International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 2, Issue 8, 2015, PP 1-8
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

Biometric Detection in Fingerprint, Iris, and 2D face using hybrid of IQA and SIFT

P.Supraja[1], T.Aruna[2]

[1]PG scholar, Dept of ECE, Gokula Krishna College of Engineering, JNTUA, Sullurpeta, AndhraPradesh, India.
supraja.pavuluru@gmail.com

[2]Asst prof, Dept of ECE, Gokula Krishna College of Engineering, JNTUA, Sullurpeta, AndhraPradesh, India.
arunakoushi@gmail.com

Abstract: *Security is the major concern for today's scenario. A high level industry uses passwords like thumb, face, voice, iris, etc. So many security systems are available, but not reliable. The biometric details are very useful and essential one of the developing security world, but the biometric details are made fake by the hackers. There are so many methods used to authentication the biometric details in both the hardware and software base. In one of the previous method is Image quality assessment (IQA). In this method extract the eleven qualities of the biometric images. These image qualities features are used to classify the authentication process. In this paper we combine the both IQA and Scale-invariant feature transform (SIFT) and use the Quadratic Discriminate Analysis (QDA).In this paper first we extract the eleven image quality features and extract the SIFT matching points of the image then combine the both features. QDA classifier is used to classify the authentication process of biometric details by using both the extract features of IQA and SIFT. This method is well to detect the authentication of biometric details, if it was spoofed by hackers*.

Keywords: *Image Quality Assessment, Quadratic Discriminate Analysis, Biometrics, Security.*

1. INTRODUCTION

Image and biometric details of men is designed artificial by using some software it is called spoofing. Spoofing is one of the most problems in developing security world. In spoofing process is done by so many software and skilled person. In future world security is the important one to every person. The biometric data will help in all fields to identification process. So we need to develop new method to find and rectifies the spoofing data. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 11 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. 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. In this process authentication is used to determine the identity of a person/user. Authentication is a very important concept in security, because many critical security services are dependent on authenticating users. In general, methods of authentication fall into three categories:

Something the user knows (passwords, PINs) something the user has (i.e. Tokens: ID Cards, smartcard) something the user is (i.e. Biometrics).

2. PROPOSED SYSTEM

In the present work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality

assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack).

Advantages of proposed system:

1. It is speed and very low complexity.
2. It very well suited to operate on real scenarios.
3. It does not deploy any trait-specific property.
4. General image quality measures fast to compute, combined with very simple classifiers.

Comparison of existing system and proposed system:

	COMPARISION	
	EXISTING SYSTEM	PROPOSED SYSTEM
FINGER PRINT TRAINING AND CLASSIFICATION	QDA	ANN,QDA, LDA
IRIS TRAINING AND CLASSIFICATION	QDA	ANN,QDA, LDA
FACE TRAINING AND CLASSIFICATION	LDA	ANN,QDA, LDA
PHASES	IDENTIFICATION	IDENTIFICATION & AUTHENTICATION
IMAGE QUALITY MEASURES	10	15

The existing system has only identification phase, whereas proposed system has both identification and authentication phase. Existing system check only the person accessing the system is real or fake but proposed system also check the person accessing the system is an authorized user or not. Comparison is shown in the above table.

Identification Phase:

1) Results: Fingerprints

The real and fake image found in this database is shown in Fig1.

The classifier used for the two scenarios are Artificial Neural Network (ANN),Quadratic Discriminant Analysis (QDA), Linear Discriminant Analysis(LDA).Comparative results were reported with particular Implementations of the techniques based on QDA training. The results obtained are presented in Table. The table presents the comparison between existing and proposed system.

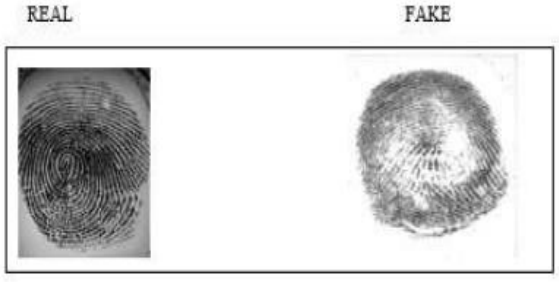


Fig1. *Real and fake fingerprint images*

2) Results: Iris

The real and fake images found in this database are shown in Fig2. The classifier used for the two scenarios are Artificial Neural Network(ANN), Quadratic Discriminant Analysis (QDA), Linear Discriminant Analysis (LDA).The results obtained are presented in the above Table.

