patches. Also, in an ultimate attack in which an unnaturally 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.

The potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing) different quality measures present diverse sensitivity to image artifacts and distortions for example, measures like the mean squared error respond additional to additive noise, while others such as the spectral phase error are extra sensitive to blur; while gradient-related features respond to distortions concentrated around edges and textures. Therefore, using a large range of IQMs exploiting complementary image quality properties should allow detecting the aforementioned quality differences between real and fake samples expected to be found in many attack attempts (i.e., given that the technique with multi-attack protection capabilities). So consider that there is sound proof for the "quality-difference" theory and that image quality measures have the possible to achieve success in biometric protection tasks.

IV. EXPERIMENTS AND RESULTS

The evaluation experimental protocol has been designed with a two-fold objective:

- First, evaluate the "multi-biometric" dimension of the protection method. That is, its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose three of the most extended image-based biometric modalities have been considered in the experiments: iris, fingerprints and 2D face.
- Second, evaluate the "multi-attack" dimension of the protection method. That is, its ability to detect not only spoofing attacks (such as other Liveness detection specific approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples (see Fig. 4).

With these goals in mind, and in order to achieve reproducible results, we have only used in the experimental validation publicly available databases with well described evaluation protocols. This has allowed us to compare, in an objective and fair way, the performance of the proposed system with other existing state-of-the-art Liveness detection solutions. The task in all the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples. As explained, for this purpose we build a 25-dimensional simple classifier based on general IQMs. Therefore, in all cases, results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; and the False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as HTER = (FGR + FFR)/2.

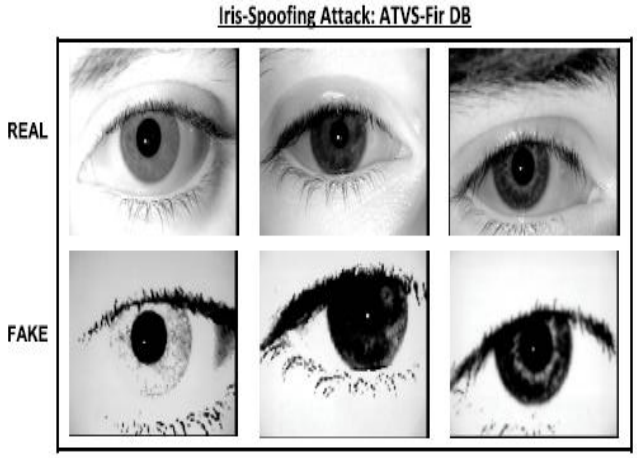

Fig.5. Typical real iris images (top row) and their corresponding fake samples (bottom row) that may be found in the ATVS-FIr DB used in the iris-spoofing experiments. The database is available at http://atvs.ii. uam.es/.

A. Results: Iris

For the iris modality the protection method is tested under two different attack scenarios, namely: i) spoofing attack and ii) attack with synthetic samples. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method. In all cases the final results are obtained applying two-fold cross validation. The classifier used for the two scenarios is based on Quadratic Discriminant Analysis (QDA) as it showed a slightly better performance than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments, while keeping the simplicity of the whole system.

1. Results: Iris-Spoofing: The database used in this spoofing scenario is the ATVS-FIr DB which may be obtained from the Biometric Recognition Group-ATVS. The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the Bio Sec baseline corpus. It follows the same structure as the original Bio Sec dataset, therefore, it comprises 50 users×2 eyes×4 images×2 sessions = 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG Iris Access EOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels. In Fig.5 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other 50 eyes available in the dataset.

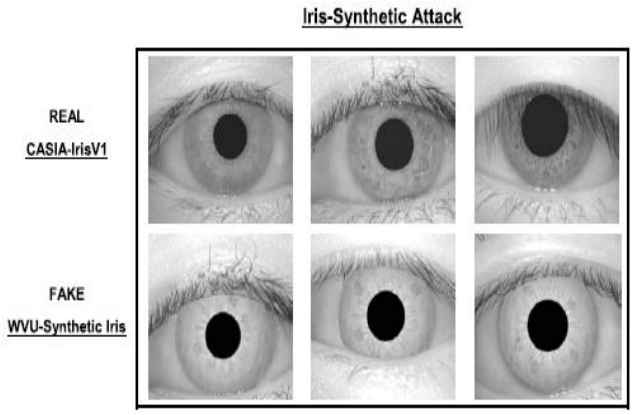

Fig.6. Typical real iris images from CASIA-IrisV1 (top row) and fake samples from WVU-Synthetic Iris DB (bottom row), used in the iris-synthetic experiments the databases are available at http://biometrics.idealtest.org and http://www.citer.wvu.edu/.

