# False Biometric Discovery by Means of the Features of Image Excellence

**N. Umamaheswari[1] S. Jacinth Beulah[2] P. Jenifer[3] M. Jeniga Gemsy Thepora[4]**
[1,2]P.G Student [3, 4]Assistant Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Francis Xavier Engineering College, Tirunelveli

*Abstract*— A biometric structure is a computer system, which is used to spot the self on their behavioural and physiological quality. A typical biometric system consists of sensing, feature removal, and matching modules. But currently a day's biometric systems are attacked by using fake biometric classification. The biometric technique which used are face recognition, fingerprint recognition, and iris appreciation and also commence the attack on that structure and by using Image superiority estimation. In biometric detection, forged fraudulent actions in modalities such as face, fingerprint, and iris are detected. A biometric authentication is used to ensure the actual presence of real image in contrast to the fake self-manufactured synthetic samples. The threads include both direct and spoofing attacks. The biometric detection is used to detect the fake image in faster, user friendly and non-intrusive manner. In this project, 25 image quality features are extracted from one image and this information is used to discriminate the fake traits. This approach represents the very low degree of complexity and hence it is used in real time applications. Harris corner detector is used to identify the corners in the given image so that the quality assessment has been detected. With the help of these quality features, the image is classified as real or fake image. The classifier used here is SVM classifier and Back propagation classifier.

***Key words:*** Image Quality Assessment, Biometrics, Security Attacks, Countermeasures

## I. INTRODUCTION

Biometrics refers to metrics associated to human uniqueness and traits. Biometrics authentication or realistic authentication is used in computer science as a appearance of classification and right to use-control. It is also used to make out entity in group that are under surveillance. Biometric identifiers are the distinguishing, computable uniqueness used to label and illustrate individuals.

Biometric identifiers are often categorizing as physiological against behavioral distinctiveness. Physiological characteristics are interrelated to the profile of the carcass.

Behavioral characteristics are related to the outline of behavior of a human being, including but not imperfect to type rhythm, gait, and voice. Some examiners have coined the term behaviometrics to illustrate the latter class of biometrics. Many different aspect of human physiology, chemistry or behavior can be used for biometric confirmation.

The collection of a meticulous biometric for use in a precise purpose involves a weighting of a number of factors. Universality means that each person using a system should hold the attribute. Uniqueness means the trait should be satisfactorily different for individuals in the applicable populace such that they can be well-known from one another. Immovability relates to the behavior in which a trait varies over time. Performance relates to the accurateness, velocity, and toughness of expertise used.

Acceptability relates to how well persons in the relevant population recognize the technology such that they are enthusiastic to have their biometric trait capture and assesse Circumvention relates to the simplicity with which a peculiarity power be imitate using an entity or replacement. No particular biometric will assemble all the provisions of every potential capitulation.

In substantiation mode the arrangement performs a one-to-one evaluation of a confine biometric with a precise pattern stored in a biometric datasets in order to substantiate the personality is the self they announce to be. Three steps are occupied in the substantiation of a person. In the initial stride, suggestion model for all the users are produce and store in the model databases. In the second step, some samples are in time with reference models to produce the authentic and fake scores and calculate the doorstep. Third step is the tough step. This process may use a elegant card, username or ID number to point out which pattern should be used for comparison. 'Positive recognition' is a frequent use of the verification style, "where the aim is to put off multiple people from by means of same uniqueness".

Subsequent, in classification mode the organization perform a one-to-many contrast against a biometric database in attempt to found the uniqueness of an indefinite individual. The organization will achieve something in identifying the personage if the judgment of the biometric sample to a stencil in the database falls within a beforehand set sill. During the staffing phase, the pattern is simply store somewhere. During the similar phase, the obtain template is passed to a matcher that compare it with other existing templates, estimate the detachment between them using any algorithm. The alike program will analyze the mold with the contribution. That will followed by amount produced for any accurate use or purpose. Variety of biometrics in any practical purpose depending upon the typical capacity and user necessities. We should deem routine, adequacy, Circumvention, durability, inhabitants treatment, extent, distinctiveness stealing deterrence in select a scrupulous biometric. Collection of biometric based on user situation consider feeler availability, machine availability, Computational time and consistency, Cost, feeler part and influence outflow

## II. RELATED WORKS

- It Evaluate the "multi-biometric" wideness of the protection scheme. That is, its potential near to accomplish a better-quality performance, compare on the road to supplementary attribute-explicit advance, underneath particular biometric modalities. For this rationale three of the a large amount of unlimited likeness-based biometric modalities embrace is considered here the models iris, fingerprints and 2D face.

 

– It estimate the "multi-harass" dimension of the guard method. So as to, its ability to spot not only spoofing attacks but also deceptive drop a line to attempts usual out with replication or modernize model With these goal in mind, and in organize to complete reproducible results, we include only worn in the untried validation widely accessible database with gleaming described estimate procedures.

