SVM Classification For Fake Biometric Detection Using Image Quality Assessment: Application to iris, face and palm print

P. Pravallika
Department of ECE
University College of engineering, JNTUK
Kakinada, India
Pravallika0593@gmail.com

Dr. K. Satya Prasad
Department of ECE
University College of engineering, JNTUK
Kakinada, India

Abstract— **The increasing interest in the evaluation of biometric systems security is an important issue to be considered. The different threats called direct or spoofing attacks where in these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behavior of the genuine user , to fraudulent access of the biometric system have motivated to new efficient protection measures. In this paper, we present a novel software-based fake biometric detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The use of image quality assessment for liveness detection is motivated by the assumption 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. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using general image quality features extracted from one image to differentiate between real and fake samples. This proposed work enhances the security of biometric recognitions, by using the liveness detection through image quality assessment and by fusion of multiple biometric traits. The SVM classifier is used for differentiating between the real and fake samples.**

Keywords—liveness detection; real; fake; image quality assessment; biometric system; spoofing attacks

I. INTRODUCTION

The word "biometrics" is derived from the Greek words as bio means “life” and metric means “to measure”.

BIOMETRICS refers to the automatic identification of a person. A biometric is a unique, measurable characteristic or trait for automatically recognizing a human being[3]. This technology can be used to protect and secure our valuable information and property. It is based on the biometric classification as physiological / behavioral characteristics. In this method of identification the person to be identified is required to be physically present at the point of identification; identification based on biometric techniques counters the need to remember passwords or smart cards.

The usage of computers in information technology has been increased, so it is necessary to secure access to sensitive or personal data. Instead of PINs, biometric techniques can prevent unauthorized access to fraudulent use of smart cards, desktop PCs, workstations, and ATMs, cellular phones, computer networks. The disadvantages in PINs, passwords, tokens are they may be forgotten or shared or stolen. Thus biometric systems of identification are more secured.

In recognition the system requires to search many stored sets of database characteristics and pick the one best match with the unknown individual. There are various types of biometric systems are being used for real–time identification; the popular among them are face recognition and fingerprint matching. There are also other biometric systems as iris and retinal scan, hand geometry speech, gesture recognition [1].

A biometric system is a pattern recognition system, which is used for personal identification by determining physiological or behavioral characteristics possessed by the user. Biometrics are often classified as physiological and behavioral characteristics. Physiological characteristics are related to the physical shape of the body. Examples such as DNA, palm print, hand geometry, iris recognition, retina and odor/scent, fingerprint, palm veins, face recognition, Behavioral characteristics are related to the behavior of the person, including but not limited to typing ,rhythm, gait, and voice.

There are levels of security from the most basic to the most robust with biometrics being the most secure:

- Something you *have* - such as an ID with a photograph
- Something you *know* - such as a password or PIN.
- Something you *are* - such as fingerprints, face scans iris, voice.

Biometric technology used in many fields as Government applications such as e-passports, ID cards, and border control. However in the past few years the quality of biometric

measurement has become a big issue. Recently, the interest in the biometric systems security has led to the creation of very diverse initiatives on this major field of research. Biometrics can be fraudulently accessed hence it is necessary to offer security to those systems. Besides the advantages, biometric systems have some drawbacks, including the lack of secrecy, the fact that a biometric trait cannot be replaced. Our devices are now a day's storages of personal, professional, commercial, and other kinds of information. Hence it is essential to be kept confidential and secured from fake traits.

Fake biometrics means, the user creates the fake identities like fingerprint, iris on printed paper or uses synthetic or gummy prints for identification. In fake biometrics the user first captures the identities of the real user and then create the fake sample for identification[1]. There are many methods to detect the fake users and hence these biometric systems are more secure, because every person will have different characteristics for identification. A multi biometric system uses the multiple source of information for recognition of person. Multi biometric system is more secure than single biometric system.

The paper is organized as follows. In Section II, the Liveness Detection, image quality assessment and quality measures are reviewed. The image fusion and proposed block diagram is described in Section III. The SVM classification and its algorithm are introduced in Section IV . Conclusion and results are given in Section V.

