" A CASE STUDY ABOUT FAKE IDENTIFICATION IN BIOMETRIC SYSTEM THROUGH IQA AND RESEARCH AND RESULT ANALYSIS ABOUT THE FACE, FINGERTIP AND IRIS IMAGES."

Abhijit Magdum1, Prof.P.P.Belagali2
Student1, Professor2,
Department of Electronics1, Department of Electronics2,
Dr.J.J.M.C.O.E. Jaysingpur, Maharashtra, India1.
Dr.J.J.M.C.O.E. Jaysingpur, Maharashtra, India2.

Abstract: Biometric systems are increasingly used for identity verification due to their reliability and ease of use. However, these systems are vulnerable to presentation attacks (a.k.a. spoofing), where a fake biometric sample (like a printed face image or silicone fingerprint) is presented to the sensor. This paper explores the use of Image Quality Assessment (IQA) techniques to detect such fake attempts. IQA methods analyze biometric image characteristics to distinguish between live and spoof samples. Various image features such as blurriness, texture, colour variance, and noise artifacts are evaluated using algorithms and machine learning techniques to enhance system reliability. Fake identities always have some different feature than original such as sharpness, different colour, information quality etc. In this paper, liveness detection method is used. Which provide a very good performance and low degree of complexity Also quality of Image is using two methods Full- Reference (FR) and No-Reference (NR). This image quality assessment (IQA) method is suitable for real time application which has been used for very low complexity.

1. INTRODUCTION

The terms ―Biometric system related to the technology. That means bio (life) and metric (measure).It analyse the human characteristics, such as face, iris, hand, fingerprint etc. This system also recognizes person according to their characteristics. The physiologic Characteristics are related to the size of the organs for example face, iris, retina, etc. and Behavioural characteristics are related to behaviour of person [4] i.e. Voice, signature, keystroke etc. Biometric system divides in sensing, feature extraction, and matching modules. In this paper, Image Quality Assessment (IQA) is used to determine the real and fake image. which depend on multi attack and multi biometric protection method. IQA is able to perform under different biometric system and spoofing scenarios. It also provides very good protection level again certain Non-spoofing attacks. Image quality assessment consists of two methods such as subjective and objective method. Subjective method gives best results, related to the human vision but this method is more expensive and costly. Objective method is used to determine the quality of image depending on the point of view of original image.

Image quality measurements are used to design and implement a system that provides security against the fake image by using IQA technique. Fake identities always have some different feature than original image (real).The IQA measurement of structural distortion should be a good approximation. So the efficient and accurate measures should certainly enhance their applicability in real world application.

2. SECURITY OF BIOMETRIC SYSTEM

In the security level of biometric system is improved by first detecting the fake image and then removes that image. It is mainly used in identification and access control on their behavioural and physiological category. For example Signature scan is used to measure the speed and pressure stroke. Voice measure the sound wave, Retina measures the unique characterize of blood vessel and vein pattern, also it include Key stroke, face, iris and fingerprint etc.

Internal Structure of biometric system This paper introduces, a Software base multi attack protection method which is based on various biometric modalities such as iris, face, finger image. The Biometric system consists of two models such as verification and identification mode. The first mode is the verification also it called authentication. In verification mode it performs one to one comparison between captured.
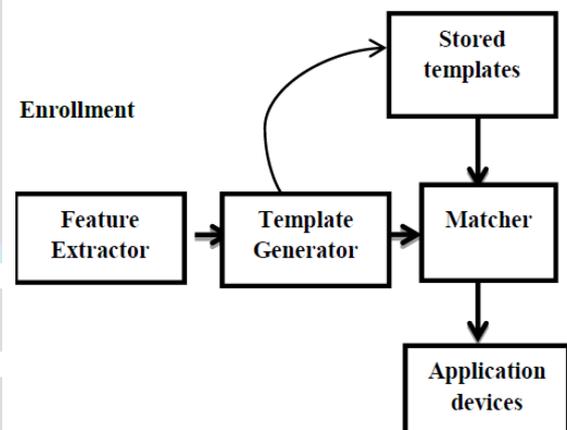

Fig-2: Basic Block Diagram of Biometric In fig.2 shows feature extractor module is used to correct the feature and extracted from the source.[5][6] During enrollment process,[3] biometric information is captured and stored in templates, from a single source. The data base, card, or both are stored in templates .During matching module the stored template is passed to the matcher, and compare with existing templates. The matching program analyzes the template from the individual input source.