The Liveness detection results achieved by the proposed approach under this scenario appear in the first row of Table I, where we can see that the method is able to correctly classify over 97% of the samples. In the last column we show the average execution time in seconds needed to process (extract the features and classify) each sample of the two considered databases. This time was measured on a standard 64-bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b. As no other iris Liveness detection method has yet been reported on the public ATVS-FIr DB, for comparison, the second row of Table I reports the results obtained on this database by a self-implementation of the anti-spoofing method proposed. It may be observed that the proposed method not only outperforms the state-of-the-art technique, but also, as it does not require any iris detection or segmentation, the processing time is around 10 times faster.

2. Results: Iris-Synthetic: In this scenario attacks are performed with synthetically generated iris samples which are injected in the communication channel between the sensor and the feature extraction module (see Fig. 4). The real and fake databases used in this case are:

- **Real database:** CASIA-IrisV1. This dataset is publicly available through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA).2 It contains 7 grey-scale 320×280 images of 108 eyes captured in two separate sessions with a self developed CASIA close-up camera and are stored in bmp format.
- **Synthetic database:** WVU-Synthetic Iris DB. Being a database that contains only fully synthetic data, it is not subjected to any legal constraints and is publicly available through the CITeR research center.

B. Results: Fingerprints

For the fingerprint modality, the performance of the proposed protection method is evaluated using the LivDet 2009 DB [11] comprising over 18,000 real and fake samples. As in the iris an experiment, the database is divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set). The same QDA classifier already considered in the iris related experiments is used here.

1. Results: Fingerprints-Spoofing LivDet: The LivDet 2009 DB [11] was captured in the framework of the 2009 Fingerprint Liveness Detection Competition and it is distributed through the site of the competition.4 It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: i) Biometrika FX2000 (569 dpi), ii) Cross Match Verifier 300CL (500 dpi), and iii) Identix DFR2100 (686dpi). The gummy fingers were generated using three different materials: silicone, gelatine and playdoh, always following a consensual procedure (with the cooperation of the user). As a whole, the database contains over 18,000 samples coming from more than 100 different fingers. Some typical examples of the images that can be found in this database are shown in Fig.7, where the

material used for the generation of the fake fingers is specified (silicone, gelatine or playdoh).

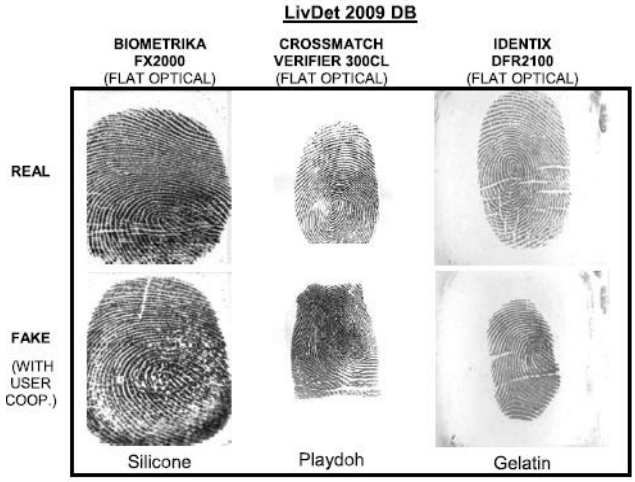

Fig.7. Typical examples of real and fake fingerprint images that can be found in the public LivDet09 database used in the fingerprint anti-spoofing experiments. The database is available at http://prag.diee.unica.it/ Liv Det09/.

C. Results: 2D Face

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB] which is publicly available from the IDIAP Research Institute. The database contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320 × 240 resolution webcam of a 13-inch Mac Book Laptop. The recordings were carried out fewer than two different conditions: i) controlled, with a uniform background and artificial lighting; and ii) adverse, with natural illumination and non-uniform background. Three different types of attacks were considered: i) print, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users; ii) mobile, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; iii) high def, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024×768. In addition, access attempts in the three attack subsets (print, mobile and high def) were recorded in two different modes depending on the strategy followed to hold the attack replay device (paper, mobile phone or tablet): i) hand-based and ii) fixed-support. Such a variety of real and fake acquisition scenarios and conditions makes the REPLAY-ATTACK DB a unique benchmark for testing anti-spoofing techniques for face-based systems. As a consequence, the print subset was selected as the evaluation dataset in the 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [12]. Some typical images (frames extracted from the videos) from real and fake (print, mobile and high def) access attempts that may be found in the REPLAY-ATTACK DB are shown in Fig.8.

