FAKE IDENTIFICATION IN FINGERPRINT, IRIS AND FACE RECOGNITION USING IMAGE QUALITY ASSESSMENT

S.Chinthu[1], C.Dhanabal[2]

[1,2]Dept of CSE, Mount Zion College of Engineering and Technology,
Anna University, Chennai (India)

ABSTRACT

A biometric system is a computer system which is used to identify the person on their behavioral and physiological characteristic (for example fingerprint, face, iris, key-stroke, signature, voice, etc). A typical biometric system consists of sensing, feature extraction, and matching modules. But now a day's biometric systems are attacked by using fake biometrics. This paper introduce three biometric techniques which are face recognition, fingerprint recognition, and IRIS recognition (Multi Biometric System) and also introduce the attacks on that system and by using Image Quality Assessment For Liveness Detection how to protect the system from fake biometrics. The multi biometric system is secured than uni-biometric system. To ensure the actual presence of a 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 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 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.

Keywords: ***Liveness Detection Techniques, Image Quality Assessment, Biometric Authentication, Novel Software Based Fake Detection.***

I INTRODUCTION

A biometric system is a computer system .Which is used to identify the person on their behavioral and physiological characteristic (for example fingerprint, face, iris, key-stroke, signature, voice, etc). A typical biometric system consists of sensing, feature extraction, and matching modules. But now a day's biometric systems are attacked by using fake biometrics. This approach introduce three biometric techniques which are face recognition, fingerprint recognition, and iris recognition (Multi Biometric System) and also introduce the attacks on that system and by using Image Quality Assessment For Liveness Detection how to protect the system from fake biometrics.

1.1 Liveness Detection Methods

Liveness detection methods are usually classified into one of two groups: (a) Hardware-based techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye); (b) Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself). The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user.

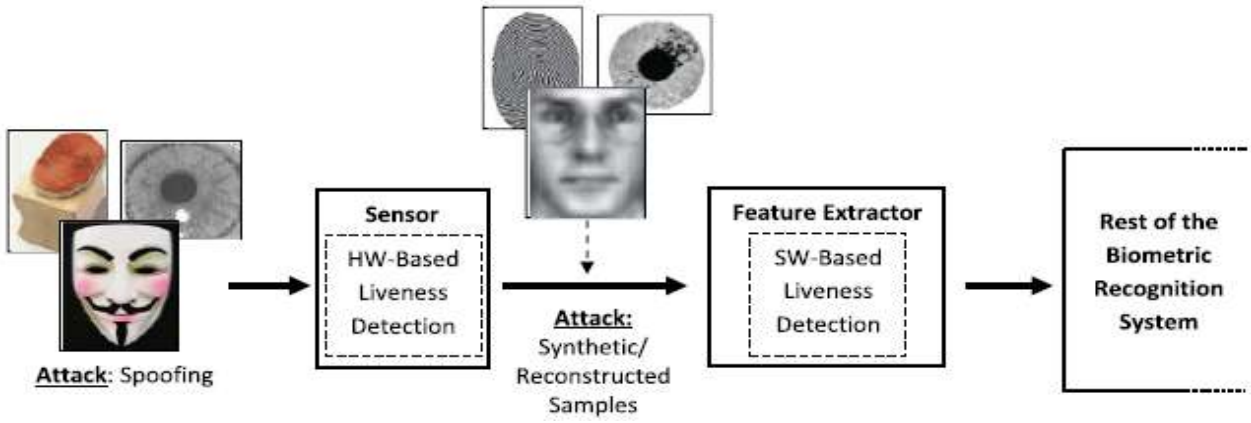


Fig 1: Liveness Detection Techniques

1.2 Image Quality Assessment

In the current state-of-the-art, the rationale behind the use of Image Quality Assessment features for liveness detection is supported by three factors: Image quality has been successfully used in previous works for image manipulation detection and steganalysis in the forensic field. To a certain extent, many spoofing attacks, especially those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed iris or face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the present research work, by the use of different quality features. Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

