ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

# Intruder Detection For Biometric Access

[I]M. Enoch sam, [II]Nathan pinto. D, [III]Amar. M, [IV]Sudheer. K, [V]C. Mahesh, [VI]Vijayalakshmi. G.V
[I]P.G. Scholar, Embedded systems, Karunya University
[II,III,IV]B.Tech, ECE, Dr.TTIT,VTU
[V]Assistant Professor, Electrical Technology, Karunya University
[VI]Assistant Professor, Dr.TTIT, VTU

**Abstract**
*To ensure genuine and real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this system developed, we present a novel fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, using image quality assessment. This approach presents a very low degree of complexity, which makes it suitable for real-time applications, using image quality features extracted from one image used for authentication purpose to distinguish between legitimate and impostor samples.*

**Keywords**
*Biometric, Liveness Assessment, Fraudulent, Non-Intrusive, Legitimate.*

## I. Introduction

In recent past, the increasing interest within the analysis of biometric systems security has led to the creation of various extremely diverse initiatives targeted on this major field of research, the publication of many analysis works disclosing and evaluating completely different biometric vulnerabilities, the proposal of recent protection strategies sessions and workshops in biometric-specific and signal processing conferences, the organization of competitions have targeted on vulnerability assessment [1].

The acquisition of specific datasets, the creation of groups and laboratories specialized within the evaluation of biometric security, or the existence of several European projects with the biometric security topic as main research interest [2] [3]. Among the various threats analysed, the alleged direct or spoofing attacks have driven the biometric community to check the vulnerabilities against this sort of dishonest actions in modalities like the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some sort of synthetically made object (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the real user (e.g., gait, signature), to fraudulently access the biometric system.

As this kind of attacks is performed within the analog domain and therefore the interaction with the device is completed following the regular protocol, the same old digital protection mechanisms (e.g., encryption, digital signature or watermarking) don't seem to be effective [4][5]. the knowledge flow of a biometric access system is easy. First the biometric is presented to the sensing element by the person requesting access. A camera might capture a face or iris, a sensing element might capture a fingerprint, a microphone might capture a voice; in every case, the raw biometric data is acquired and sent to the biometric feature extractor.

The extractor is mostly computer code that extracts the features vital for determining identity from the raw data. For a fingerprint, this could be the minutiae points and for a face this might be the gap between the eyes [6][7]. This extracted feature data is termed a template. The template is then sent to the matcher. The matcher compares the newly-presented biometric data to previously submitted template data to create a decision [8]. presented in conjunction with a personal identification number or access card, the template is also matched against that of one registered user for verification. or else, it should be compared to all or any registered users for identification. For effective implementation of biometrics, intruder detection even has to be included.

## II. System Description

The block diagram gives the information that, the input image which is unseen image of either iris or fingerprint. Such that the features of the query image are extracted and then it is classified using a classifier (quadratic discriminative analysis).

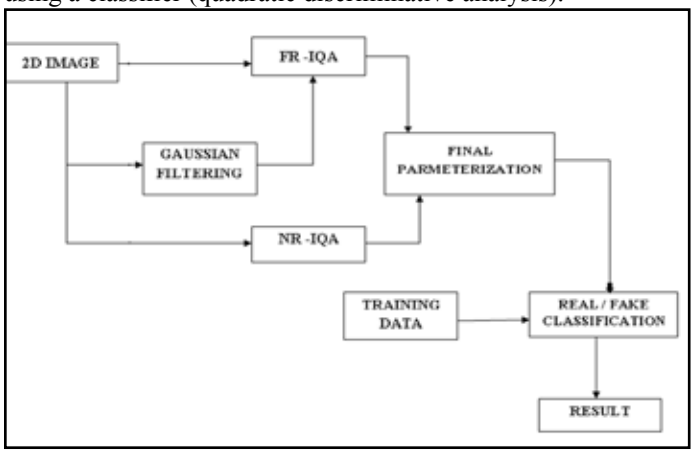


Fig. 1: System Block diagram

The work presented in this project consists of eight major parts or blocks:

### A. 2D Image

It is the image given to the system, to be classified as real or fake. Images used in this project are of size 640x480 in case of iris images, for fingerprint images it is 300x300. To classify this image, all the parameters of this input image are being calculated.

