Live Ness Detection for Biometric System using Image Quality Assessment

Prof. S.V.Shelke[1] Shubhangi Shingade[2] Namrata Shinde[3] Manisha Ghare[4]
[1,2,3,4]Department of Electronics & Telecommunication Engineering
[1,2,3,4]Bharati Vidyapeeth's College of Engineering for Women, Pune

Abstract— To verify the actual presence of real biometric sample in contrast to reconstructed (fake) samples is a major problem in biometric authentication, which needs the development of new and efficient protection method. In this paper we present a software based liveness detection method which can be used in different biometric systems to detect different types of fake attempts. The aim of the proposed system is to increase the security of the biometric system by adding live ness assessment using image quality assessment (IQA). The proposed system is less complex which is suitable for real time applications, by using general image quality features extracted from one image to differentiate between real and fake samples.

Key words: Attacks, Biometrics, Image Quality Assessment, Live ness Detection, Security

I. INTRODUCTION

Biometric is a fast growing technology to recognize the identity of a person using unique behavioral or physical traits such as face, fingerprint, retina, iris, signature, voice, gaits and hand or palm geometry etc. Although several advance techniques have been achieved in biometrics, several spoofing techniques have been developed to break the biometric systems and the security of such systems against attacks is still an open problem. These attacks are grouped into 8 classes:
1.Spoof attack (a fake biometric sample to the sensor), 2.Replay attack (replay of stored biometric signal), 3.Substitution attack, 4.Attack on genuine feature values (spoofing the biometric traits), 5.Denial of feature extraction (Trojan horse attack), 6.Attacks on template database, 7.Transmission attack (Attacking the channel between the database and matching), 8.Attacking on final result (accept/reject). All these attacks are due to technological advancement which reduces the security and reliability of biometric system. Hence it is required to guarantee a high level of security.

II. PROPOSED WORK

A. Liveness Detection

Liveness detection is one of the protection method against spoofing attacks. Liveness detection methods are classified into 2 groups:

Hardware Based Method (special sensor based): It uses physiological features of life in biometric sample such as facial expression changes, blood pressure, mouth movement, specific reflection properties of the eye, eye blinking, finger skin sweat etc, by adding special sensors to biometric systems. It present a higher fake detection rate but they are very costly and complex.

Software Based Method: In this method the fake trait is detected once the sample has been acquired with a standard sensor. It is less expensive than hardware based method as no extra device such as special sensor is needed, also it is fast, user friendly, non-invasive and having good fake detection rate. Hence this method is most preferable. In this work we present software based method.

B. Image Quality Assessment for Liveness Detection

Following assumption must be considered while using the image quality assessment for liveness detection- "It is expected that a genuine sample acquired and fake image captured will have different quality."These quality difference may include: degree of sharpness, color and luminance level, amount of information (entropy), local artifacts, natural appearance or structural distortions.

C. The Security Protection Method

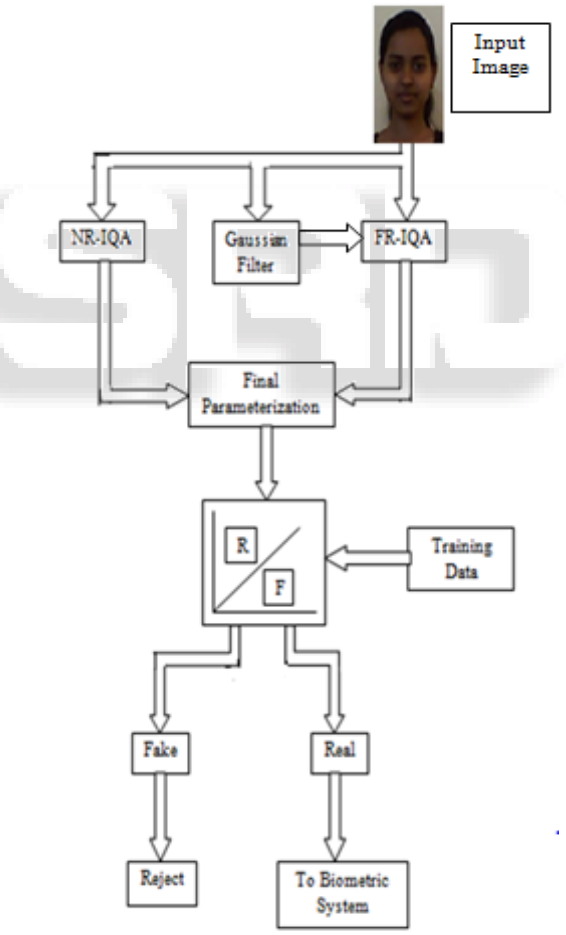

Fig. 1: Block Diagram of the Proposed System

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned as real or fake. The key point of the process is to calculate a set of features which helps to build an appropriate classifier which gives the probability of the image "originality". In the present work we propose a novel parameterization by using image quality measures. The diagram of the protection approach proposed in this

work is shown in Fig. 1. In order to keep its simplicity and generality, the system needs only one input. Furthermore, as the method operates on the full image with no searching for any trait-specific properties, it does not require any preprocessing steps (e.g. iris detection, fingerprint segmentation or face extraction) prior to the computation of the IQ features. These features reduces its computational load. As soon as the feature vector has been generated, the sample is classified as real or fake using some simple classifiers.

As shown in figure there are two main parts, first is feature extraction and second is classification. Full reference image quality measures are calculated using input image and its Gaussian filtered image and No reference image quality measures are calculated using only input image. Then final parametrization is done. Further with the help of classifier classification is done as real or fake. If it is fake then warning is given as fraudulent access attempt and access get denied. If it is real then it gives output as genuine user and passed to Biometric authentication system.

III. EXPECTED RESULT

1) It is expected that the proposed method should able to identify whether the given biometric sample is real or fake.
2) The proposed method should able to adapt to different types of attacks.
3) It should also able to generalize well to different databases, acquisition conditions and attack scenario.

IV. FUTURE SCOPE

The proposed system opens new possibilities for future work, including:

1) Extension of the feature set with new image quality measures
2) Further evaluation on other image-based modalities (e.g., palmprint, hand geometry, vein)
3) Inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos);
4) Use of video quality measures for video attacks.

V. CONCLUSION

Proposed system is able to detect whether given biometric sample is real or fake. This system enhances security as well as can be use for multi-biometric systems. It is user friendly, cost effective, less complex, time saving and faster.

REFERENCES

[1] Javier Galbally, Julian Fierrezvol and Sebastian Marce, Image Quality Assessment for Fake Biometric Detection: Application to Iris, fingerprint and Face Recognition, IEEE transactions on image processing vol.23, no. 2, February 2014.
[2] Prathamesh M. Sonavane, Fake Biometric Trait Detection Using Image Quality Features © 2015 IJEDR | Vol.3, Issue 2 | ISSN: 2321-9939.
[3] Ms. Kavita H. Waghmode, Dr. Prof. P.K. Ajmera, Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition IJIERT vol.2, issue 2 Feb.-2015.
[4] S.Hemalatha, Amitabh Wahi, A Study of Liveness Detection in Face Biometric Systems IJCA Vol.91 – No 1, April 2014.
[5] Pradnya M. Shende, Dr.Milind V. Sarode, Prof. Mangesh M. Ghonge, A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric IJCSET | April 2014 | Vol.4, Issue 4,129-132.

