Find Pretend Biometric Mistreatment Image Quality Assessments for Spoofing Detection

Ms. C. Nivetha Shrie[1], Dr. J. Vellingiri[2]
[1, 2] Department of CSE
[1, 2] Kongunadu College of Engineering and Technology, Trichy, TamilNadu, India

Abstract- *The Face, iris and fingerprint are most promising biometric authentication system that can be identify and analysis a person as their unique features that can be quickly extracted during the recognition process. To ensure the actual presence of a real legitimate trait in difference to a fake self-pretended synthetic or reconstructed sample is a important problem in biometric verification, which needs the development of new and efficient protection measures. Biometric systems are vulnerable to spoofing attack. A dependable and efficient countermeasure is needed in order to combat the epidemic growth in identity theft. The biometric detection and authentication deals with non-ideal scenarios such as blurred images, reflections and also faked by the other users. For this reason, image quality assessment approaches to implement fake detection method in multimodal biometric systems. Image quality assessment approach is used to construct the feature vectors that include quality parameters such as reflection, blur level, color diversity, error rate, noise rate, similarity values and so on. These features are stored as vector in database. Then implement Multi level Support Vector Machine classification algorithm to predict fake biometrics.*

Keywords- Multimodal biometrics, Image Quality, Spoofing attack, Fake detection, Feature Vector.

I. INTRODUCTION

Biometric is epidemically growing technology for automated acknowledgment or authentication of the uniqueness of a person using distinctive physical or behavioral characteristics such as fingerprints, face, iris, retina, voice, hand geometry and signature etc. To ascertain a personnel identity biometric relies on - who you are or what you do, as conflicting to what you remember -such as a PIN number or secrete keyword or what you use -such as an ID card. However, significant advances have been realized in biometrics, several spoofing techniques have been established to deceive the biometric systems, and the protection of such systems against attacks is still an open problem. Among the changed threats examined, the direct or spoofing attacks have provoked the biometric community to study the liabilities in contradiction of this type of duplicitous actions in performances such as the fingerprint, the face, the signature, or even the bearing and multimodal tactics. Spoofing attacks arise when a person tries to masquerade as someone else faking the biometrics data that are confined by the acquisition sensor in an attempt to avoid a biometric system and thereby aheadillegal access and advantages. Some type of falsely created artifact e.g. gummy finger, printed iris image, face mask, photograph, audiovisual, 3d Model or imitate the behavior of the actual user (e.g., gait, signature) etc. are used by the imposter to fake the biometric scheme. Consequently, there is an accumulative essential to detect such efforts of attacks to biometric systems. Liveness detection is one of the existing countermeasures in contradiction of spoofing attack. It aims at physiological signs of being in biometric illustration such as eye blinking, face expression changes, mouth movements, finger skin sweat, blood pressure, particular replication properties of the eye etc. by accumulating exceptional sensors to biometric system. Use of multimodal system is another beneficial countermeasure in contradiction of spoofing attack. Combining face or iris or fingerprint recognition by means of other biometric modalities such as bearing and language is perception of multimodal system. Indeed, multimodal systems are intrinsically more tricky to spoof than uni-modal systems. Multimodal systems are more complex than the single modal systems. The multimodal biometrics system illustrated in fig 1.

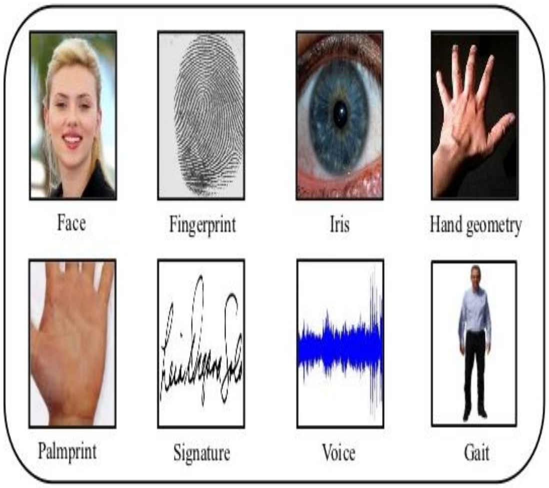

Fig 1: Multimodal Biometric system

Therefore, there is an increasing need to detect such attempts of attacks to biometric systems. In addition to spoofing attacks, there are other ways to attack system. If an impostor (user that does not have permission to access the system) has access to scores of the recognition system, the user can easily circumvent the system. However, this type of attack is more difficult to be performed. Since the acquisition sensor is the most vulnerable part (any user has easy access to this part of the system), spoofing attack techniques have become more attractive for impostor users.

