Fake Biometric Detection Using Liveness Detection System Applications: Iris and Fingerprint Recognition System

Pradnya M. Shende[1] , Dr.Milind V. Sarode[2]
[1] *M.E. (comp. Sci. Engg), J. C. O.E. T. Yavatmal, India,* shende_pradnya@rediffmail.com,
[2] *H. O. D. (Comp. Engg.), J. C. O.E. T. Yavatmal, India,* parthmilindsarode@rediffmail.com

Abstract: To make sure the actual presence of a real justifiable feature in difference to a fake self-manufactured artificial or reconstructed trial is a major problem in biometric authentication, which requires the development of novel and efficient protection measures. In this paper, here a novel software-based fake detection method is used in iris and fingerprint recognition systems to detect different types of fake access attempts. The purpose of the proposed system is to improve the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-invasive manner.
KeyWords: -Biometric, Liveness Detection, Attacks, Feature Extraction.

1. INTRODUCTION

Biometric system has gained extensive range of applications in security field. Biometric systems communicate on the biometric uniqueness or data taken from the user for authentication [1]. Such biometric data is stolen or duplicated by unauthorized users. Most of the biometrics systems depend on identifying the physiological uniqueness of the user. It becomes easier to spoof in these biometric systems with the help of fake biometric; it further reduces the reliability and security of biometric system. Among the different accessible biometric traits, iris and fingerprint recognition systems have been usually regarded as two of the most reliable and precise [2, 3]. This reality has led researchers to disburse special attention to its vulnerabilities and in exacting to analyze to what extent their security level may be compromised by spoof in attacks. These attacking methods consist on presenting an unnaturally generated iris and fingerprints to the sensor so that it is recognized as the legal user and access is decided. That's way in this paper for improving security level uses the liveness detection system. Information about biometric and multi-biometric is describe in section 1.1, types of multi-biometric that are iris and fingerprint is describe in section 1.2, types of attack describe in section 1.3, liveness detection is describe in section 1.4.

1.1 BIOMETRIC AND MULTI-BIOMETRIC

Biometrics makes use of biological conditions that deals with data statistically. It verifies a individual's uniqueness by analyzing his physical characteristics or behaviors (e.g. fingerprint, voice, face, signature, keystroke rhythms). The systems trace data from the user and match up to it each time the user is claimed. A biometric system is a computer system that implements biometric detection algorithms. A usual biometric system consists of sensing, feature extraction and matching modules.

We can classify the biometric techniques into two classes:

- **Physiological based techniques** contain fingerprint, hand geometry, facial analysis, retinal analysis, DNA and measure the physiological characteristics of a person.
- **Behavior based techniques** contain key stroke, voice, smell, signature, sweat pores analysis and measure behavioral characteristics.

Biometric recognition systems based on the above methods and work in two modes: *identification* mode, there is the system identifies a person penetrating a large data base of enrolled for a match; and *authentication* mode there is the system verifies a individual's claimed identity from his previous enrolled pattern. The categories of biometrics systems are shown in figure 1[6].

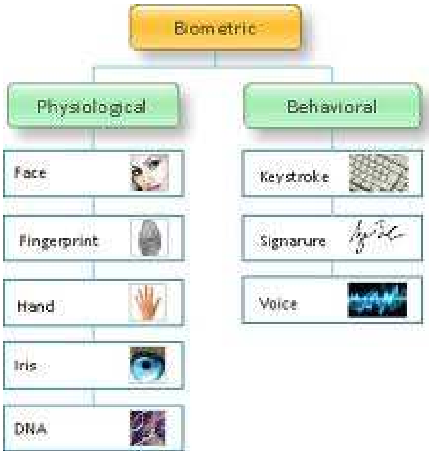

Figure 1 Categories of biometric [6]

Multiple characters of an individual, or multiple feature extraction and matching algorithms working on biometric. This types of systems is known as multi-biometric systems, which is get better the matching accuracy of a biometric system while rising inhabitants coverage and deterring spoof attacks.

1.2 TYPES MULTI-BIOMETRIC USED IN THIS PAPER

- **IRIS RECOGNITION**

Iris recognition is an automatic method of biometric which uses mathematical model recognition techniques on video images of the irises of an individual's eyes, whose multifaceted random patterns are sole and can be seen from some distance. Iris cameras carry out recognition of a person's identity by analysis of the random patterns that are observable within the iris of an eye from some distances. It combines computer apparition, pattern detection, arithmetical inference and optics. The iris is the colored ring around the pupil of every human being and similar to a snowflake, no two are the same. Each one is unique iris, exhibiting a unique form. The figure 2 shows what is mean by iris.