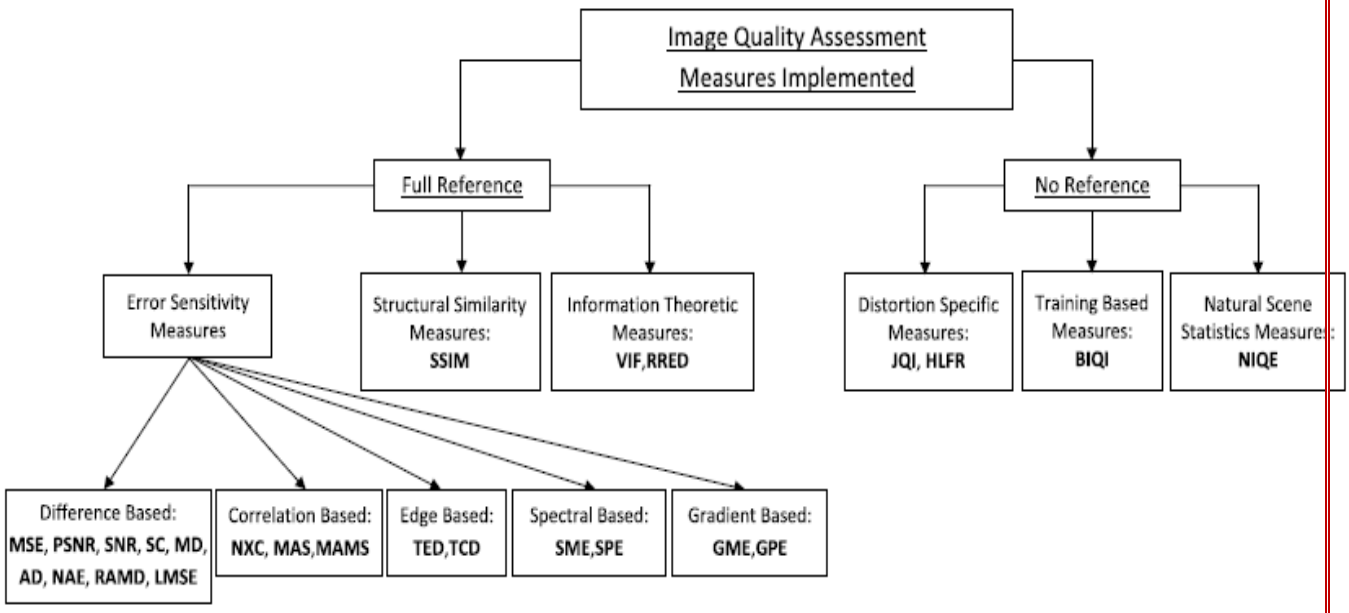


Fig 2: Image Quality Assessment Measures

1.3 Anti-Spoofing Approaches in Bio-metric Devices

Among the different threats analyzed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. 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 (e.g., gait, signature), to fraudulently access the biometric system

- Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements:
- Non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user;
- User friendly, people should not be reluctant to use it;
- Fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time;
- Low cost, a wide use cannot be expected if the cost is excessively high;
- Performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

1.4 Security Protection Method

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using 25 general image quality measures. A general diagram of the protection approach proposed in this work.

II. RELATED WORK

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research the publication of many research works disclosing and evaluating different biometric vulnerabilities, the proposal of new protection methods, the dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences, the organization of competitions focused on vulnerability assessment, the acquisition of specific datasets, the creation of groups and laboratories specialized in the evaluation of biometric security, or the existence of several European Projects with the biometric security topic as main research interest. All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics to the improvement of the systems security to bring this rapidly emerging technology into practical use. Among the different threats analyzed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact, or tries to mimic the behavior of the genuine user, to fraudulently access the biometric system. As this type of attacks is performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection is not effective. The aforementioned works and other analogue studies have clearly shown the necessity to propose and develop specific protection methods against this threat.