II. Liveness Detection Using Image Quality Assessment

A. Types of Attacks

There are different fraudulent access attempts using various synthetic traits and gummy prints and printed iris, face on papers. Basically the types of attacks[7] are classified as

- **DIRECT ATTACKS: -**This attacks are done with artificial biometric samples, e.g. gummy fingers and printed iris etc., In this type of attacks no exact knowledge regarding the system is wanted. Moreover, the attack is carried out in the analog domain, outside the digital restrictions of the system.

- **INDIRECT ATTACKS:** In this type of attacks the impostor needs to have some extra information about the internal operational of the system and, in some cases, physical access to some of the application mechanism is also needed.

Different levels of attacks against a biometric system are

- Artificial biometric traits may be presented at the sensor.
- Illegal data may be submitted to the system.
- The feature template may be changed by some program.
- Matcher may be changed with that gives high scores.

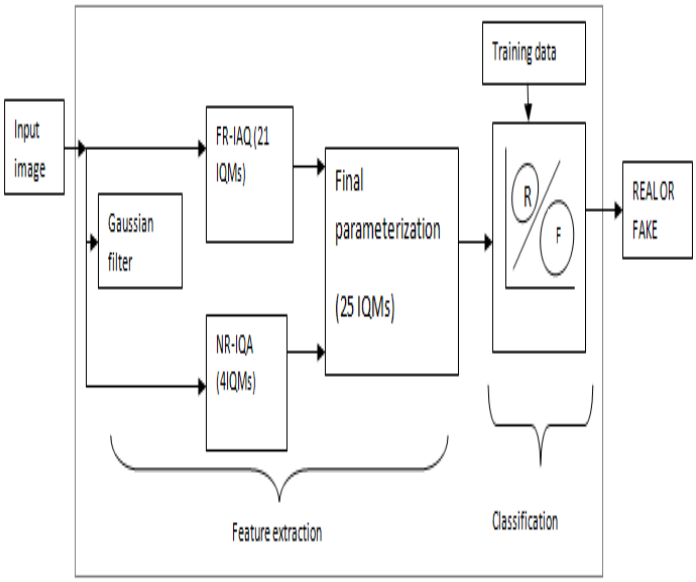

Fig.1. General diagram of the biometric protection method based on Image Quality Assessment (IQA)

B. Liveness Detection

As it is necessary to enhance the security for biometric systems from various attacks. Liveness detection is generally a 2 class classification among fake and real. The various previous methods used are multiple biometrics and physiological features to distinguish between real and fake etc. This method uses only input image related features against trait specific features so it needs only one image for acquisition which is an advantage. The two types of liveness detection methods are

- *Software-based techniques:* In this type the fake trait is detected by using the features from the image itself rather than the trait features.
- *Hardware-based techniques:* In this type it adds some device to the sensor in order to detect some properties of a living trait like, fingerprint sweat, blood pressure, or specific reflection properties of the eye.

Liveness detection methods should have the requirements as follows:

- User friendly
- Fast
- Low cost
- High performance

The two methods have advantages and disadvantages over the other and, so the combination of both would be more advantageous and high protection security approach. The advantages of hardware-based methods have high fake rate detection and software based methods are less expensive and less intrusive.

C. Image Quality Assessment

We use image quality assessment for liveness detection based on the statement that : " It is assumed that a fake image captured during the attacks will have different quality from the real image acquired during normal operation."[1] The quality differences may include difference in color and luminance levels, general artifacts, quantity of information, sharpness, structural distortions or natural appearance. The fake sample will lack the properties found in original images. The usage of IQMs for image quality properties allow detection of quality differences between real and fake samples.We extract some general image quality measures, for simplicity system takes only one image and extract quality measuring features for the image itself rather than trait specific features. This method does not need any other iris detection, face extraction and finger print minutiae extraction for processing the features. This method reduces the computational load to the system and these quality measured features are used to distinguish between real and fake samples. IQMs are classified according to four general criteria.

- Performance -Tested for good performance for various applications
- Complementarity - The complementary properties like sharpness, structure are used to make system general as possible.
- Speed – it is related to complexity and it should not take long time for the response.
- Complexity- Features should be less complex to reduce computations.

There are two types of image quality measures which are Univariate or No reference measures and Bivariate or Full reference image quality measures.

