IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 5, May 2015.
www.ijiset.com
ISSN 2348 – 7968

An Efficient Approach for Multi Biometric Fake Detection Mechanism for fingerprint, Face and Iris Recognition System

[1]K.Arunkumar.[2]Mrs. T.Viveka. M.E.,

[1]PG Student, Department of CSE, University College of Engineering, Nagercoil,

[2]Teaching Fellow of CSE Dept, University College of Engg. Nagercoil.

***Abstract*—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). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required).An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection),the computation load needed for image processing purposes is very reduced, using only *general* image quality measures fast to compute, combined with very simple classifiers. It has been tested on publicly available attack databases of iris, fingerprint and 2D face, where it has reached results fully comparable to those obtained on the same databases and following the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art.**

Index Terms - Image quality assessment, biometrics, security, Attacks.

1.INTRODUCTION

Fake biometrics means by using the real images (fig 1. iris images captured from a printed paper and fig 2. Fingerprint captured from a dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different type that are face recognition system, fingerprint recognition system, iris recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioral biometric). Figure 3 show the type of different biometric [6]. Multi biometric system means a biometric system is used more than one biometric system for one multi-biometric system. A multi biometric systemis use the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this Survey Base seminar report Image quality assessment for liveness detection

technique is used for find out the fake biometrics. Image assessment is force by supposition that it is predictable that a fake image and real sample will have different quality acquisition. 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, fig 1[5] shows iris images captured from a printed paper are more likely to be fuzzy or out of focus due to shaky; face images captured from a mobile device will almost certainly be over-or under -discovered; and it is not rare that fingerprint images which is shows in fig 2.[4] captured from a dummy finger. In addition in ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor, this fake sample will most probably not have some of the properties found in natural images.

Image quality assessment is a most important topic in the image processing area. Image quality is a trait of any image Usually compared with an ideal or perfect image. Digital images are subject to a large range of distortions during storage, achievement, compression, processing, transmission and reproduction, several of which may result in a degradation of visual quality. Imaging systems introduces some amount of distortion or artifacts which reduces the quality assessment. In general quality assessment is of two type one is subjective visual quality assessment and second one is objective visual quality assessment [2].Objective image quality metrics can be classified on the basis of availability of an original image, with the distorted image is to be compared. Accessible approaches are known as full-reference, meaning that a complete reference image is assumed to be known. In many practical applications, however, the reference image doesnot exist, and a no-reference or "blind" quality assessment approach is desirable.

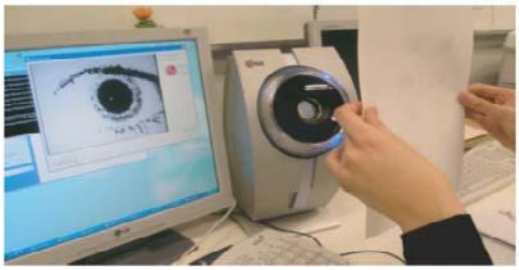

Fig 1[5]: Fake iris

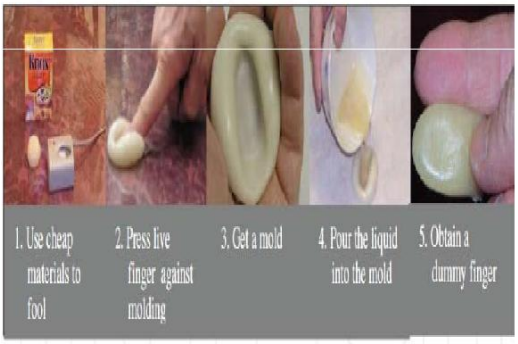

Fig 2[4]: fake fingerprints

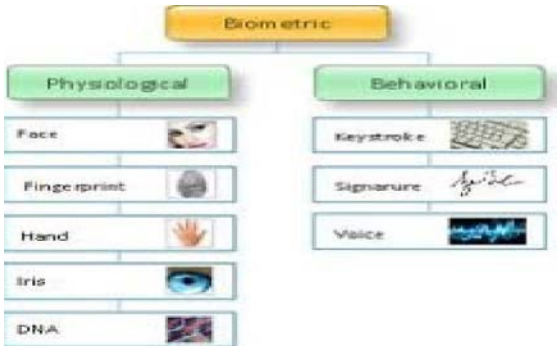

Fig 3[7]: Different types of biometric

2. LIVENESSDETECTIONMETHODS

Liveness detection methods are generally classified into two types (see Fig. 4): (*i*) *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); *(ii)Hardware-based* techniques, which add some particulardevice to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or

