ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

Advanced Image Quality Measures Algorithm for Biometric Detection

Reshma S.R[1], **Shally K**[2]

PG Scholar, Dept of Electronics and Communication, Mohandas College of Engineering[1]

Assistant Professor, Dept of Electronics and Communication, Mohandas College of Engineering[2]

Abstract: Security is major concern for today's scenario. Inorder to meet the growing needs of security, several researches are done to provide more privacy to the user. In this paper, an authentication method using image quality assessment is used. There are various biometric methods are available, sclera vein recognition, iris recognition, face recognition etc. Since there are so many techniques are available they are not so reliable. Nowadays biometrics systems are attacked by using fake samples. Since biometrics are concentrated on their accuracy it suffers from the innate disadvantage of time consumption during enrolment and verification process. Even the sclera patterns can be faked to access the biometric systems. Inorder to make the system more efficient, image quality measures are used to detect the input image as real or fake. The proposed method extract 25 image quality measures and confirms whether the input biometric sample is real or fake. This methodology has been compared with QDA and Naive Bayes classifiers.

Keywords: QDA, biometrics, security spoofing, image quality assessment.

I. INTRODUCTION

The use of biometric is increasing as need for security increases. Following this raise in popularity now threats have appeared. Fake samples can be obtained from genuine samples for eg: finger print, iris on printed paper, face images taken in mobile phones etc. Biometric have the potential to uniquely identify a person's physiological and behavioural characteristics more effectively and accurately than other techniques.

Two biometric samples of same biometric trait of two different persons may not be same. This different parameters of an individual can be used for detection.

This work is a review on biometric method using image quality assessment for fake trait detection. Quality of image is a characteristics that measures perceived image degradation.

This quality measures includes structural information, brightness, amount of information present, noise content etc.

These characteristics are differ for each sample input image. These quality is differ both fake and real sample. This quality difference can be used for detection.

II. METHODOLOGY

2.1. Image Quality Assessment

Fig 2.1 shows the proposed system which enhances the protection of biometric systems. Here, the protection is initiated by adding a software based liveness detection and finally sclera vein recognition of the real input image.

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."

A. Gaussian Filtering

The input sclera image is first Gaussian filtered to get a smoothed version of the input. A Gaussian low pass filter of size 3x3 and = 0.5 is used.

Gaussian filter produces, for each pixel in the image, a weighted average such that central pixel contributes more significantly to the result than pixels at the mask edges the weights are computed according to the Gaussian function:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu)^2/(2\sigma^2)}$$

B. FR-IQA

FR-IQA stands for Full Reference Image Quality Assessment [2]. As the name implies it needs a reference image for calculating the image qualities.

The quality between the input and the smoothed sclera image is calculated.

The various FR-IQMs [2]considered are MSE, PSNR, SC, SNR, MD, AD, RAMD, NAE, LMSE, PRNSD, NXC, MAS, MAMS, RM, TED, TCD, SME, SPE, GME, GPE, SSIM, MS-SSIM, VIF, VSNR and RRED.

DOI 10.17148/IARJSET

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

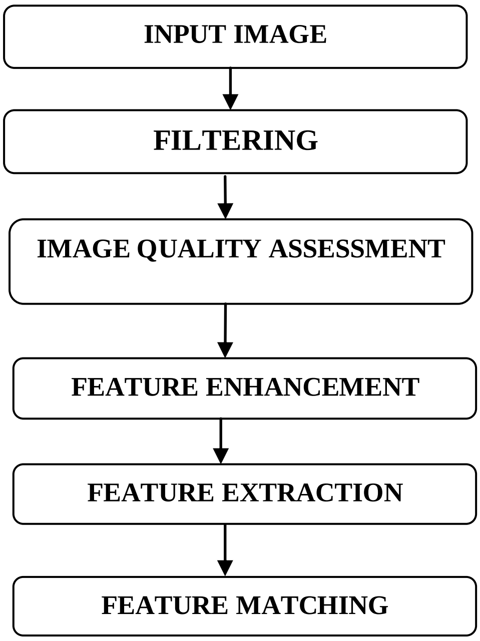


Fig 2.1. Block diagram of proposed method

C. NR-IQA
No Reference Image Quality Assessment does not require a reference image for quality computations. The various NR measure considered are JQI, HLFI, BIQI, NIQE.