Univariate measures- These measures the quality of the target image without using any reference image.

Bivariate measures- These measures need a reference image to identify the quality of an image.

A. Full Reference IQ Measures

In full reference IQ measures the comparison between input and reference image is used. The full reference IQM are classified as:

- 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: Natural way to measure the quality of an image is to Determine the error between the distorted & reference image. It measure the errors i.e signal

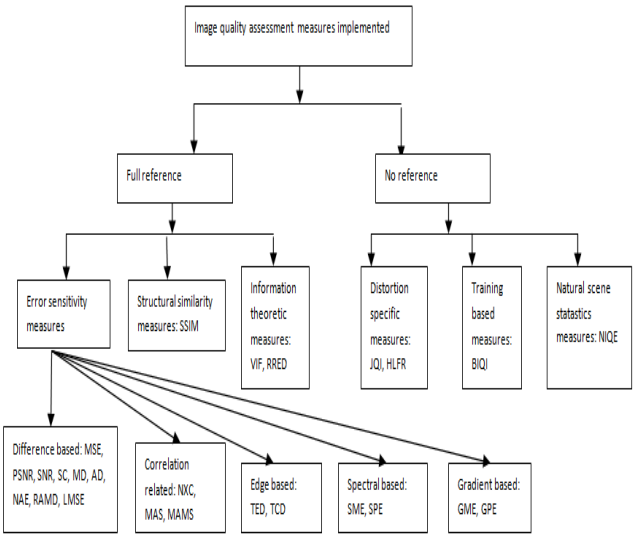

Fig.2. Classification of the image quality measures implemented in the work

difference between the input and reference images (filtered input image).

a) Pixel Difference Measures

Pixel difference measures compute the distortion between input & reference image on the basis of their pixel wise difference. Pixel wise difference measures include: Mean Squared Error(**MSE**), Peak Signal to Noise Ratio (**PSNR**),Maximum Difference(**MD**), (**SNR**) ratio. Structural Content (**SC**), Correlation Quality (**CQ**), Average Difference (**AD**), Normalized Absolute Error (**NAE**) ,Root Mean Square Error (**RMSE**), Peak Mean Square Error (**PMSE**)Mean Absolute Error(**MAE**), R-Averaged Maximum Difference (**RAMD**) and Laplacian Mean Squared Error (**LMSE**),Error Root Mean Square Contrast(**ERMSC**).

b) Correlation Based Measures

It measures the similarity between the two digital images. The three correlation based measures are: Normalized cross correlation (**NXC**), Image Fidelity (**IF**), Mean angle similarity (**MAS**), Mean angle magnitude similarity (**MAMS).**

c) Edge Based Measures

These measures make use of local and global gradient information to provide boundaries to regions of interest. Edge based measures include: Total Edge Difference (**TED**) and Total Corner Difference (**TCD**).

d) Spectral Distance Measures

In these, the distortion functions obtained from the complex Fourier spectrum of images are considered. In this two spectral distance measures are considered: the Spectral Magnitude Error (**SME**) and the Spectral Phase Error (**SPE).**

e) Gradient Based Measures

We use the gradient similarity to measure the change in contrast and structure in images. Two simple gradient-based features included are: Gradient Magnitude Error (**GME**) and Gradient Phase Error (**GPE**).

2. Structural Similarity Measures

Natural images are highly structured and their pixels exhibit strong dependencies. Structural Similarity Index Measures **(SSIM)** index is a single-scale approach.

3. Information Theoretic Measures

one important aspect of information theoretic measures is the "information fidelity" . Information fidelity criteria is to relate visual quality to the amount of information that is shared between the images being compared. Two information theoretic measures are: the Visual Information Fidelity (**VIF**) and the Reduced Reference Entropic Difference index (**RRED**).

B. No Reference IQ Measures

A Univariate measure uses a single image as input image. The Univariate IQM are classified into three,they are:

1. Distortion-Specific Approaches

Distortion specific means that the algorithms can assess the quality of an image under the assumption that the image is affected by distortion X, where X could be JPEG compression, blur and so on. It relay on visual quality loss by specific distortion. Two distortion specific approaches used are: JPEG Quality Index (**JQI**), High Low Frequency Index (**HLFI**).