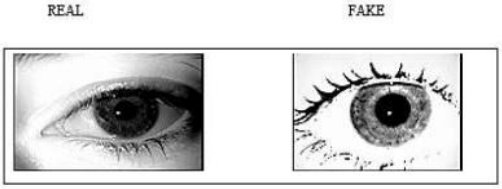


Fig2. *Real and fake iris images*

3) Results: 2D Face

The database contains short videos captured during attacks. The videos were captured under two different conditions:

i) Controlled, with artificial lighting and uniform background.

ii) Adverse, with non-uniform background and natural illumination. Different types of attacks are considered are: print, webcam, high def. Real and fake access is found in REPLAY-ATTACK-DB.

Fig3. *Real and fake 2D face image*

Authentication Phase:

In this phase the same replay attack database is used.

Thus we can conclude that Biometric systems are becoming increasingly popular both as standalone security systems and as added security largely because of one reason convenience. People can easily forget a password, but will never forget to bring their finger, iris, face. The main problem that are faced by biometric security system are direct and indirect attack. The proposed system protects biometric security system from these types of attack and thus increase the security level .A novel liveness detection scheme for fingerprint, iris, face based on quality related measures has been presented.

The proposed method was tested on fingerprint, iris, and face database. Here training of database and classification are done using Artificial Neural Network (ANN), Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).Among the three classifiers, ANN is more efficient and provide accurate result. Image Quality measures are extracted from real and fake images and using these measures vector the classification of image is done.

3. MODULES

- Query image
- Preprocess
- Filter
- Extract the feature
- Classification.

Module Description:

Query image:

It is the input image of the process this image is original or fake. The spoofing image is created by photo editing software. That input images are load and shown in the fig.

Preprocess:

The preprocess step is important one in the image processing. In that process we removing the noise and resize the image and some process done for output.

Convert to Gray:

In preprocess step the first step is gray image. In image process all image in grayscale. In the grayscale image the RGB is removed because some process is done in without RGB image. So first we remove the RGB in given query image.

Resize the image:

It is the second preprocess step in this step we change the image size. Because the query image is in any size it affect the time consuming and output quality. So we change the image size our comfortable range.

Filter:

In filter process we remove the noise from input image. The noise is the unwanted pixel of the image. We use Gaussian filter to remove the noise in query image.

Gaussian filter:

Gaussian filtering g is used to blur images and remove noise and detail.

In one dimension, the Gaussian function is:

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

Where σ is the standard deviation of the distribution. The distribution is assumed to have a mean of 0. Shown graphically, we see the familiar bell shaped Gaussian distribution.

The Gaussian function is used in numerous research areas:

– It defines a probability distribution for noise or data.

– It is a smoothing operator.

– It is used in mathematics.

The Gaussian function has important properties which are verified with The Gaussian function has important properties which are verified with respect to its integral:

$$I = \int_{-\infty}^{\infty} \exp\left(-x^2\right) dx = \sqrt{\pi}$$

Extract the Feature:

In our proposed system we use Image Quality Assessment (IQA). the input gray-scale image **I** (of size $N \times M$) is filtered with a low-pass Gaussian kernel in order to generate a smoothed version $\hat{}\mathbf{I}$ .Then, the quality between both images (**I** and $\hat{}\mathbf{I}$) is computed according to the corresponding full-reference IQA metric. This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples.