II. RELATED WORK

Julian Fierrez, et.al [3] proposed a novel parameterization using quality events which is verified on a thorough liveness detection system. Image quality can be assessed by measuring one of the following properties: frame strength or directionality, veracity of the ridge-valley structure ridge continuity, ridge clarity, or estimated authentication performance when using the appearance at hand. A number of information are used to measure these properties: (i)angle information provided by the direction field,(ii) pixel intensity of the gray-scale image, (iii)Gabor filters, which represent another implementation of the direction angle, and power spectrum. (iv) Fingerprint quality can be assessed either examining the image in a holistic method, or combining the quality from local non-overlapped blocks of the image

J. Galbally, et.al [2] studies two cases for attack detection in faces. The first case study examines the efficiency of the Bayesian-based hill-climbing attack on an Eigen face-based system. The second study employs the previously found optimal configuration to attack a GMM Parts-based system. By using the same optimal configuration between studies we can determine if the performance of the attack is highly dependent on the values of the parameters selected.

Javier Galbally, et.al [6] presented liveness detection solutions for great importance in the biometric field as they help to prevent direct attacks those accepted out by means of synthetic traits, and very difficult to detect), improving this mode of level of the security provided to the user.

Jaime Ortiz-Lopez,et.al, [4] introduced a publicly existing database, procedures and a typical technique to guesstimate counter measures to spoofing attacks in face recognition systems. There seems to survive no consensus on best practices and techniques to be situated on attack exposure using non-intrusive systems. The number of publications on the subject is little. A missing key to this puzzle is the absence of typical databases to test counter-measures, trailed by a set of protocols to evaluate performance and allow for objective comparison.

Alessandra Lumini, et.al[5] proposed the image reconstruction approach exploits the evidence stored in the pattern to recreated a accurate image by guessing several aspects of the original unknown fingerprint through four processing steps. The attacking scenario measured in this work supposes that only the mandatory evidence stored in a Impression Particulars Record of the ISO template is available.

Lacey Best-Rowden, et al.,[13] implement face quality actions to determine when the fusion of resource sources will help boost identification accuracy. The quality actions are also used to assign weights to altered media sources in fusion schemes.

III. IMAGE DISTORTION ANALYSIS BASED FACE SPOOFING DETECTION

Biometrics provides tools and techniques based on behavior, physical and chemical traits to recognize humans in an automatic and a unique manner. The most common cues are fingerprint, face, iris, hand geometry, hand vein, signature, voice and DNA. Due to recent pattern recognition advances applied to face recognition, biometric systems based on facial characteristics have been largely applied to problems, including access control, surveillance and criminal identification. At the same time that significant advances have been achieved in biometrics, several spoofing techniques have been developed to deceive the biometric systems, and the security of such systems against attacks is still an open problem.

Spoofing attacks occur when a person tries to masquerade as someone else falsifying the biometrics data that are captured by the acquisition sensor in an attempt to circumvent a biometric system. Security is main concern for today’s scenario. A high level industry uses passwords like thumb, face, voice, iris, etc. So lots of security systems are available. But not so reliable. Here the developing system which is very precise and reliable. The system has two stages which is rooted system. Even if any stage is split incorrectly, unofficial entry will be identified. Existing framework analyzed image distortion analysis approach to identify the fake faces. IDA includes specular reflection, chromatic moment, blurriness and color diversity). Specular Reflection Features analyze illumination of the images.