### B. Full Reference IQ Measures

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work

such a reference image is unknown, as the detection system only has access to the input sample [9]. To overcome this limitation, the strategy of using Gaussian filtered image as reference image was already successfully used for image manipulation detection and for steganalysis is implemented. Same strategy is also used here.
The input grey-scale image I (of size 640 × 480) is filtered with a low-pass Gaussian kernel (σ = 0.5 and size 3 × 3) to generate a smoothed version Iˆ. Then, the quality between both images (I and Iˆ) 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.

### C. No-Reference IQ Measures

Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image [10]. Automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference.

### D. Gaussian Filtering

To produce a reference image which should be undistorted for assessing in the calculation of Full-Reference IQA measures Gaussian filtering is being used. The Gaussian kernel is of, σ = 0.5 and size 3 × 3.

### E. Final Parametrization

All the features or parameters of the given input image is being tabulated in the form of matrix in-order to make it easy for the classifier.

### F. Training Data

This contains the values of all parameters of 160 images used for training purpose in the form of 160x27 size matrix.

### G. Classification

Iris: For the iris modality, the protection method is tested under two different attack scenarios, namely Spoofing attack and Attack with synthetic samples [11]. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method.
Fingerprints: As in the iris evaluation, the database are divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set) [12]. The classifier used in this project is quadratic discriminant analyser.

## III. Implementation

The Image Quality Analysis was carried out on biometrics namely Iris and Fingerprint. To carry out the work the images from the databases, Iris (LivDet 09), fingerprint (ATVS-Flr DB) were used.
Iris (LivDet 09) database was obtained from 5 persons, in which each person's left eye images were captured in 10 different sessions in different conditions. In same way, right eye images of same person were captured. Therefore, 100 Images were obtained for 5 people in real category. Similarly, fake samples of the same 5 persons were obtained for both eyes using different spoofing techniques. Therefore, there are 100 images for the fake samples.

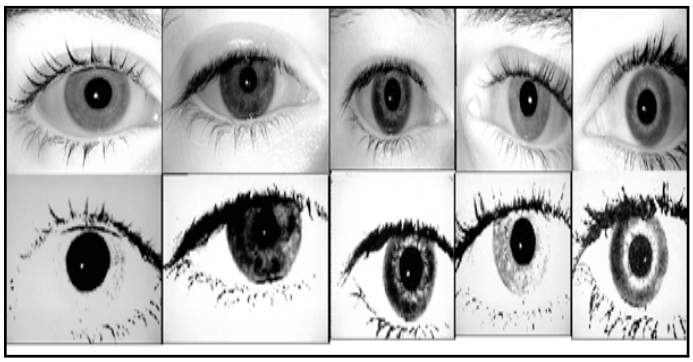

Fig. 2: Input Iris Images to System

Figure 2 shows Iris sample images in which it has 5 user's original images (top row) and same 5 user's fake images(bottom).
Fingerprint (ATVS-Flr DB) database was obtained from 5 persons, in which each person left thumb impression were captured in 20 different sessions in different conditions. Therefore, 100 Images were obtained for 5 people in real category. Similarly, fake samples of the 5 persons were obtained using different spoofing techniques. Therefore, there are 100 Images for fake samples [13].
Figure 3 shows Fingerprint sample images in which it has 5 user's original images (top row) and same 5 user's fake images (bottom).

### A. Classification of Dataset

In dataset as said before, there are 100 real images and 100 fake images. These images are separated in to training and query set as shown in the Figure 4.
Out of real images 80% of the images are considered for training purpose and remaining 20% of the images are separated into query set. Similarly, even for the fake images 80% of the images are grouped into training set and 20% of the images are grouped into query [14].
In training set 16 real Images and 16 fake Images of each person are present, therefore a total of 160 images of 5 persons are present. In query set 4 fake Images and 4 real Images of each person are present, therefore a total of 40 images of 5 persons are present.