## III. METHODOLOGY

### *A. Pre-processing:*

In this module, the input image is selected and hence the image is smoothed with the help of Guassian filter. Guassian filter is used to smooth the input image with the frequency of 0.5 and kernel 3.hence it produces two images original image and the smoothen image.

### *B. Feature Extraction:*

In this module, with the help of smoothen image and the original image the features are extracted
The features include

– Pixel difference measures
– Correlation based measures
– Edge based measures
– Spectral distance measures
– Gradient based measures

Hence these values are derived with the help of Harris corner detector and the fourier transform functions. These 25 full-reference and no- reference quality features are derived and it is used in classification. The features are derived from the pixel difference measures, Harris corner detector is generally used to detect feature points in both the images and detect the corresponding points to calculate the feature values in Total edge difference and Total corner difference. Fourier transform function is used in Spectral magnitude error and spectral phase error.

### *C. Classification:*

In this module the values derived from the image is stored at the back end and hence the image is tested using the svm classifier and Back propagation classifier. The svm classifier uses both training and testing. The training phase is used to store the trained image feature values in the two dimensional array. After training, testing phase is done and the tested image features are compared with the trained values. If they are found to be same then it is real image or else it is fake. The back propagation classifier helps to calculate the weight with the help of 25 features and compare with the stored data, if it is found to be same then it is real otherwise fake.