D) Classification
The classification using QDA classifier is shown below.Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, for experiments we have considered standard implementations in Matlab of the quadractic discriminant analysis

QDA Classifier

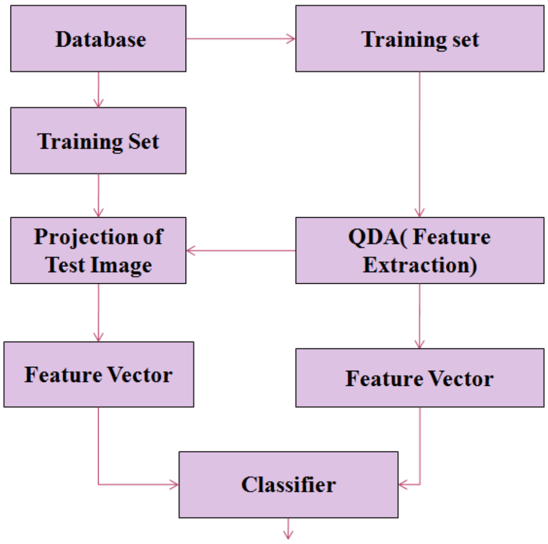


Fig 2.2: Flowchart

In Linear discriminant analysis we provide the following steps to discriminant the input images:

Step-1
We need a training set composed of a relatively large group of subjects with diverse characteristics. The appropriate selection of the training set directly determines the validity of the final results. The database should contain several examples of biometric images for each subject in the training set and at least one example in the test set. These examples should represent different frontal views of subjects with minor variations in view angle. They should also include different facial expressions, different lighting and background conditions, and examples with and without glasses. It is assumed that all images are already normalized to m x n arrays

Step-2
For each image and sub image, starting with the two dimensional m x n array of intensity values I(x, y), we construct the vector expansion φ(mx n). This vector corresponds to the initial representation of the face. Thus the set of all faces in the feature space is treated as a high-dimensional vector space.

Step-3
By defining all instances of the same person's characteristics as being in one class and of different subjects as being in different classes for all subjects in the training set, we establish a framework for performing a cluster separation analysis in the feature space. Also, having labeled all instances in the training set and having defined all the classes, we compute the within-class and between-class scatter matrices.
Now with-in class scatter matrix 'Sw' and the between class scatter matrix 'Sb' are defined as follows:

$$S_W = \sum_{j=1}^{c}\sum_{i=1}^{N_j}(x_i^j - \mu_j)(x_i^j - \mu_j)^T$$

Where x_i^j -is the ith sample of class j

μ_j - is the mean of class j

C – is the class number

A between-class matrix is defined as follows

$$S_b = \sum_{j=1}^{c}(\mu_j - \mu)(\mu_j - \mu)^T$$

Where μ- is the mean of all classes

$$\mathrm{J(W)} = \frac{\|\mathrm{W^T S_W W}\|}{\|\mathrm{W^T S_b W}\|}$$

Here W is the projection matrix and the optimal projection matrix (W*) can be obtained by solving the generalized eigenvalue problem.

$$S_b W^* = \Lambda S_W W^*$$

The with class scatter matrix represents how face images are distributed closely with-in classes and between class scatter matrix describes how classes are separated from each other. When face images are projected into the discriminant vector W.

QDA approach is more robust than estimating the distribution of data by using only up to second order moments (mean and covariance) of the class distribution. Maximizing the between class scatter matrix, while minimizing the within-class scatter matrix, a transformation function is found that maximizes the ratio of between-class variance to within-class variance and find a good class separation as illustrated as follows:

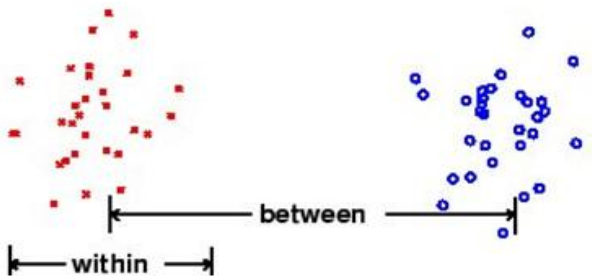


Fig 2.3: Class Separation in QDA

Classification using Naive Bayes

Naive Bayes classifiers are based on Bayes' theorem. It assumes that the value of a particular feature is independent of value of any other feature in the same class. It is conditional probability model. The advantage of using this classifier is that it requires only a small amount of training data to find the parameters needed for classification.