3. IMAGE QUALITY ASSESSMENT METHOD

In image processing system, The Quality Assessment (QA) of an image measures its reduction at different stages such as acquisition, compression, transmission, and reproduction. The quality of image depends on by environmental disasters such as adverse brightness, noise, blur. Predicting quality should be accurate, consistent and

monotonic for a good image quality measurement (IQM).image quality measurement (IQM) is categories into four general methods such as performance, complementarily, complexity and speed. Image quality approaches for good performance and high computation load which has been considered. The evaluation of image quality assessment further classified into two devices such as subjective and objective method as shown in fig2. The Subjective experiment is used for viewing distance, display device, lighting condition, subjective mood, and vision ability. The main approach of Objective image quality assessment is used for mathematical tool which are capable to an image quality accurately. Objective quality assessment method can be classified into two main types. The first type is Full-reference and last is No-reference image. The References image of perfect quality is fully available in FR-IQA method. The FR IQA methods are used for gray scale image in full references including (MSE, PSNR, SNR, SC, MAS, and MAMS) etc. This FR-IQA Method used for colour image. It has different dynamics range NR-IQA method used colour image it has different dynamic range.NR-IQA Method in which don't have access to the references image also determined the quality level of image.
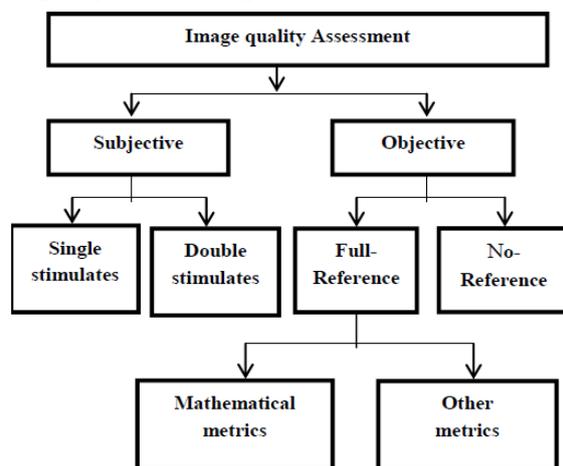

Fig-3: Classification of IQA method

4. LITERATURE SURVEY

I. "Javier Globally, Sebastian Marcel, Member, and Julia Fierez". IEEE Transactions on image processing, vol.23, no 2, February 2014.

 Image Quality Assessment for Fake Biometric detection:

 This paper proved, image quality assessment (IQA) technique used in fake biometric detection system also provide very good performance again multi-attack (non-spoofing).

 It used for multitask and multi biometric protection method.

 This paper has used liner discriminate analysis (LDA) and quadratic discriminate analysis (QDA) for iris and fingerprint modality.

II. J.Galball,J.Ortizlopez,J.Fierrez.andJ.Ortega-Garcia"inproc.5thIAPR Mar/Apr.2012

 Iris Liveness Detection Based on Quality Related Features:

 In this paper, new parameterizations based on Quality related measure. This is used in software for iris liveness detection.

– Hough transform used to detected iris from the background.

 Image quality measure IQM is used for high frequency to detected fake image. Real sample will different from fake image.

 It is also tried to detected external element by using feature extraction module that are eyelid or eye lashed.