2.1 Biometric recognition: Security and privacy concerns

Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. But how secure is biometrics? And what are the privacy implications?

2.2 Artificial irises: Importance of vulnerability analysis

Because of wide area deployment, heterogeneity, dynamism, and other characteristics of large-scale distributed system (LDS), experimental environment supporting dynamic analysis is important for vulnerability analysis of LDS. In this paper, we summarize the requirements of experimental environment for LDS vulnerability analysis, propose and establish a universal emulation experimental environment for LDS vulnerability analysis, so-called LDSVAE (Large Distributed System Vulnerability Analysis Environment). By incorporating some novel techniques, including combined virtual and real network emulation, large-scale network topology automatic generation, image compression and long-distance reloading; LDSVAE provides a vulnerability analysis environment supporting wide area distribution and dynamic reconstruction for various types of LDS.

2.3 On the vulnerability of face verification systems to hill-climbing attacks

We use a hill-climbing attack algorithm based on Bayesian adaption to test the vulnerability of two face recognition systems to indirect attacks. The attacking technique uses the scores provided by the matcher to adapt a global distribution computed from an independent set of users, to the local specificities of the client being attacked. The proposed attack is evaluated on an eigenface-based and a parts-based face verification system

using the XM2VTS database. Experimental results demonstrate that the hill-climbing algorithm is very efficient and is able to bypass over 85% of the attacked accounts (for both face recognition systems). The security flaws of the analyzed systems are pointed out and possible countermeasures to avoid them are also proposed.

2.4 Biometric template security

Biometric recognition offers a reliable solution to the problem of user authentication in identity management systems. With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy of biometric technology. Public acceptance of biometrics technology will depend on the ability of system designers to demonstrate that these systems are robust, have low error rates, and are tamper proof. We present a high-level categorization of the various vulnerabilities of a biometric system and discuss countermeasures that have been proposed to address these vulnerabilities. In particular, we focus on biometric template security which is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting the template is a challenging task due to intrauser variability in the acquired biometric traits.

2.5 A high performance fingerprint liveness detection method based on quality related features

A new software-based liveness detection approach using a novel fingerprint parameterization based on quality related features is proposed. The system is tested on a highly challenging database comprising over 10,500 real and fake images acquired with five sensors of different technologies and covering a wide range of direct attack scenarios in terms of materials and procedures followed to generate the gummy fingers. The proposed solution proves to be robust to the multi-scenario dataset, and presents an overall rate of 90% correctly classified samples. Furthermore, the liveness detection method presented has the added advantage over previously studied techniques of needing just one image from a finger to decide whether it is real or fake.

III. SYSTEM DESIGN

3.1 System Architecture

Image quality assessment for liveness detection techniques used to detect the fake biometrics. Due to Image quality measurements it is easy to find out real and fake users because fake identities always have some different features than original it always contain different color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. Multi-Biometric system is challenging system. It is more secure than uni-biometric system. In this paper studied about the three biometric systems that are face recognition, iris recognition, fingerprint recognition, and the attack on these three systems. Multi biometric system is used for various applications. And in future for making this system more secures adding the one more biometric system into this system and trying to improve the system.