There are so many image quality is there we use only eleven image quality that is

1. Mean square error (MSE)
2. Peak Signal to Noise Ratio (PSNR)
3. Signal to Noise Ratio (SNR)
4. Structural Content (SC)
5. Maximum Difference(MD)
6. Average Difference (AD)
7. Normalized Absolute Error (NAE)
8. NormalizedCross-Correlation (NXC)
9. Total Edge Difference (TED)
10. Total Corner Difference (TCD)
11. Structural Similarity Index (SSI)

These are our selected image quality to extract the image features. Image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the

reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features. Although their efficiency as signal fidelity measures is somewhat controversial up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system they are easy to calculate and usually have very low computational complexity. These features compute the distortion between two images on the basis of their pixel wise differences. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale. Image enhancement or improving the visual quality of a digital image can be subjective. Saying that one method provides a better quality image could vary from person to person. For this reason, it is necessary to establish quantitative/empirical measures to compare the effects of image enhancement algorithms on image quality. Using the same set of tests images, different image enhancement algorithms can be compared systematically to identify whether a particular algorithm produces better results. The metric under investigation is the peak-signal-to-noise ratio. If we can show that an algorithm or set of algorithms can enhance a degraded known image to more closely resemble the original, then we can more accurately conclude that it is a better algorithm.

Classification:

Quadratic Discriminant Analysis is used to classify the image is original or fake. It is a common tool for classification A standard approach to supervised classification problems is quadratic discriminant analysis (QDA), which models the likelihood of each class as a Gaussian distribution, then uses the posterior distributions to estimate the class for a given test point (Hastie et al., 2001). The Gaussian parameters for each class can be estimated from training points with maximum likelihood (ML) estimation. The simple Gaussian model assumption is best suited to cases when one does not have much information to characterize a class, for example, if there are too few training samples to infer much about the class distributions. Unfortunately, when the number of training samples *n* is small compared to the number of dimensions of each training sample *d*, the ML covariance estimation can be ill-pose.

Flow diagram:

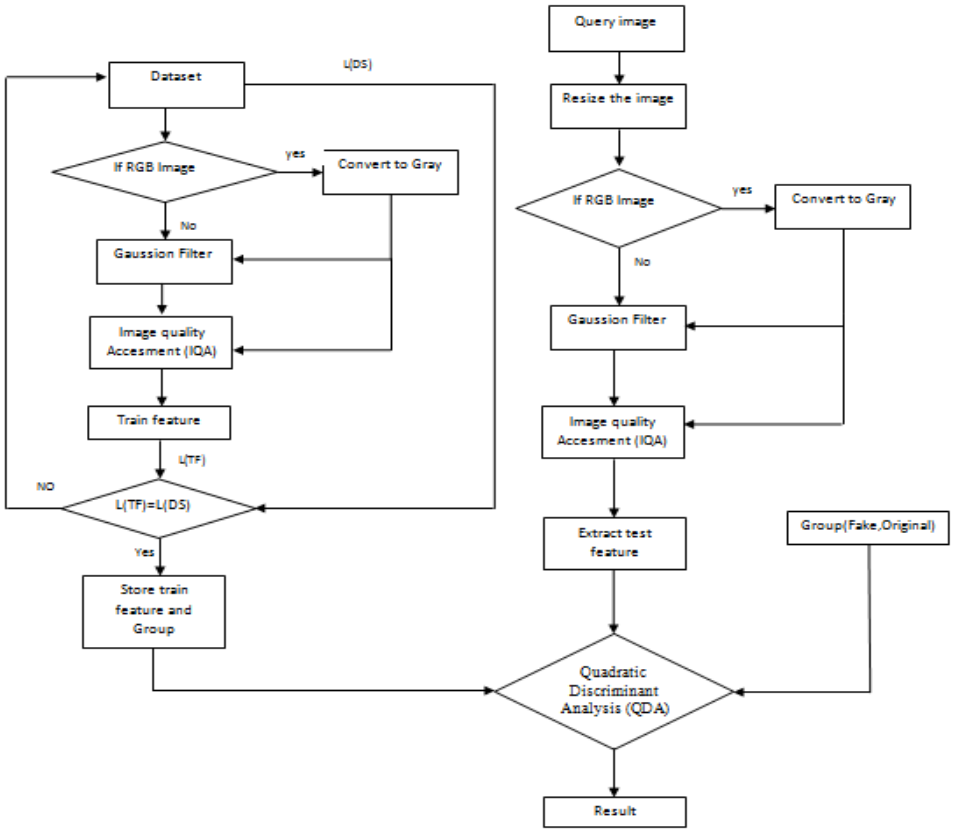
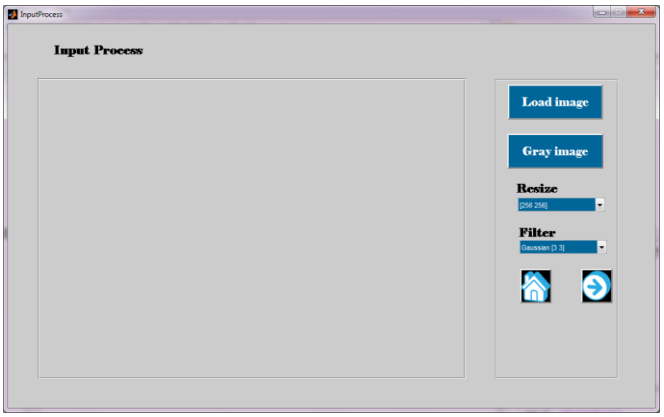
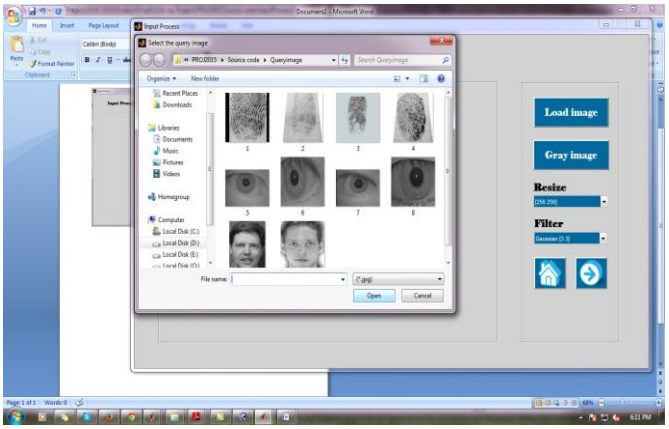
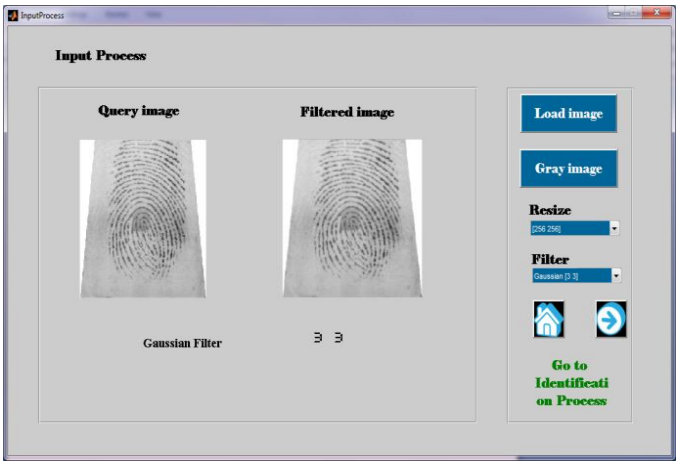