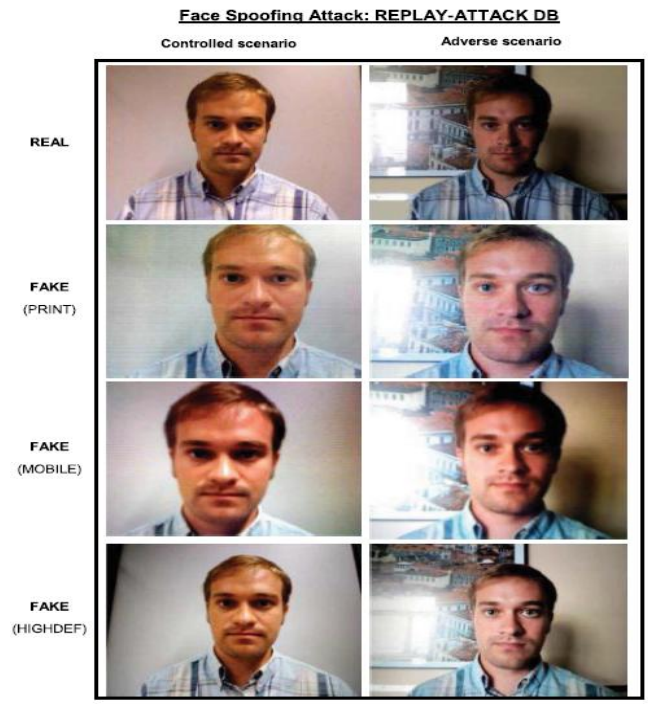

Fig.8. Typical examples of real and fake (print, mobile and high def) face images that can be found in the public REPLAY-ATTACK DB used in the face anti-spoofing experiments. Images were extracted from videos acquired in the two considered scenarios: controlled and adverse. The database is available at https://www.idiap.ch/ dataset/replayattack.

V. 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 levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. Multi- Biometric system is challenging system. It is more secure than uni-biometric system. In this paper studied about the three biometric systems that are face recognition, iris recognition, fingerprint recognition, and the attack on these three systems. Multi biometric system is used for various applications. And in future for making this system more secures adding the one more biometric system into this system and trying to improve the system. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this "quality-difference" hypothesis, in the present research work we have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing). For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts.

The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databases with well defined associated protocols. This way, the results are reproducible and may be fairly compared with other future analogue solutions. The present research also opens new possibilities for future work, including: i) extension of the considered 25-feature set with new image quality measures; ii) further evaluation on other image-based modalities (e.g., palm print, hand geometry, vein); iii) inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos); iv) use of video quality measures for video attacks (e.g., illegal access attempts considered in the Replay-Attack DB); v) analysis of the features individual relevance.

VI. REFERENCES

[1] Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian 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.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[3] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.

[4] 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.

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

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

[8] ISO/IEC 19792:2009, Information Technology Security Techniques Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[9] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[10] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[11] 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.

[12] 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.

Author's Profile:

K.Rakesh, PG Scholar, Dept of ECE, Farah Institute of Technology, Chevella, R.R.(Dt), TS, India,
Email: rakeshgoud4121@gmail.com.

Md. Rafeek Pasha, Masters Degree in Embedded Systems from JNTUH, Hydeabad and Graduated in B.Tech. ECE from Kakathiya Univercity, Warangal.He have a 6 Years Teaching Experience in Various Engineering colleges. Presently he works as a Associate Professor in Department of ECE. His Research interests include Embedded Systems, Microproceesor and Micro Controller and VLSI Design and Technology.

Anil Sooram, Graduated in B.Tech ECE in 2007 from JNTU Hyd. He received Masters Degree in M.Tech [ECE] from JNTUH University, Hyderabad. Presently he is working as Associate Professor in ECE Dept. in Farah Institute of Technology, Chevella, R.R. Dist Telangana State, India. His research interests include Wireless Communications, Embedded Systems. He has published 3 research papers in International Conferences, Journals. He has received best Teacher award from Farah Group.sss