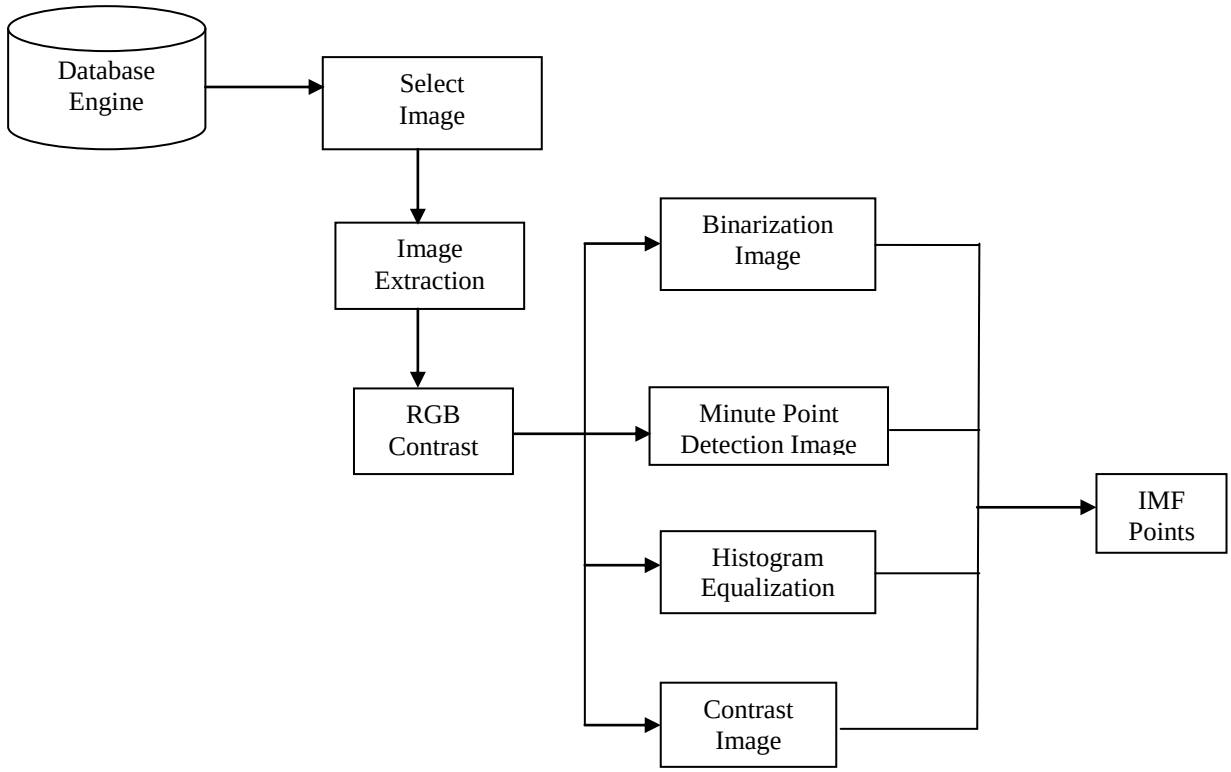


Fig.3 System Architecture

3.2 Modules

1. Liveness detection
2. Image Quality Assessment for Liveness Detection
3. Fingerprint Recognition
4. Iris Recognition
5. Face Recognition
6. Attacks on System

3.2.1 Liveness Detection

Liveness detection methods are generally classified into two types:

Software-based techniques, in this type the fake trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to differentiate between real and fake traits are extracted from the biometric sample, and not from the trait itself);

Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye liveness detection techniques, which use different physiological properties to differentiate between real and fake character.

3.2.2 Image Quality Assessment for Liveness Detection

The use of image quality assessment for liveness detection is motivated by the supposition that: "It is expected that 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." Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be unclear or out of focus due to trembling; face images captured from a mobile device will most likely be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local gaining artifacts such as spots and patches. Also, in an ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images.

3.2.3 Fingerprint Recognition

Multi Biometric System is use more than one biometric system for one multi biometric system for more security. Unibiometric system is easy to hack but multi biometric system is not easy to hack because one person does not obtain two traits of the same individual. This is the reason that multi biometric system is more secure than unibiometric system. How to work the multi biometric system? It contains the two steps

a. Enrolment on that Multi biometric first creates the data base of users.
b. verification on that when user try to gate access on the system then at that time first system captures the characteristic of the person then system match the input data to the data base sample.

And then person get authentication or conclude as a fake user. An introduction of application of biometric system used in this paper is face recognition system, fingerprint recognition system; iris recognition system shows multi-biometric recognition system.