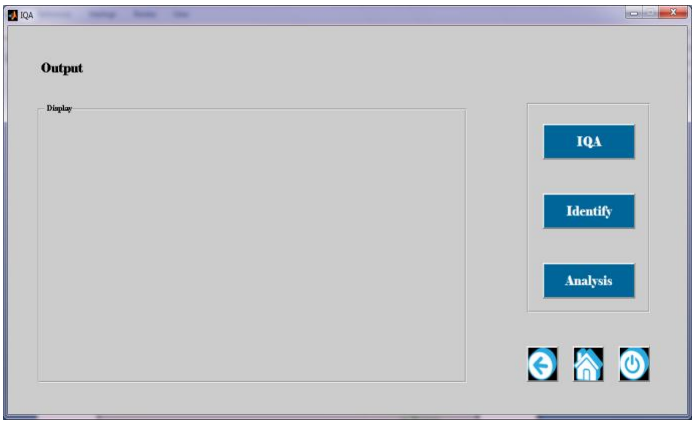
Fig4. *Flow Diagram*

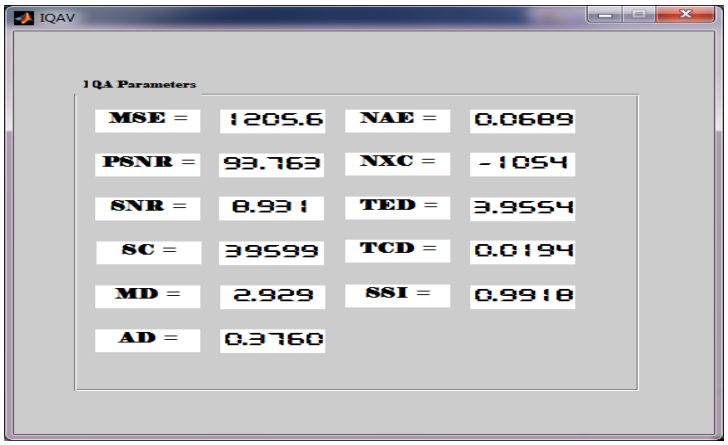
Result Analysis:

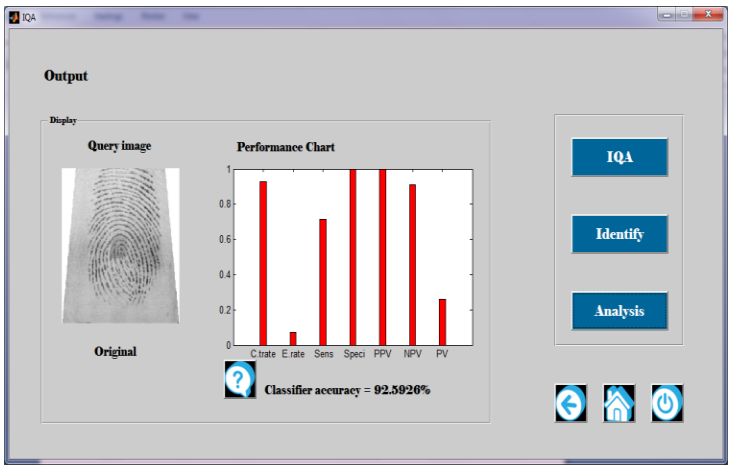












4. CONCLUSION AND FUTURE SCOPE

The study of the biometric systems against different types of attacks has been a very active field in future. This is enhanced the field of security technologies for biometric-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task. For this purpose we have considered a feature space of 11 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 in proposed system contain some conclusions. It adapt the different biometric details by high performance method, It able to analysis multi biometric details, and it is simplest, secure and less complexity method.

In our proposed we use software based spoofing attack system. In this process get several advantages over the existing system but in feature some enhancement is there for good security in biometric authentication. In that characters we use hybrid the hardware and software based biometric system to increase the accuracy of authentication.

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]. 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]. J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.

[10]. M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," Signal Process., Image Commun., vol. 27, no. 8, pp. 875–882, 2012.

[11]. N. B. Nill and B. Bouzas, "Objective image quality measure derived from digital image power spectra," Opt. Eng., vol. 31, no. 4, pp. 813–825, 1992.

AUTHORS' BIOGRAPHY

P.Supraja, received the B.tech degree in Electronics and Communication Engineering from Narayana Engineering College, Gudur, University of JNTUA in 2012. She is currently working towards the Master's Degree in Digital Electronics and Communication Systems in Gokula Krishna College of Engineering, University of JNTUA. Her interest lies in the areas of Image processing, Embedded System, and Digital Communication.

Mrs. T.Aruna, received her B.tech degree in ECE from Audisankara College of Engineering and Technology, University of JNTUH in 2005, M.tech degree from Sri Venkata Perumala College of Engineering and Technology, University of JNTUA in 2012.Presently she is working as an Assistant Professor in the Department of ECE at Gokula Krishna College of Engineering, Sullurpet.