Probabilistic Model

Let $X = (x_1, x_2 .. x_n)$ be a vector to be classified with instance probabilities $p({}^{C_k}\!/_{x_1, x_2 .., x_n})$

Where n- number of features

C-class variable

If n is large, then such a model is not feasible. But using Bayes' theorem, the conditional probability can be decomposed as

$$p({}^{C_k}\!/_{X}) = \frac{p(C_k)\, p({}^{X}\!/_{C_k})}{p(X)}$$

Here the denominator is independent the value of class and feature it act like a constant. The numerator is equivalent of joint probability model.

$$p(C_k, x_1, \ldots., x_n)$$

Thus the joint model can be expressed as

$$p({}^{C_k}\!/_{x_1, \ldots. x_n}) \alpha \quad p(C_k, x_1, \ldots.., x_n)$$

$$\alpha \quad p(C_k)\, p({}^{x_1}\!/_{C_k})\, p({}^{x_2}\!/_{C_k})\, p({}^{x_3}\!/_{C_k}) \ldots$$

$$\alpha \quad p(C_k) \prod_{i=1}^{n} p({}^{x_i}\!/_{C_k})$$

Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, for our experiments we have considered standard implementations in Matlab of the Naive Bayse classifier.

2.2. Fake Sample Detection

A typical biometric detection system includes image filtering, feature enhancement, feature extraction, and feature matching. The first step in the detection process is image filtration. Several methods have been designed for filtering. Mainly used is Gaussian filtering, because it is very effective in the reduction of impulse and Gaussian noise. After image filtering, it is necessary to enhance and extract the parameter features finally classification is done based on the degree of similarity between the feature vector obtained and template stored as database.

III. EXPERIMENTS AND DISCUSSIONS

The database is taken from UBIRIS version 1 and version 2, and REPLAY ATTACK. The UBIRIS version 1 database consists of 1877 RGB images taken in two distinct sessions (1205 images in session 1 and 672 images in session 2) from 241 identities. Both high resolution images (800 x 600) and low resolution images (200 x 150) are provided in the database. In UBIRIS version-2 the images were actually captured on nonconstrained conditions at-a-distance, on-the-move and on the visible wavelength. Here 261 subjects of sclera, all total of 522 images are present in this version. From these subjects a total of 11,102 eye images are present in two sessions. Few subjects are there where the Volunteers are wearing glasses.

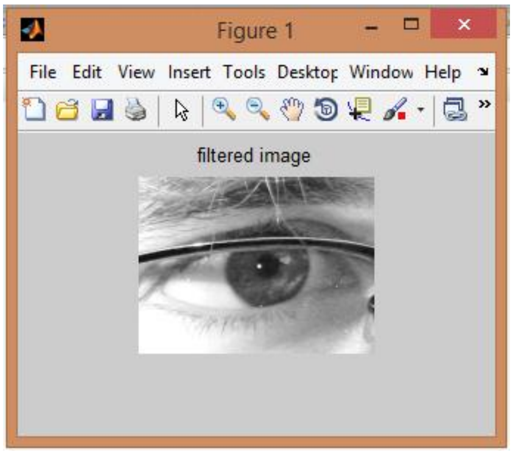
The image quality measures are calculated on these images and threshold is calculated based on the ratios. The clustering is done using a sampling structure. The number of clusters to be taken is fixed to 4 with radii r=5,10,15,20. The number of clusters also needs to be fixed. A large number of clusters may sometimes miss out true correspondences and accumulate unwanted minutiae. The paper focuses on the number of clusters as 10. These clusters are then stored as templates. The total number of sample points was taken to be 79.

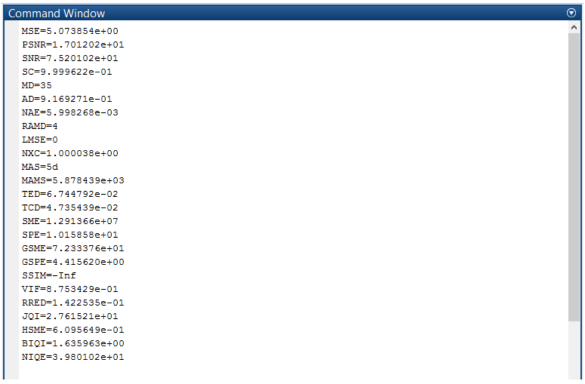
The proposed system could extract 25 features to accurately detect the sclera vein pattern is real or fake.

Performance Analysis

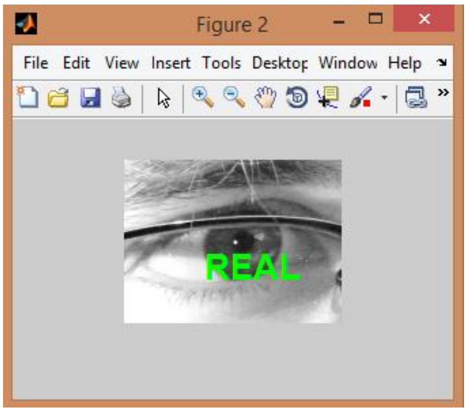
ROC curves are often used in a biometrics to measure the accuracy of the biometric matcher. An ROC curve plots the rate of "false positives" (i.e. impostor attempts accepted) on the x-axis, against the corresponding rate of "true positives"(i.e. genuine attempts accepted) on the y-axis. ROC curves are threshold independent, allowing performance comparison of different systems under similar conditions. The most accurate and efficient biometric system occupies the top position in the ROC curve.