Every fingerprint of each person is considered to be unique, Even the Twins also contain different fingerprint. Fingerprint recognition is the most accepted biometric recognition method. Fingerprints have been used from long time for identifying individuals. Fingerprints consist of ridges and furrows on the surface of a fingertip. Now fingerprint recognition system is used in iphone, there are many areas where the fingerprint recognition system used.

3.2.4 Iris Recognition

Iris Recognition Iris recognition is a computerized method of biometric identification which uses mathematical Model recognition techniques on video images of the irises of an individual's eyes, whose Complex random patterns are single and can be seen from some distance. Iris cameras perform detection of a person's identity. The iris scans process start to get something on film. It combines computer vision, statistical inference, pattern recognition and optics. The iris is the colored ring around the pupil of every human being and like a snowflake; no two are the same. Each one is unique.

3.2.5 Face Recognition

The most acceptable biometrics is Face reorganization. Because it is one of the most universal method of identification that human use in their visual interactions and acquisition of faces. The face recognition systems make different between the background and the face. It is most important when the system has to identify a face within a throng. The system then makes use of a person's facial features – its valleys and peaks and landmarks and treats these as nodes that can be compared and measured against those which are stored in the system's

database. There are approximately 80 nodes comprising the face print that makes use of the system and this includes the eye depth, jaw line length, distance between the eyes, cheek bone shape, and the width of the nose. It is very challenging to develop this recognition technique which can accept the effects of facial expressions, age, slight variations in the imaging environment.

3.2.6 Attacks on System

Attack on the face recognition system in that figure fake and genuine image are shown and that images are find out due to different method of face recognition. In face recognition system fake users attack on system by capturing the picture to the mobile devices or camera. And try to authenticate. But attackers attack on fingerprint recognition system. Attackers first capture real fingerprint then they make fingerprint by using silicon, plastic and gelatine and try to access the system. They show that how the fake fingerprint makes. An example of the images that can be found in this database, where the material lused for the creation of the fake fingers is specified system is as shown below.

To create a fake iris is of tree step

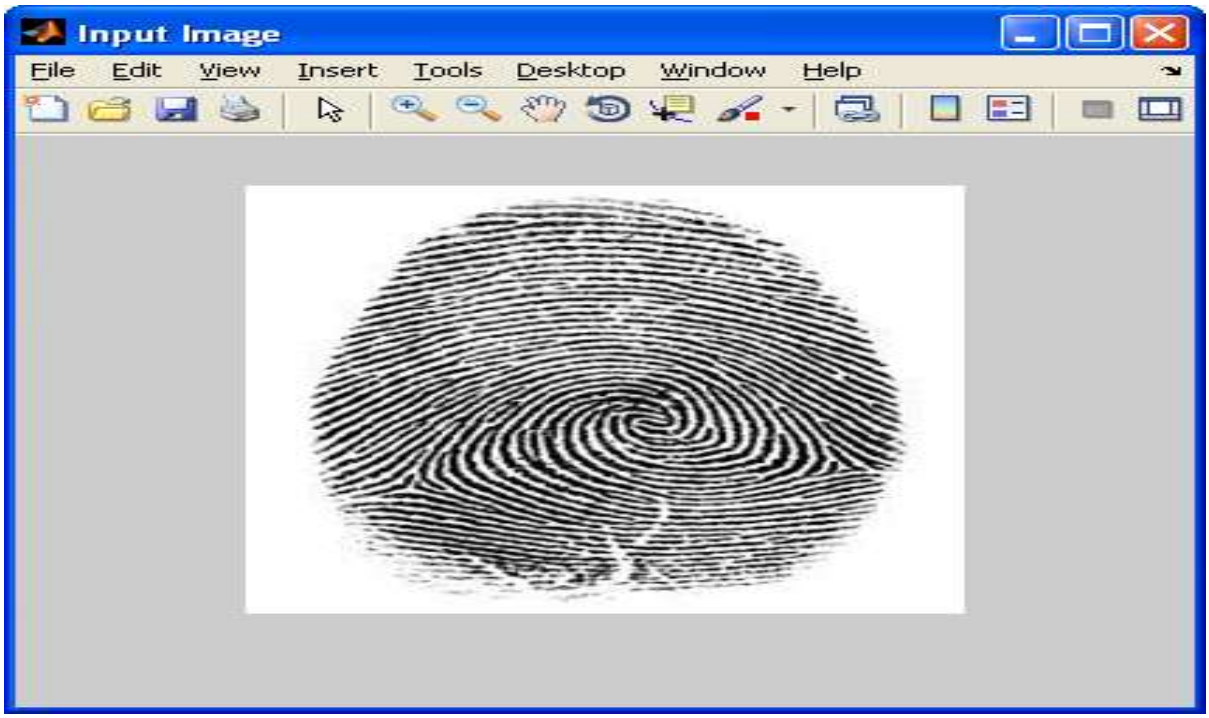
a) Original images are capture for a better quality, then