ISSN 2348 – 7968

specific reflection properties of the eye)[1].

liveness detection techniques, which use different physiological properties to differentiate between real and fake character. Liveness assessment methods represent a difficult engineering problem as they have to satisfy certain challenging requirements *(i)* user friendly, people should be averse to use it; *(ii)* fast, results have to be generate in avery less time interval as the user cannot be asked to interact with the sensor for a long period of time; *(iii)* low cost, a large use cannot be expected if the cost is very high; *(iv)* performance, in calculation to having a good fakedetection rate, the protection system should not degrade the recognition performance (i.e., false rejection) of the biometric system[1].

The two types of methods have certain advantages and disadvantages over the other and, in general, a combination of both would be the most advantageous protection approach to increase the security of biometric systems. As a common comparison, hardware-based schemes generally present a higher fake detection rate, at the same time software-based techniques are in general less expensive (like no extra device is needed), and less intrusive since their implementation is clear to the user. moreover, as they run directly on the acquired sample (and not on the biometric trait itself),

software-based techniques may be embedded in the feature extractor module which makes them potentially accomplished of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system against the addition of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor..

3.IMAGEQUALITYASSESSMENTFORLIVE-NESSDETECTION

The use of image quality assessment for liveness detection is motivated by the supposition that: “It is expected that a 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.”[1] 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 willmost likely lack some of the properties found in natural images.

The potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing).Different quality measures present diverse sensitivity to image artifacts and distortions. For example, measures like the mean squared error respond additional to additive noise, while others such as the spectral phase error are extra sensitive to blur; while gradient-related features respond to distortions concentratedaround edges and textures. Therefore, using a large range of IQMs exploiting complementary image quality properties should allow detecting the aforementioned quality differences between real and fake samples expected to be found in many attack attempts

ISSN 2348 – 7968

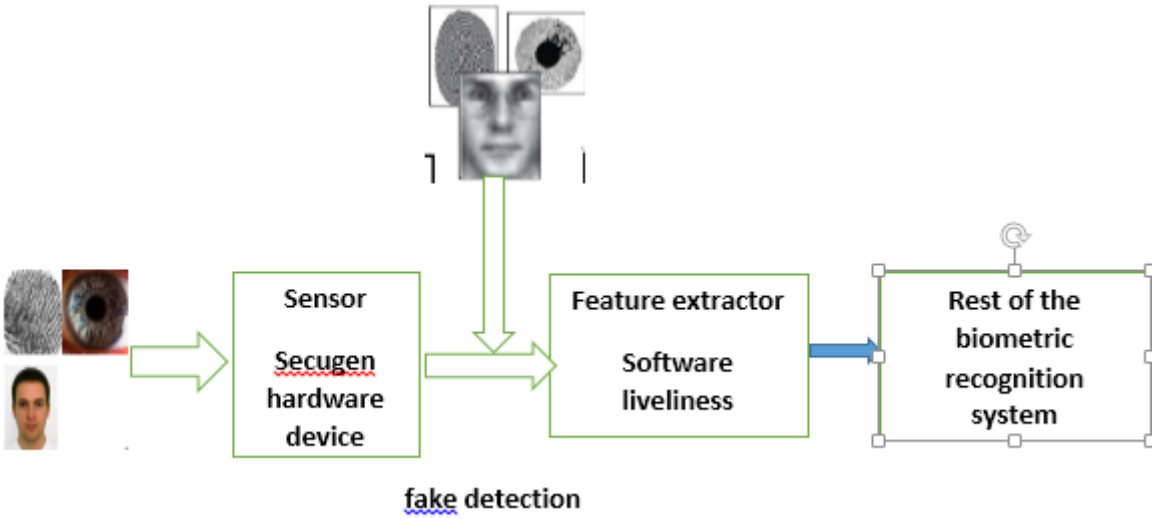

Fig 4.Types of attacks potentially detected by hardware based (Spoofing) and software-based (spoofing + reconstructed/synthetic samples) liveness detection techniques