From the ROC curve, it is clear that the proposed method is efficient when compared to other unimodal biometric authentication techniques





```
MSE=5.073854e+00
PSNR=1.701202e+01
SNR=7.520102e+01
SC=9.999622e-01
MD=35
AD=9.169271e-01
NAE=5.998268e-03
RAMD=4
LMSE=0
NXC=1.000038e+00
MAS=5d
MAMS=5.878439e+03
TED=6.744792e-02
TCD=4.735439e-02
SME=1.291366e+07
SPE=1.015858e+01
GSME=7.233376e+01
GSPE=4.415620e+00
SSIM=-Inf
VIF=8.753429e-01
RRED=1.422535e-01
JQI=2.761521e+01
HSME=6.095649e-01
BIQI=1.635963e+00
NIQE=3.980102e+01
```



	Input samples tested	Correctly detected samples	Wrongly detected samples
Fake fingerprint	222	197	25
Real fingerprint	222	195	27
Fake iris	240	206	34
Real iris	240	204	36

Fig 2.4:Classification done using QDA

$$\text{Accuracy} = \frac{\text{No: of Samples correctly detected}}{\text{Total No: of inputs}}$$

$$= \frac{197+195+206+204}{222+222+240+240} = 86.7\%$$

	Input samples tested	Correctly detected samples	Wrongly detected samples
Fake fingerprint	222	207	15
Real fingerprint	222	205	17
Fake iris	240	218	22
Real iris	240	216	24

Fig 2.5:Classification done using NB

$$\text{Accuracy} = \frac{\text{No: of Samples correctly detected}}{\text{Total No: of inputs}}$$

$$= \frac{207+205+218+216}{222+222+240+240} = 91.5\%$$

IV. CONCLUSION

The biometric system using image quality assessment for fake trait detection is an advanced system which provides high security. To improve the efficiency, image quality assessment is also done to find the genuinity of the biometric image. The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios. Moreover an improved biometric detection is also provided. The classification is done using QDA and Naive Bayes classifier .As the comparison between these two classifiers Naive Bayes provide better accuracy than QDA.

ACKNOWLEDGEMENT

I would like to thank for REPLAY ATTACK database.

REFERENCES

[1]. Diego Gragnaniello, Giovanni Poggi, Member, IEEE, Carlo Sansone, Member, IEEE, and Luisa Verdoliva," An Investigation of Local Descriptors for Biometric Spoofing Detection VOL. 10, NO. 4, APRIL 2015

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

[3]. N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, Jul. 2014

[4]. Meng-Hui Lim, Andrew Beng Jin Teoh, Senior Member, IEEE, and Kar-Ann Toh, Senior Member, IEEE"Dynamic Detection-Rate-Based Bit Allocation With Genuine Interval Concealment for Binary Biometric Representation" Vol. 43, No. 3, June 2013

[5]. Abhijit Das, Umapada Pal, Michael Blumenstein, Miguel Angel Ferrer Ballester, "Sclera Recognition -A Suvey",2013

[6]. S.Crihalmeanu and A.Ross, Multispectral sclera patterns for ocular biometric recognition,pattern Recognition Letters,vol 33,p.p.1860-1869,2012

[7]. Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode "Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition" Vol.2, No.1, February 2012

[8]. Zhan SHI, Jinglu HU" Local Linear Discriminant Analysis with Composite Kernel for Face Recognition" June, 10-15, 2012

[9]. L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in Proc. 21st Int. Conf. Pattern Recognit., 2012, pp. 537–540.

[10]. Jiming Li, Yuntao Qian" Dimension Reduction Of Hyperspectral Images With Sparse Linear Discriminant Analysis" 2011 IEEE

[11]. Y. Kim, J.-H. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," IEEE Trans. Consum. Electron., vol. 57, no. 2, pp. 756–762, May 2011.

[12]. Z.Zhou, Y.Du, N.I.Thomas and E.J.Delp, Multi-Angle Sclera Recognition System,IEEE Workshop on Computational Intelligence in Biometrics and Odentity Management:p.p.103-108,2011

[13]. B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise," Pattern Recognit., vol. 43, no. 8, pp. 2845–2857, 2010.

[14]. Andreas Humm, Student Member, IEEE, Jean Hennebert, Member, IEEE, and Rolf Ingold,Member, IEEE," Combined Handwriting and Speech Modalities for User Authentication" IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 39, No. 1, January 2009