Then blurriness is measured based on the difference among the actual input image and its blurred version. Then convert the normalized facial image from the RGB space into the HSV (Hue, Saturation, and Value) space and then calculate the mean, deviation, and skewness of each channel as a chromatic feature. Finally analyzed color reproduction loss in input images.Feature vectors are then fed into multiple SVM classifiers. The proposed scheme is to achieve a more stable face spoof detection performance.

IV. MULTIMODAL BIOMETRIC SYSTEM USING IMAGE QUALITY ASSESSMENT

To ensure the genuine presence of a real rightful trait in difference to a fake self-manufactured imitation or recreated sample is a major trouble in biometric verification, which requires the improvement of new and effective security measures. Background to fingerprint detection describes the biometric use of fingerprints scanning is also done by biometric tools. The objective of proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a speedy, user friendly and non-intrusive manner, through the use of image quality assessment. Image quality assessment divided into full reference and no reference methods.

Full-reference (FR) IQA methods rely on the accessibility of a clean undistorted reference image to estimate the quality of the test sample. Full reference IQA contains three types of measurements such as error sensitivity measures, structural likeness measures and information theoretic measures. No-Reference IQ Measures does not require of a reference sample to regulate the quality level of an image. This measurement contains such as distortion measures, training based measures and natural scene statistics measures. Then implement image fusion approach to combine all biometric features that includes iris, face and fingerprint features. And finally QDA based classification technique can be implement to finalize whether image is real or fake.

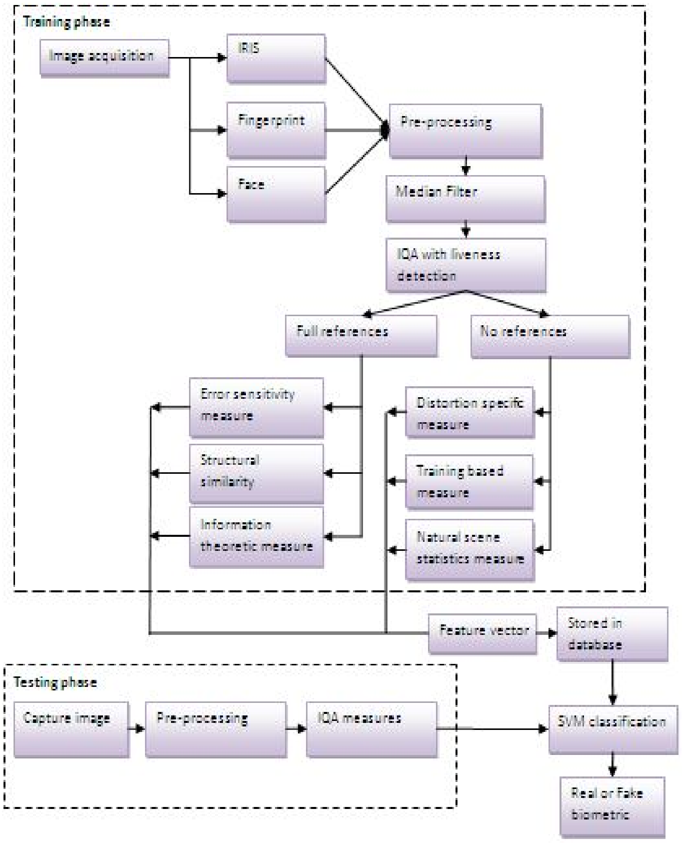

Fig 2: Proposed Framework

V. RESULTS AND DISCUSSION

5.1 Fingerprint Recognition System:

Every fingerprint of each person is considered to be distinctive, Even the Twins also contain different fingerprint. Fingerprint recognition is the most conventional biometric recognition method. Fingerprints impressions have been used from long time for identifying individuals. Fingerprints contain of ridges and furrows on the surface of a fingertip. Now fingerprint identification system is used in iphone, there are numerous areas where the fingerprint recognition system used.

But attackers attack on fingerprint recognition system. Attackers first detain real fingerprint then they make fake fingerprint by using silicon, gelatin and playdoh and try to access the system.