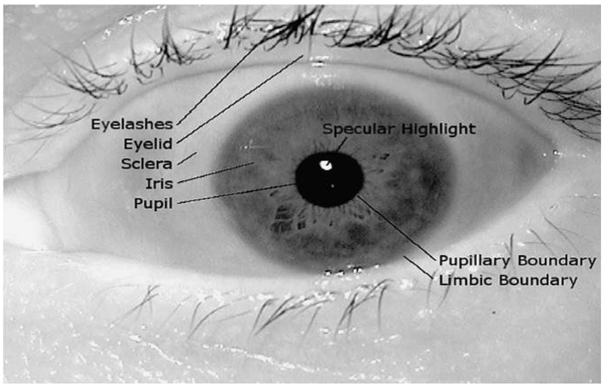

Figure 2 Information about eye.

- **FINGERPRINT RECOGNITION**

Fingerprint detection explains the process of obtaining a digital demonstration of a fingerprint and comparing it to a stored digital version of a fingerprint. Between all biometric techniques, finger-print recognition is the most accepted system due to the following advantages:
1) High uniqueness—identical twins who have the same DNA but different fingerprints
2) Universality—the size of the inhabitants with legible finger-prints exceeds the size of the inhabitants with passports.
3) High management—at the age of seven months, a fetus's fingerprint is fully developed, and fingerprint uniqueness does not change in the lack of injury or skin disease. Nevertheless, after a small injury to a fingertip, the pattern will grow back as the fingertip heals. Fingerprints are classified into six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop which is shown in figure 3 [7].

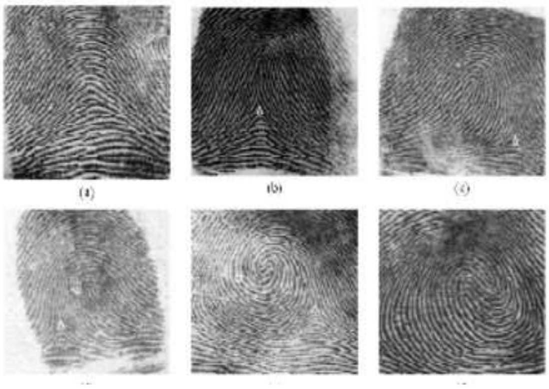

Figure 3 Classification of fingerprint [7].

1.3 TYPES OF ATTACK

Recognized and classified eight probable attack points to biometric recognition systems. These vulnerability points, is shown in Figure 4, can broadly be separated into two main groups:

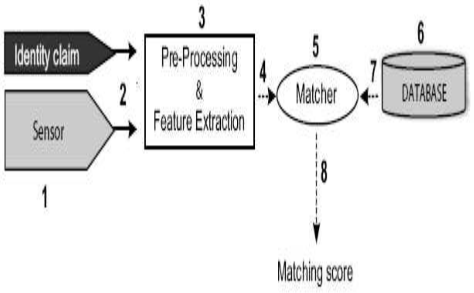

Figure 4 Architecture of biometric verification system. Possible attack points are numbered from 1 to 8.

- **DIRECT ATTACKS: -**The sensor is attack with artificial biometric samples, e.g. gummy fingers (point 1 in Figure 4). It is significance note that in this type of attacks no exact knowledge regarding the system is wanted. Moreover, the attack is carried out in the analog domain, outside the digital restrictions of the system; there for digital security mechanisms (watermarking, digital signature, etc) cannot be used.

- **INDIRECT ATTACKS: -** This group having all the remain seven points of attack indentified in Figure 4. Attacks 3 and 5 might be carried out by means of a Trojan Horse that bypasses the system modules. In attack 6, the method database is manipulated. The remaining points of attack (2, 4, 7 and 8) take advantage of possible feeble points in the communication channels of the method. In resistance to direct attacks, in this type the impostor needs to have some extra information about the internal operational of the system and, in large cases, physical access to some of the application mechanism.

1.4 LIVENESS DETECTION SYSTEM

A new liveness detection system for iris and fingerprints is presented. The liveness detection technique presented has the additional advantage over previously studied systems of needing just multi-Biometric i.e. iris and fingerprint image (the same used for authentication) to make a decision whether it comes from a real or fake. General diagram of the liveness detection system presented in this work is as shown in figure 5.

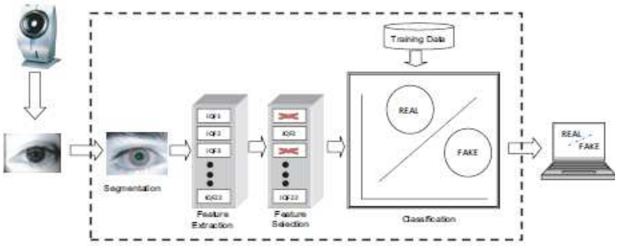

Figure 5 General diagram of the liveness detection system [4].