III. "Zhou Wang, student Member, IEEE and Alan C.Bovik"fellow, IEEE signal processing letter, March.

 Universal Image Quality Index:

 In this paper, there are various images processing applicable for easy to calculate the error. In Image quality index there are combination of three factors used that are contrast distortion, loss of correlation and luminance distortion.

 In contrast distortion, will measuring the similarity of contrast and dynamic range will be [0, 1].

 Loss of correlation will measures the degree of liner correlation between _x' and _y'.It's dynamic range will be [-1, 1].

 In Luminance distortion dynamic range will be [0, 1], it will measures mean luminance in between _x' and _y'.Traditional method of error calculated the quality of image.

IV."SNEHAS,Mrs.R.INDUMATHI", IJETS.ISSN (P):2349-3968 volume 2 Is March-2015.

 Fake Biometric Detection Using Improved Feature in Image and Dempster-Shafer Method:

 In this paper, software based multi biometric and multi attack protection method base on image quality assessment method used to identify whether image are real and fake.

 It also on adding livens assessment that provides good performance and low degree of complexity. Various biometric system used in iris, fingerprint, face and hand palm.

 This project used for Dempster –Shafer theory in fake identification.

V.RJayavadivel,Prabhushankar, S.*Rajesh*",ISSN (online):2319-8753 Vol.4, ISSUE7 July 2015.

☐ **Statistical Image Quality Assessment for Fake Biometric Detection Based on SVM, Application to Iris and Face Recognition:**

☐ This paper used (IQA) image quality assessment play an important role for the performance of biometric system including iris and faces image. Quality of data assessment is a key word in order to the application of Iris and face biometric.

☐ Classified technique of this project SVM support vector machine is used for training and testing the iris and face image.

☐ The real time work on iris and face image which are applicable for biometrics system that should be done by efficient.

VI. **"IsmailAvcibas, Member, IEE, Nasir Member, IEEE; transactiononprocessing,vol.12, N2February 2003.**

☐ **Steganalysis Using Image Quality Metrics:**

☐ This paper is based on the factor that hiding information in digital media which requires alterations of the signal. That introduces some forms of image quality metric based on distance between an unmarked image and its filtered image.

☐ In image quality assessment can be used to describe between cover image and stego images.

☐ In Steganalysis used for low pass filtering which is based on Gaussian surface. Image quality metric based on distances between an unmarked image and its filtered version.

6. CONCLUSION

From above Literature survey, we can conclude that important element in Quality of image metrics by improving in robustness of large real word of biometrics system, they are simple fast non-intrusive user friendly and cheap. In additional to verify the competitive performance they show multi biometrics and multi attack characteristics. They are also used in liveness detection technique refer to the ability to detect particular properties such as face, finger, iris etc. In this paper, we are going to implemented method to analyze different database, acquisitions, condition and different attack of scenarios. For remove the noise and blur image we used Low pass Filter to improve the quality level of image by using image quality assessment technique (IQA).In our project we detected various biometric application such as Iris, Face, Finger. This technique are used in ATM machine, Banking sector, Airport, Railway, Home appliances in fake biometric detection system.

7.REFERENCES:

[1]. Javier Galbally, Sebastian Marcel, Member, IEEE, and Julian Fierrez, February 2014 Image

[2]. CASIA Face Anti-Spoofing Database

[3]. "Image Quality Assessment for Presentation Attack Detection" – IEEE Transactions

[4]. MSU Mobile Face Spoofing Database Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint.

[5] Galbally, J., Marcel, S., & Fierrez, J. (2014). Image Quality Assessment for Fake Biometric Detection. IEEE Transactions on Image Processing.

[6]. OpenCV and Scikit-learn documentation

[7]. Zhang et al., "A survey on anti-spoofing methods," 2021

[8]LivDet Competition Reports (2017–2021)

[9] Zhang, Z., et al. (2021). Face Anti-Spoofing Using Deep Learning and IQA Features. Pattern Recognition.