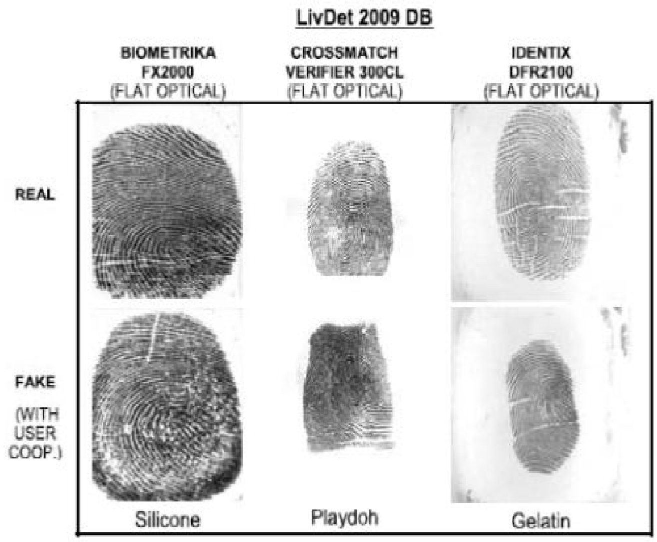
LivDet 2009 DB
BIOMETRIKA FX2000 (FLAT OPTICAL)
CROSSMATCH VERIFIER 300CL (FLAT OPTICAL)
IDENTIX DFR2100 (FLAT OPTICAL)
REAL
FAKE (WITH USER COOP.)
Silicone
Playdoh
Gelatin

Fig 3: Fingerprint datasets

5.2 IRIS Recognition System:

Iris recognition is a computerized method of biometric identification which uses numerical Typical recognition methods on video images of the irises of an individual's eyes, whose multifaceted random patterns are distinct and can be seen from some distance. Iris cameras perform detection of a person’s identity. The iris examines practice start to get approximately on film. It combines computer vision, statistical inference, pattern recognition and optics.

The iris is the highlighted ring around the pupil of every human being and like a snowflake; no two are the same. Each one is distinctive. An attack on the iris is not so easy but how to attack on the system is as shown below. To create a fake iris is of three step.

1) Novel images are capture for a better quality, then
2) They are printed on a dissertation using a commercial printer
3) Printed images are presented at the iris sensor.

The iris datasets are gathered from CASIA database and then images in fig 4.

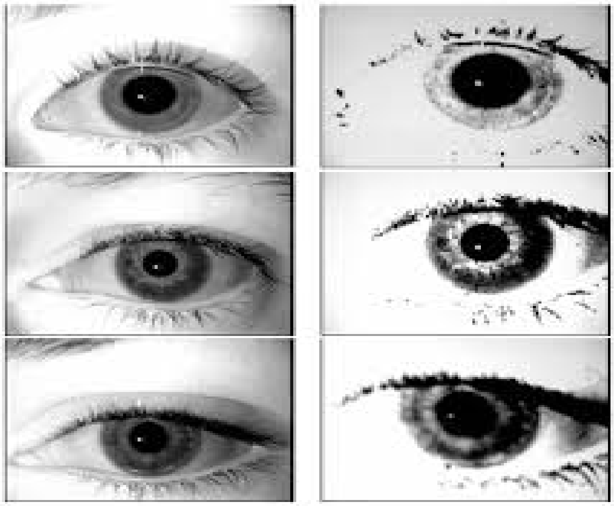

Fig 4: IRIS datasets

5.3 Face Recognition System:

The most acceptable biometrics is Face recognition, because it is one of the most general methods of documentation that humans employ in their visual interactions and acquisition of faces. The face acknowledgment systems make different among the contextual and the face. It is most substantial when the system has to categorize a face within a multitude. The system then creates use of a person's facial features – its valleys and heights and milestones and indulgences these as lumps that can be equated and plannedin contradiction of those which are stored in the system's database.

There are about 80 lumpsencircling the face print that makes use of the system and this includes the eye socket depth, jaw line length, distance between the eyes, cheekbone shape, and the size of the nose. It is very challenging to develop this recognition technique which can recognize the effects of facial expressions, age, slight variations in the imaging environment.