Liveness measurement methods symbolize a challenging engineering problem as they have to satisfy certain difficult requirements [1]: (*i)* low cost, a broad use cannot be predictable if the cost is extremely high; *(i i)* user friendly, people should not be unwilling to use it; *(i i i)* speedy, results have to be formed in a very less time as the user cannot be asked to act together with the sensor for a long period of time; *(i)* non-invasive, the system should in no case be unsafe for the individual or require an too much contact with the user; *((v)* performance, in addition to having a good fake recognition rate, the protection system should not humiliate the recognition performance (i.e., false rejection) of the biometric system. Liveness detection methods are typically classified into one of two groups [4].

- **HARDWARE-BASED TECHNIQUES**

Hardware-based techniques which add some extra 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) [4].

- **SOFTWARE-BASED TECHNIQUES**

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 differentiate between real and fake individuality are extracted from the biometric sample, and not from the trait itself) [4].

2. LITERATURE REVIEW

Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez and Javier Ortega-Garcia this are the scientist who done work on A liveness detection scheme for iris based on quality related measures is presented. The novel anti-spoofing technique is experienced on a database comprising greater than 1,600 real and fake (high quality printed images) iris samples proving to have a very elevated possible as an effectual protection system against direct attacks.The liveness recognition method presented one iris image (the same used for verification) to make a decision where it is real or fake eye [1].

Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega-Garcia this are the scientist who done work on a new fingerprint parameterization for liveness detection based on quality measures is presented. The novel characteristic set is used in a whole liveness detection system and experienced on the development set of the LivDET competition, comprising greater than 4,500 real and fake images acquired by means of three different optical sensors. The proposed key proves to be vigorous to the multi-sensor situation, and. The liveness detection method presented has the additional advantage over existing studied techniques of needing just one image from a finger to make a decision where it is real or fake [8].

Gian Luca Marcialis, Aaron Lewicke, Bozhao Tan, Pietro Coli1, Fabio Roli1, Stephanie Schuckers, Dominic Grimberg, Alberto Congiu1, Alessandra Tidu1 and the LivDet 2009 Group those are done work on Software based fingerprint liveness detection. Fingerprint recognition systems are vulnerable to artificial spoof fingerprint attacks, like molds made of silicone, gelatin or Play-Doh. "Liveness detection", which is to identify energy information from the biometric cross itself, has been proposed to overcome these kinds of spoof attacks. The objective for the LivDet 2009 competition is to evaluate different methodologies for software based fingerprint liveness detection with a universal experimental protocol and large dataset of spoof and live images. The performance was calculated for three datasets, from three unlike optical scanners, each with greater than 1500 images of "fake" and over 1500 images of "live" fingerprints. To increase the visibility of this vital research area in order to reduce risk of fingerprint systems to spoof attacks [9].

Hui Zhang, Zhenan Sun, Tieniu Tan, Jianyu Wang this are the scientist who done work on Iris pattern representation method namely hierarchical visual codebook (HVC) is proposed to encode the characteristic and robust texture primitives of genuine and false iris images. so, it can get less visual code quantization error, capture salient texture pattern lightly, and reduce the dependence on coding at the upper level of vocabulary tree. [10].

3. ANALYSIS OF PROBLEM

The requirement of strong secure biometric system for the person authentication and more secure biometric system for more relevant in this paper add liveness detection system.

Again the difficulties are:

- The source of Database that supports to the system.
- The speed of detection of the fake biometric.
- The main problem is to compare the iris and fingerprint feature with the database iris and fingerprints sample and give the appropriate result which is fake or real iris and fingerprints.
- Fake iris images captured from plastic eyes are difficult to recognize because the artificial cover may cause texture deformation.
- Method is not support a very high performance of test database.
- Method not measures the ratios of pupil and iris radius or areas. And more difficulties to the liveness classification problem.

4. PROPOSED WORK

The New protocol has been designed with a two-fold objective:

1. First, estimate the "iris and fingerprint Biometric Recognition" measurement of the protection method. That is, its capability to accomplish a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose two of the most comprehensive

image-based biometric modalities have been considered in the experiments: iris and fingerprints.