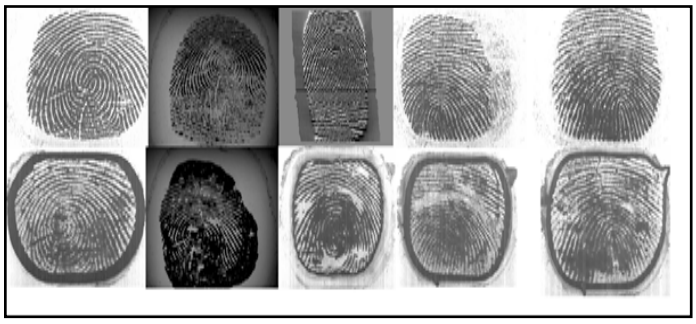

Fig. 3: Input Fingerprint Images to System

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

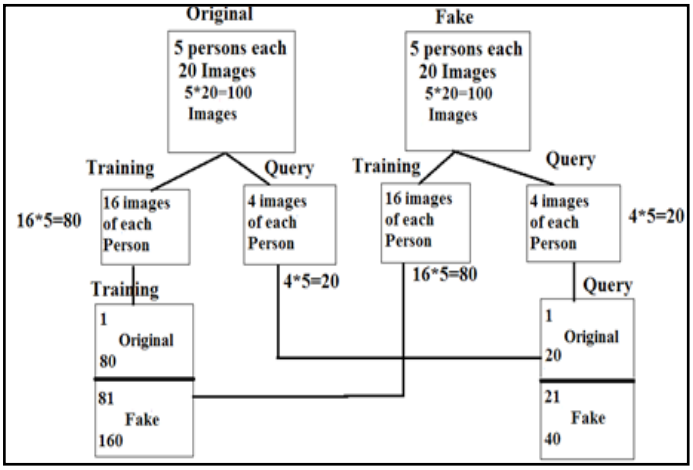


Fig. 4: Classification of Dataset

### B. Implementation Phases

The work was carried out in 2 phases, namely

(i) Training phase

(ii) Testing phase

Training phase:

For training phase 80% of images from both the databases were used [15]. For each image 27 parameters were calculated with this a training dataset of dimension 160x27 was obtained for both iris and fingerprint. The dataset is trained and validated where it includes both real and fake images using quadratic classifier.

Testing Phase:

For testing the system 40% of the images were considered these images do not overlap with Training data. These are unseen images for the system, for each of the image 27 parameters are calculated and applied to quadratic analyser, such that the classifier predicts whether the image given to the system is class 1/original or class 2/fake. And the efficiency of classifier is obtained.

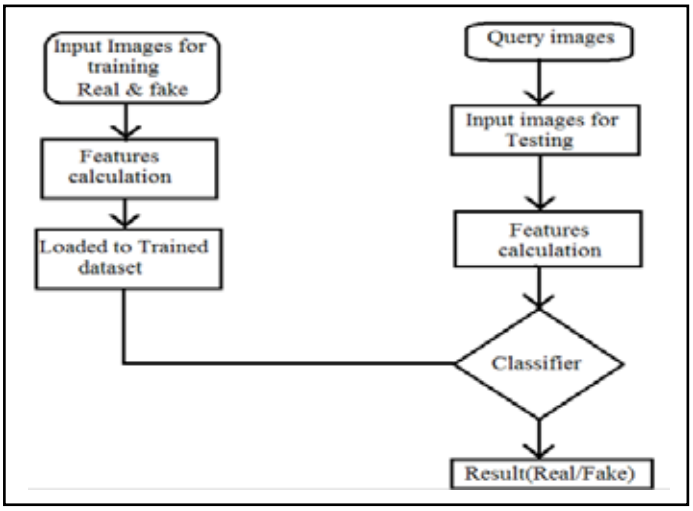


Fig. 5: Training and Testing Phase Flowchart

Input images are taken which are real or fake from the data set and given features are extracted from the images which is stored in the trained data set in form of matrix 160x27 and then the query images which are unseened images are taken and features are extract from the images which are given input images is taken one at a time and then features are compared with trained data set using the classifier to classify it as real or fake.

## IV. Results

The entire work of Intruder detection of biometric access was carried out on two biometrics Iris and Finger print, using MATLAB 2014a(v8.3) on windows 7 platform. The databases obtained for Iris (ATVS-Flr DB) and Fingerprint(Livedet09) was subdivided into two sets Training and query. Therefore, in each of Iris and fingerprint training set there are 160 images which include both real and fake images, all these 160 images were first passed through Gaussian filter.