b) They are printed on a paper using a commercial printer

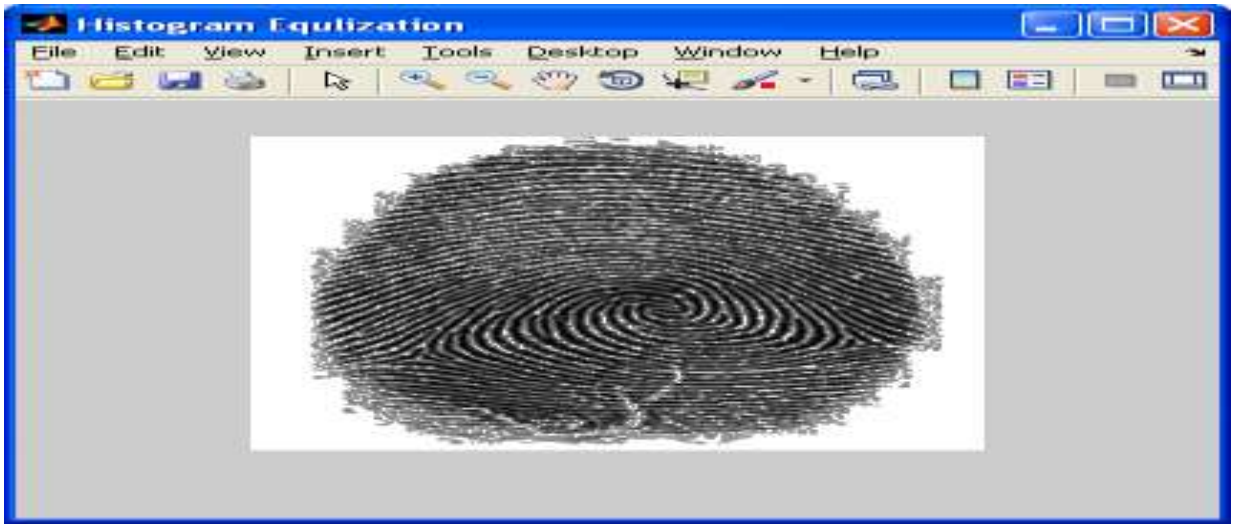
c) Printed images are presented at the iris sensor