(i.e., given that the technique with multi-attack protection capabilities). So consider that there is sound proof for the "quality-difference" theory and that image quality measures have the possible to achieve success in biometric protection tasks.

4. MULTIBIOMETRICSYSTEM

Multi Biometric system is use more than one biometric system for one multi biometric system for more security. Uni-biometric 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 (1) Enrollment on that Multi biometric first create the data base of users. And (2) 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 gate authentication or conclude as a fake user. An introduction of application of biometric system used in this paper are face recognition system, fingerprint recognition system, iris recognition system. Fig (5) shows multi-Biometric recognition system.

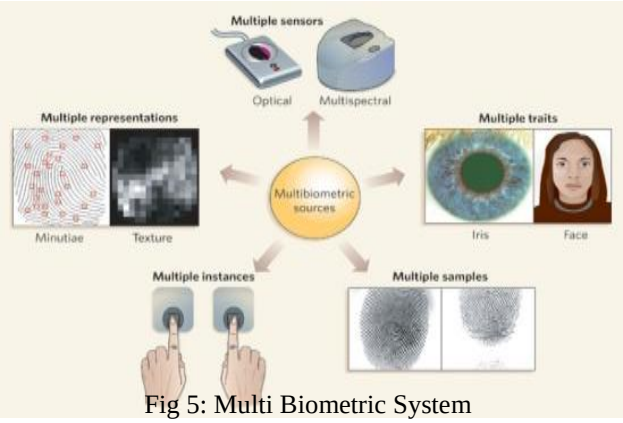

Fig 5: Multi Biometric System

4.1 Face recognition and attack on system

The most acceptable biometrics is Face reorganization, because it is one of the most universal methods of identification that humans 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

ISSN 2348 – 7968

are approximately 80 nodes comprising the face print that makes use of the system and this includes the eye socket depth, jaw line length, distance between the eyes, cheekbone 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.

Attack on the face recognition system is shown in the following figure 6[1] 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.

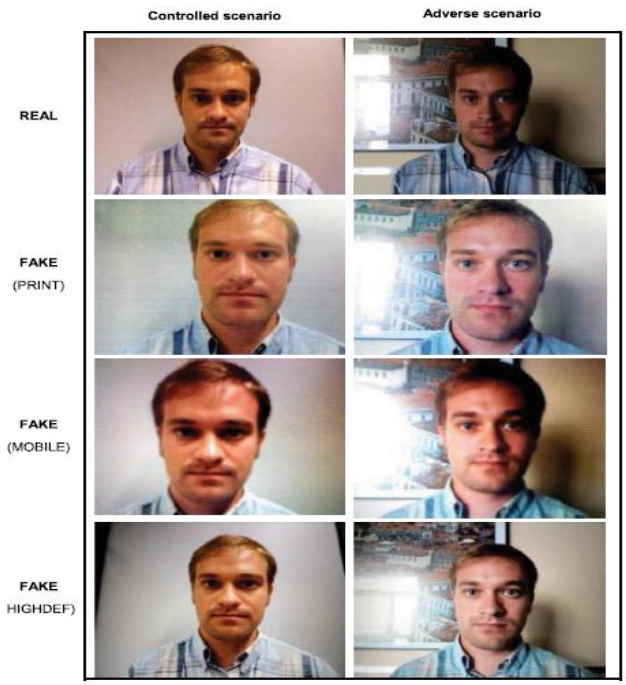

Fig 6[1]: Typical examples of real and fake (print, mobile) face images.