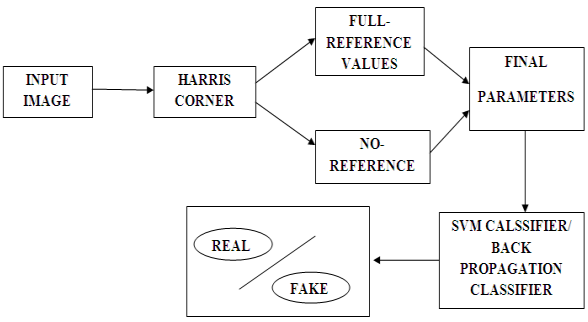


Fig. 1: Fake Biometric Detection

## IV. RESULT

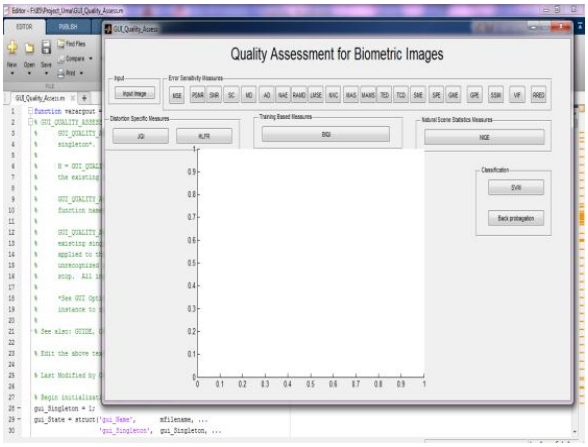


Fig. 1: Initial Output Screen

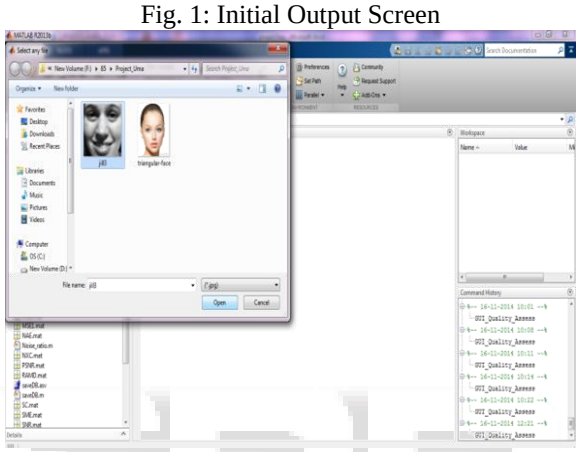

Fig. 2: Selecting Inputimage

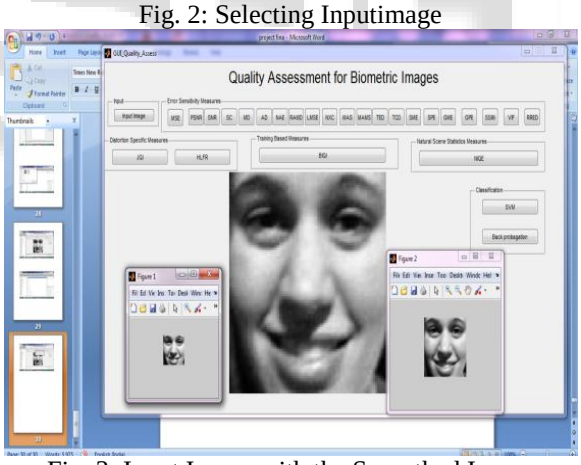


Fig. 3: Input Image with the Smoothed Image

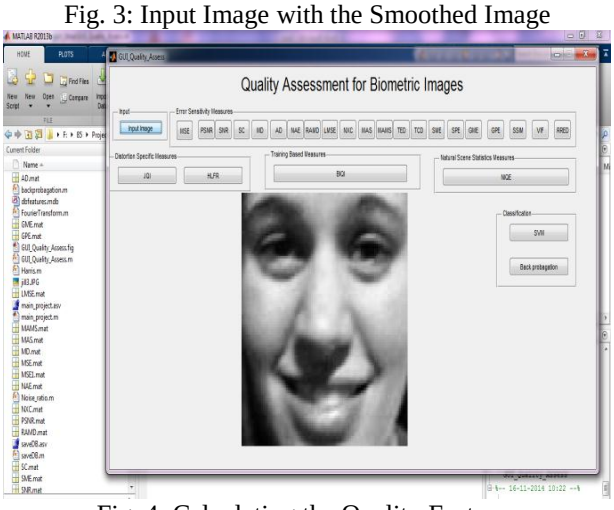


Fig. 4: Calculating the Quality Features

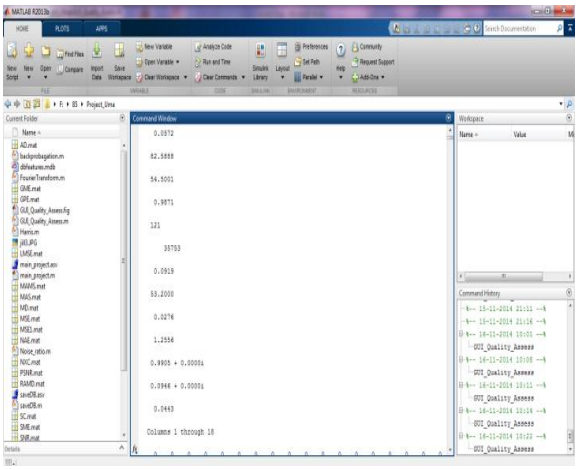

Fig. 5: Providing the 25 Quality Features

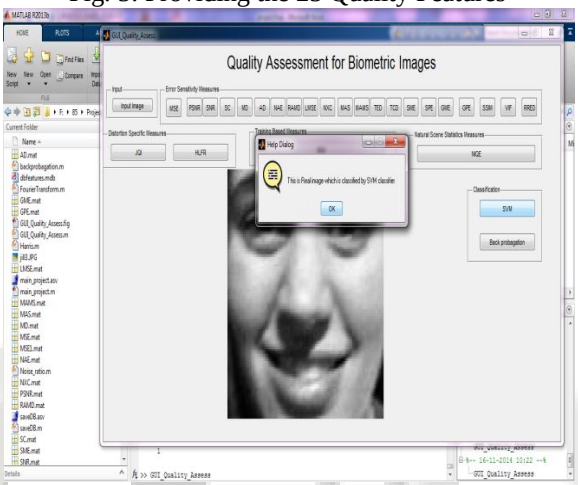


Fig. 6: Classify the Given Image as Real

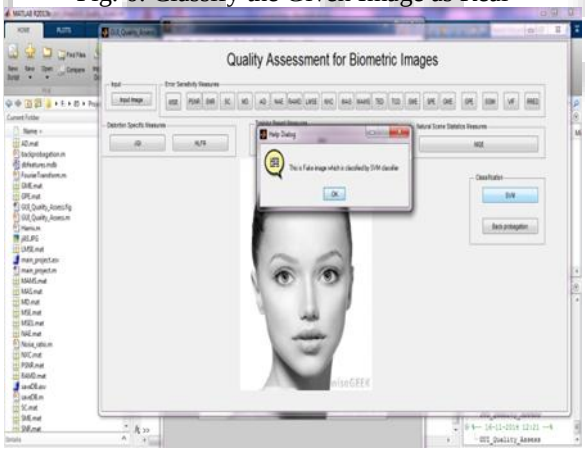


Fig. 7: Classify the Given Image as Fake

## V. CONCLUSION AND FUTURE WORK

This method is intelligent to constantly execute at a elevated point for diverse biometric behavior and this system is talented to get use to unusual type of attack as long as for all of them a lofty level of defend

- The planned process was able to simplify fine to diverse datasets, attainment circumstances and attack situation
- The fault toll achieve by the proposed shield plan is in lots of cases lesser than folks account by other mannerism-detailed high-tech anti-spoofing system which have been tested in the gallows of different self-determining contest.

The future work is found to be,

1) Application and support of a innovative biometric guard system.
2) Reproducible estimate on numerous biometric personality based on clearly accessible datasets.
3) Relative outcome with added formerly planned security solution

## REFERENCES

[1] Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition, Galbally,J. Joint Res. Centre, Eur. Comm., Ispra, Italy ; Marcel, S.; Fierrez, J., Image Processing, IEEE Transactions on (Volume:23, Issue:2) Biometrics Compendium, IEEE

[2] 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.

[3] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.

[4] 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.

[5] K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[6] 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.

[7] 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.

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

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

 