3.3 Screen Shots

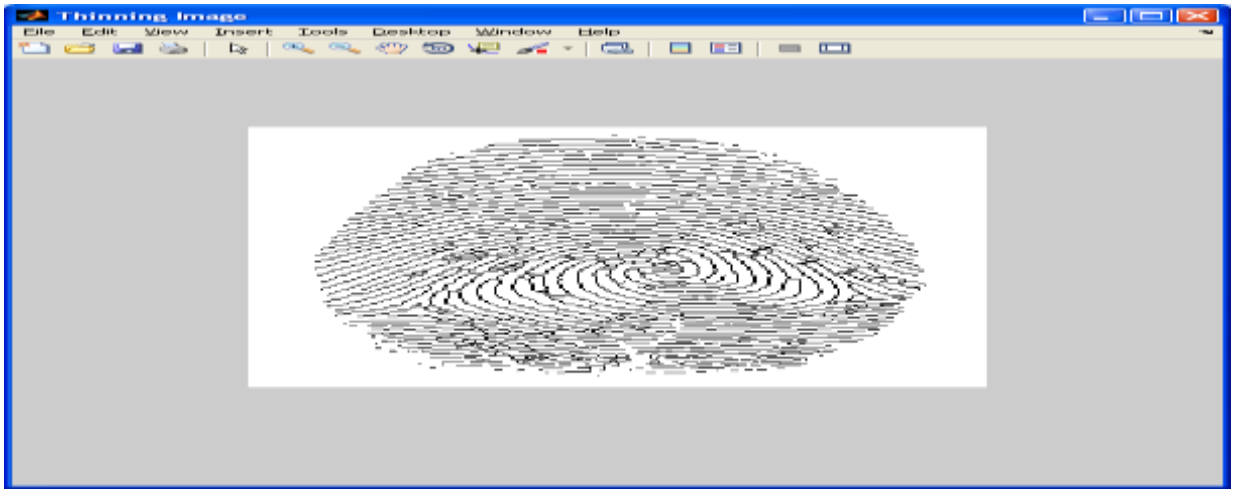
3.3.1 Gathering Input Data



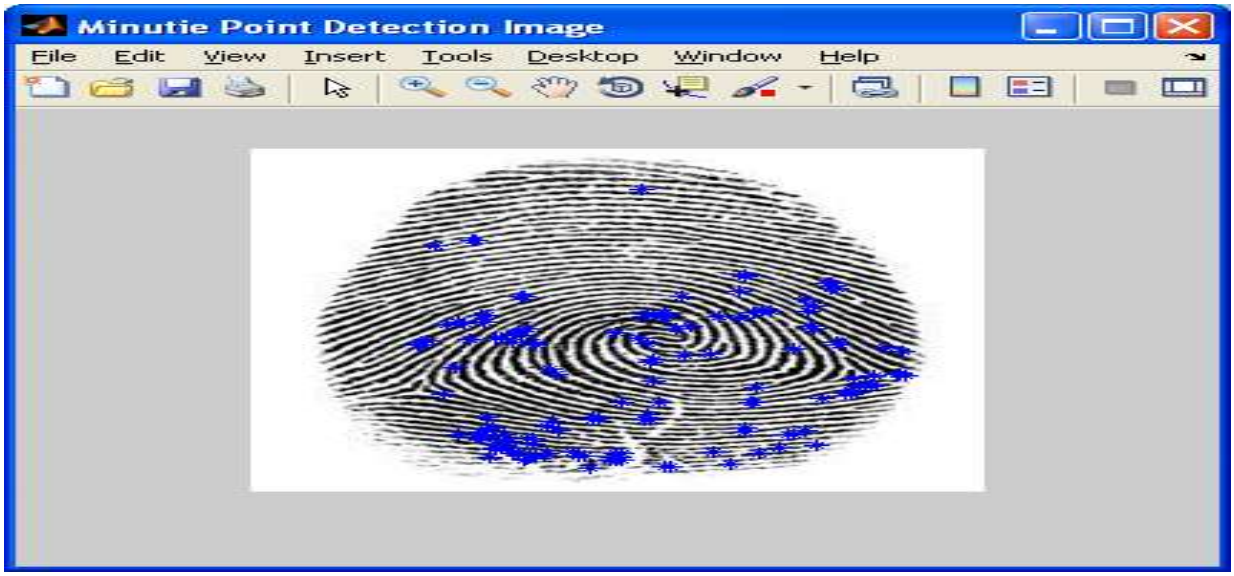
3.3.2 Histogram Equalization



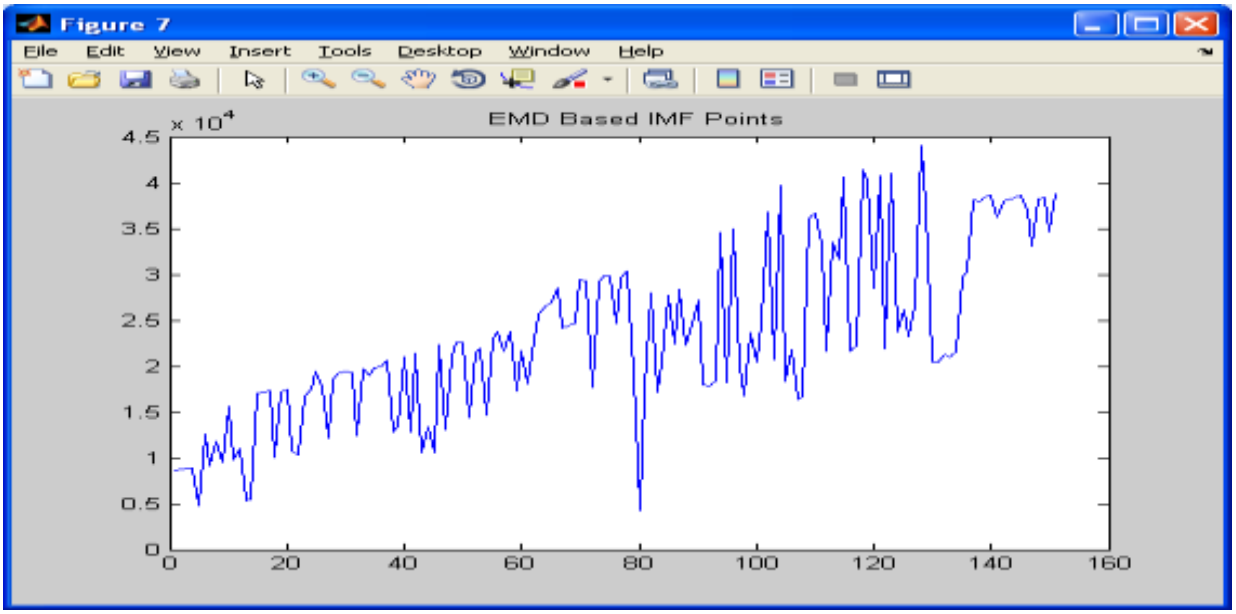
3.3.3 Thinning Image



3.3.4 Multipoint Detection



3.3.5 Performance Measures



IV. CONCLUSION

The proposed method is able to consistently perform a high level for different biometric traits ("multi-biometric"). It is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack"). The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios and the error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions. In addition to its very competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.

V FUTURE WORK

The Present System also opens new possibilities for future work, including: (a) extension of the considered 25-feature set with new image quality measures; (b) further evaluation another image-based modalities (e.g., palm-print, hand geometry, vein); (c) inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos); (d) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB); (e) analysis of the features individual relevance.

VI ACKNOWLEDGMENT

We would like to sincerely thank Assistant Prof. C.Dhanabal for his advice and guidance at the start of this article. His guidance has also been essential during some steps of this article and his quick invaluable insights have always been very helpful. His hard working and passion for research also has set an example that we would like to follow. We really appreciate his interest and enthusiasm during this article. Finally we thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

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

[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 Recognition., vol. 43, no. 3, pp. 1027–1038, 2010.

[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 Generation Computer System vol. 28, no. 1, pp. 311–321, 2012.

[6] M.A.Saad, A.C. Bovik and C.Charrier,"Blind image quality assessment: A natural sense statistics approach in the DCT domain".IEEETrans.Image Process, vol 21, no.8, pp.3339-3352, Aug 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.