The input grey-scale image I (of size 640x480) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size $3 \times 3$) to generate a smoothed version Iˆ. Then, the quality between both images (I and Iˆ) 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. Using Gaussian filtered image as the reference image all 27 IQA parameters from 160 training images (which include both Fake and Real) from iris data set were extracted and stored in a form of 160x27 matrix which is as shown in the Figure 6. Similarly, 27 IQA parameters were computed for Finger print data set to obtain a matrix of parameters of dimension 160x27 as shown in the figure 7. These values are then applied to the quadratic discriminant classifier to train the system.

After training the system to differentiate between fake and real image an input unseen image from the query set is selected and given to the trained classifier. The sample input images are shown in the Figure 8, which contains both Iris and Fingerprint. Image is first pre-processed, which describe its contents. The pre-processing involves filtering normalization segmentation and object identification, which is already discussed.

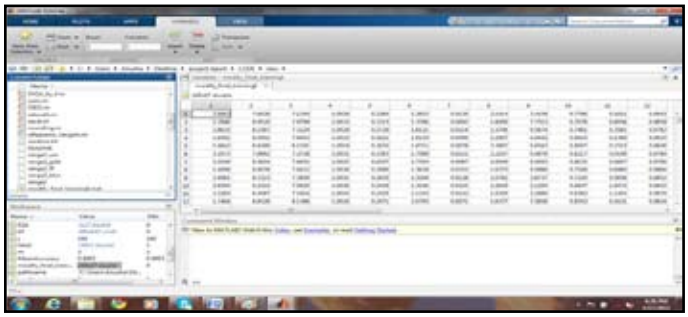

Fig. 6: Iris Dataset Matrix

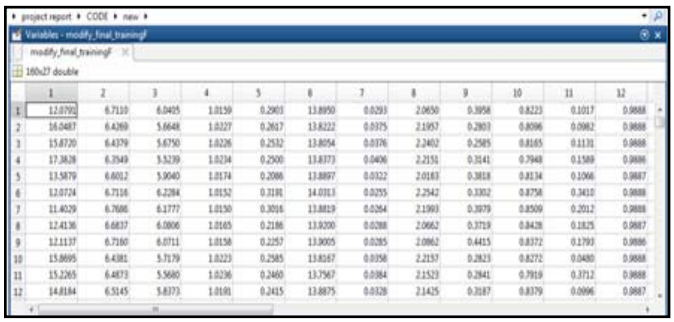

Fig. 7: Fingerprint Dataset Matrix

Fig. 8: Input Image (Iris & fingerprint)

Then using the filtered image, all the 27 parameters are calculated and then put into a matrix of dimension 1x27, which is then given as input to quadratic discriminant classifier.
Classification accuracy (efficiency) calculation:

Table 1: Efficiency calculation Table

| Parameters | Iris | Finger print |
|---|---|---|
| Number of query Images | 40 | 40 |
| Number of Images Correctly Classified | 38 | 37 |
| Number of Errors | 2 | 3 |
| Efficiency of the system (%) | 95 | 92.5% |
| Error Rate | 0.05 | 0.075 |

Efficiency of the implemented system for the iris data obtained was 95% whereas efficiency for the fingerprint obtained was 92.5%, with the error rates for iris, fingerprint to be 0.05 and 0.075 respectively.

## V. Conclusions

IQA was carried out on Iris (ATVS-Flr DB) and Fingerprint(Livedet09) databases to detect the fake biometric samples by means of 27 IQA measures. The system incorporated Quadratic classifier to predict the class(Real/Fake) for the given query image. With the proposed method 95% Classification accuracy was obtained with iris database and 92.5% accuracy was obtained with fingerprint database, this clearly shows that the efficiency of the proposed system is higher than the previous systems and can come handy in implementation of other biometric security systems.
The other conclusion we can make through this system is that IQA technique can be effectively used to classify the biometric input samples into real and fake categories with higher efficiency and low error rates.

## References

[1]. *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.*
[2]. *A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280–3283.*
[3]. *A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.*
[4]. *Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.*
[5]. *Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online]. Available:http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup- bvaeg.html.*
[6]. *D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY, USA: Springer-Verlag, 2009.*
[7]. *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.*
[8]. *ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.*
[9]. *I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.*
[10]. *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 [7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.*
[11]. *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.*
[12]. *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.*
[13]. *M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–496, Sep. 2010. [7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.*
[14]. *Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," Electron. Lett., vol. 44, no. 13,pp. 800–801, 2008.*
[15]. *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.*