2. Training-Based Approaches

Here clean and distorted images are used to train the model. Then image quality features are extracted from the test image in order to compute the quality score. Training based approach used here is Blind Image Quality Index **(BIQI).**It identifies the likeliest distortion in the image and quantifies this distortion using an NSS-based approach.

3. Natural Scene Statistic Approaches:

Natural image quality evaluator **(NIQE)** is the natural scene statistic approach used in this work. Natural image quality evaluator is completely blind image quality analyzer, without training any human rated distorted images it only uses measurable deviations observed in natural images.

III. IMAGE FUSION

In computer vision , Multisensory **Image fusion** is the process of combining relevant information from two or more images into a single image. The resulting image will be more informative than any of the input images. Several situations in image processing require both high spatial and high spectral information in a single image. However, the instruments are not capable of providing such information either by design or because of observational constraints. One possible solution for this is data fusion.

The fusion can be classified into two classes, as fusion before matching and fusion after matching shown. For fusion before matching, the information is integrated from multi biometric sources and fusion is done at the sensor level and fusion at the feature level. Whereas , fusion after matching is divided into fusion at the match score level and fusion at the decision level.

A. Fusion Before Matching

- **Sensor Level Fusion:** In this fusion level , the raw data from the sensor images are combined together. The source of information is contaminated by noise and background clutter .This level of fusion can be done in two cases as data of the same biometric trait is obtained using multiple sensors; or data from multiple snapshot of the same biometric traits using a single sensor.
- **Feature level fusion** : In this feature level fusion, different feature vectors extracted from multiple biometric sources are combined together into a single feature vector. Hence, only few researchers have focused on the feature level scheme compared to the other levels of fusions such as score level and decision level

B. Fusion Before Matching

- **Score level fusion :** In this score level fusion, the matched outputs from multiple biometrics are combined together to improve the matching performance in order to verify or identify of an individual. This is the popular approach in the biometrics due to its simplicity in score collection.
- **Decision level fusion** This fusion is similar to score-level fusion, except that the scores are replaced with match/non-match decisions.

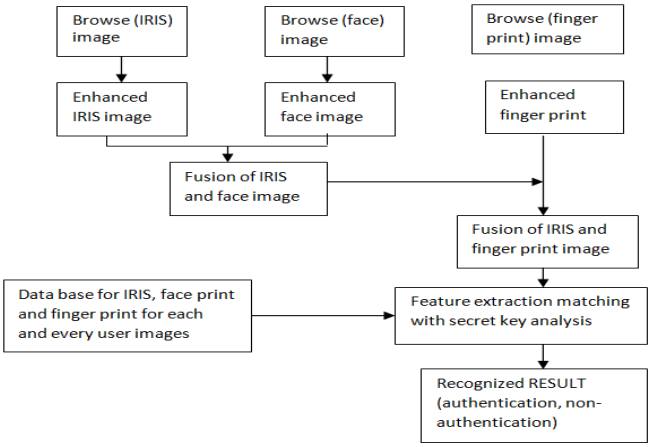

Fig.3. Block diagram explaining the proposed work

The block diagram above in Fig 3 shows that the input image is first browsed and it is enhanced for the noise removal every time. The fusion of enhanced iris and face images is done by using some fusion technique then the fused image is again applied for fusion with the enhanced palm print image. Then the final image obtained is the fusion of all three iris, face and palm print images. The image quality features are taken from the final fusion image and its is checked with database every time for the matching to classify as authenticate or non authenticate person.

IV . SVM CLASSSIFICATION

The **support vector machines** are supervised learning models with its associated learning algorithms that analyze data and recognize the patterns, this SVM algorithm [2] is used for classification . It is given with a set of training examples, each belongs to either one of the two categories as real or fake, this model assigns some new examples into one or the other category. This SVM model represents the examples as points into the space, and they are mapped so that every example is classified into two classes separated by a gap.

SVM classifier can also deal with the non linear classification problems along with the linear classification by using the kernel trick.