Attack on the face recognition system is shown in the following figure in that figure fake and genuine image are shown and that images are discover out due to different method of face recognition. In face recognition system fake users attack on system by detaining the picture to the mobile devices or camera. And try to authenticate. Possible scenarios in face database in fig 5.

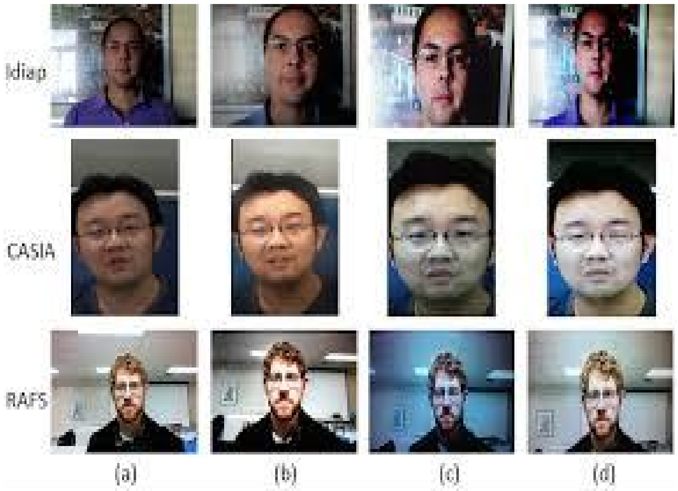

Fig 5. Face datasets

The performance of the system is measured using False Fake Rate and False Genuine Rate. Compare to existing system, our work provide reduced number of FFR and FGR. The graphical representation is in fig 6.

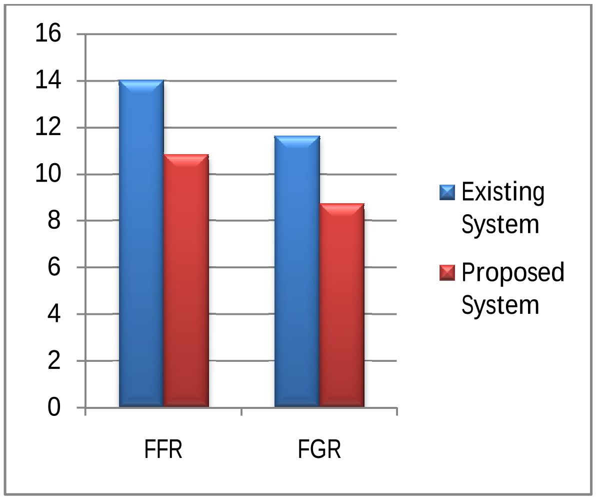

Fig 6. Performance evaluation

VI. CONCLUSION

Image quality assessment is used to detect the fake biometrics. Due to Image quality dimensions it is simple to find out real and fake users because fake identities often have some different features than original it always enclosed different luminance and color levels, general artifacts, extent of evidence, and magnitude of sharpness, found in both type of images, natural appearance or structural distortions. Multi-Biometric system is challenging system. It is more secure than uni-biometric system. This technique can analyze multi modal biometric system with image fusion approach. Implement image fusion approach to combine both biometrics (fingerprint and iris, iris and face, face and fingerprint). So we can implement image fusion technique to fuse all biometric features as in one image format. This method is used to improve security in database level. The dynamic IQA is a very promising technique in making recognition system more robust against fake based spoofing attempts to provide alert system to intimate mobile message to person who are authorized by the system.

REFERENCES

[1] 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.

[2] T. Matsumoto, “Artificial irises: Importance of vulnerability analysis,” in Proc. AWB, 2004.

[3] 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.

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

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

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

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

[8] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from asingle image with sparse low rank bilinear discriminative model,” in Proc. ECCV, 2010, pp. 504–517.

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

[10] 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.

[11] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. CVPR Workshops, 2012, pp. 124–129.

[12] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925–929.

[13] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157, Dec 2014.

[14] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE BIOSIG, 2012, pp. 1–7.

[15] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," in Proc. IEEE BTAS, 2013, pp. 1–6.

[16] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, 2011, pp. 436–441.

[17] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IJCB, 2011, pp. 1–7.