4.2 Fingerprint recognition and attacks on 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. But attackers attack on fingerprint recognition system. Attackers first capture real fingerprint then they make fake fingerprint by using silicon, playdoh and gelatin and try to access the system. The figure 2[1] show that how the fake fingerprint make. Examples of the images that can be found in this database are shown in Fig. 7[1], where the material used for the creation of the fake fingers is specified(silicone, gelatin or playdoh). Figure 2 Show how to make the fake fingerprint [4].

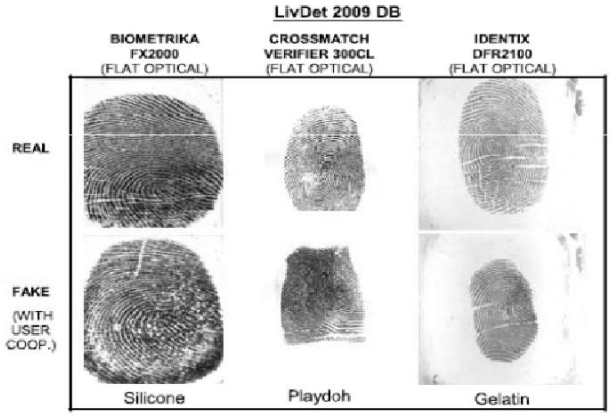

Fig 7[1]: Typical examples of real and fake fingerprint images.

4.3 Iris Recognition attacks on system

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 [6]. Each one is unique.An attack on the iris is not so easy but how to attack on the system is as shown below.

To create a fake iris is of tree step

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

2) They are printed on a paper using a commercial printer(see fig 8)

3) Printed images are presented at the iris sensor. Theprocess is seen in the figure 1.

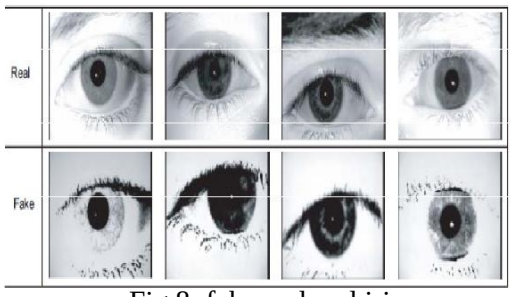

Fig 8: fake and real iris.

4.4 ***Advantages of Multi-biometric Systems over aunibiometric system***

Better Security-The multi-biometric system increases the security level. Unibiometric system is easy to attack but the multi-biometric system is not so easy because attacker cannot obtain two traits of the same individual. More secure than other system.Multiple Fingerprint scanner support. Multiple IRIS Scanner support.

4.5 Application

Multi-biometric system is used in India for making Aadhar card this multi-biometric system is used face recognition, iris recognition, and fingerprint recognition [7].Multi-biometric system used in Airport.Multi-biometric system is used in banking.

5. **CONCLUSION**

Image quality assessment for liveness detection technique is 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 unibiometric 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.

6. REFERENCES

[1] Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez vol. 23, no. 2, February 2014

[2] International Journal of Computer Applications Technology and Research Volume 2– Issue 3, 250 - 254, 2013 .

[3] 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.

[4] Fingerprint Spoof Detection Using Near Infrared Optical Analysis,Shoude Chang1, Flueraru1 and Wahab Almuhtadi3 *1Institute,* Kirill V. Larin2, Youxin Mao1, Costel,in *Proc. IAPR ICIAP*, Springer LNCS-5716. 2010, pp. 12–23.

[5] Direct Attacks Using Fake Images in Iris Verification Virginia Ruiz- Biometric Recognition Group – ATVS Escuela Politecnica Superior - Universidad Autonoma de Madrid Avda. Francisco Tomas y Valiente, 11 - Campus deCantoblanco28049 ,http://atvs.ii.uam.es

[6] International Journal of Computer Science, Engineering and Information Technology

ISSN 2348 – 7968

(IJCSEIT), Vol.2, No.1, February 2012 DOI : 10.5121/ijcseit.2012.2106 57 biometrics authentication technique for intrusion detection systems using fingerprint recognition. Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode 3 1, 2& 3 Department of Computer Science &