Algorithm For SVM Classification[2]

Training Algorithm:

Step 1: Read the Input training Images from the database.
Step 2: Obtain the Image Quality Assessment Measures as No reference and Full reference from the training images.
Step 3: Combine all the obtained image Quality Measure as a IQA feature.
Step 4: Make a Target for Svm classification.
Step 5: Svm classifier trained with two classes as real or fake**.**

Testing Algorithm:

Step 1: Read the Test Images from the database.
Step 2: Obtain the Image Quality Measures from the test images.
Step 3:Combine all the Quality Measure as a feature template.
Step 4: Feature template is now compared with the trained feature values using SVM classifier.
Step 5: Finally the output is given that the test image is fake or real.

IV. RESULTS AND CONCLUSION

The biometric systems against different types of attacks have become an active field of research. As there are many users who try to attempt for fraudulent access it is necessary to provide security for biometric systems. The "*quality-difference*" hypothesis, in the present work uses general *image* quality assessment and fusion of multi biometrics as protection tool against different biometric attacks. The image quality measures are used with simple classifiers to detect real and fake access.

The results for the authenticate and non authenticate persons are classified using the image quality features from the fusion image are given as follows:

Fig.4. Result showing the person as authenticate

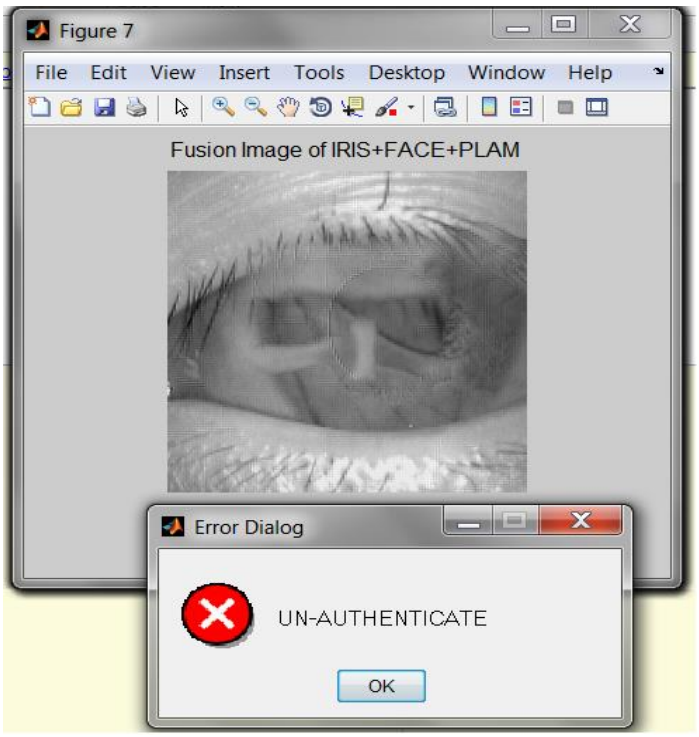

Fig.5. Result showing the person as un-authenticate

TABLE I. RESULTS WITH SVM AND OTHER CLASSIFIERS

	IRIS			FACE			PALMPRINT		
	FGR	FFR	HTER	FGR	FFR	HTER	FGR	FFR	HTER
IQA with LDA	0.50	5.2	2.85	1.6	2.4	2	15.2	17.1	16.15
IQA with QDA	0.30	4.3	2.3	3.4	4.2	3.8	13.0	16.1	14.55
IQA with SVM	0.11	2.2	1.15	1.1	2.2	1.65	9.2	10.1	9.65

There are many classifiers like LDA, QDA to train and classify the samples but svm classifier is efficient and accurate. The above table shows the results with the svm classifier.

There are also various possibilities for the future work as we can include more image quality parameters and can extend this application for vein print, hand geometry, fingerprint etc.

References

[1] Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierre "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] R.Jayavadivel, B.Prabhushankar , S.Rajesh " Statistical Image Quality Assessment for Fake Biometric Detection Based on SVM Classification: Application to Iris, and Face Recognition*"International Journal of Innovative Research in Science, Engineering and Technology* "Vol. 4, Issue 7, July 2015

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

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

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

[6] 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.

[7] 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.

[8] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *J. Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.

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

[10] Biometrics Institute, London, U.K. (2011). *Biometric Vulnerability Assessment Expert Group* [Online]. Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-bvaeg.html.

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

[12] J. Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology*, vol.14, No.1, pp. 21 – 30, 2004

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