2. Second, calculate the “multi-attack” measurement of the security method. That is, its capability to identify not only spoofing attacks (such as additional liveness detection specific approaches) but also fake access attempts carried out with artificial or reconstructed samples**.**
3. After going through the analysis of these iris and fingerprint recognition systems, their limitations in terms of security and time response, accuracy of results, importance of the outcome and relevancy of results are overcome in the implementation.
4. An efficient approach is proposed in which first there is increasing the security level and person authentication.
5. The suitable technique can be integrated with any of the iris and fingerprint recognition system to produce better and relevant results.
6. Analysis of Result.
7. Steps of the proposed work.

The figure which is as shown in figure 6 is described as:

First Step:

1. By using iris and fingerprint scanner detect the iris and fingerprint of individuals.
2. Extract the features of iris and fingerprint of individuals.
3. Generate the templates of iris and fingerprints.
4. Create the DataBase.

Second Step:

1. By using iris and fingerprint scanner detect the iris and fingerprint of individuals.
2. Extract the features of iris and fingerprint of individuals.
3. Generate the templates of iris and fingerprints.
4. Generated template matched with given DataBase.
5. Used liveness detection system in this step calculate the Iris radius Plus movement of Iris and Rigidness and continue lines in fingerprints plus measure the fingers tip pressure when user used fingerprint scanner.
6. Calculate variations in features.
7. If there is no variation found then person get access to the system or we say that person is authenticated.
8. If there isvariation fount detects that by using liveness detection.
9. If noise characteristics are found then that is remove by filter used in liveness detection system.
10. And then again identify the person is genuine or not.
11. If genuine then get access to the system.
12. And if not genuine then reject the person or declered that person is not authenticated.

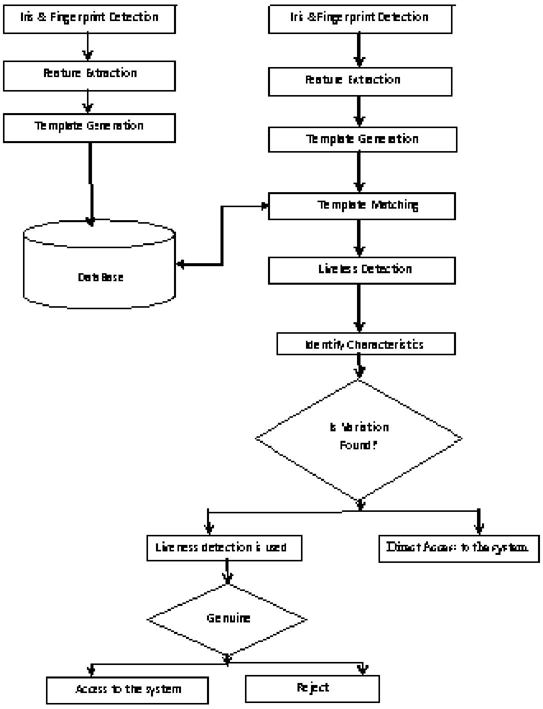

Figure 6 Graphical representation of proposed work

5. CONCLUSION

Multi-Biometric system is more secure than biometric system. This paper used liveness detection technique to detect the fake biometrics. Due to liveness detection technique it is easy to find out real and fake users because fake identities always have some unlike characteristics than original. It is more secure than unibiometric system.

REFERENCES

[1] Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez and Javier Ortega-Garcia ATVS Biometric Recognition Group,"Iris Liveness Detection Based on Quality Related Features" Universidad Autonoma de Madrid C/ Francisco Tomas y Valiente 11, 28049 Madrid. SPAIN.javier.galbally, jaime.ortiz, julian.fierrez, javier.ortega@uam.es

[2] Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode 3 1, 2& 3 Department of Computer Science & Engineering, Amravati University, India."biometrics authentication technique for intrusion detection systems using fingerprint recognition." International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012 DOI : 10.5121/ijcseit.2012.2106 57

[3] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia Biometric Recognition Group – ATVSEscuela Politecnica Superior - Universidad Autonoma de Madrid Avda. Direct "Attacks Using Fake Images in Iris Verification"Francisco Tomas y Valiente, 11 - Campus de Cantoblanco 28049 Madrid, Spain {virginia.ruiz,pedro.tome,fernando.alonso,javier.galbally,julian.fierrez,javier.ortega}@uam.es http://atvs.ii.uam.es

[4] Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez."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,

[5] Gian Luca Marcialis1, Aaron Lewicke2, Bozhao Tan2, Pietro Coli1, Fabio Roli1, Stephanie Schuckers2, Dominic Grimberg2, Alberto Congiu1, Alessandra Tidu1 and the LivDet 2009 Group* "First International Fingerprint Liveness DetectionCompetition—LivDet 2009"

[6] Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode 3 "BIOMETRICS AUTHENTICATION TECHNIQUE FOR INTRUSION DETECTION SYSTEMS USING FINGERPRINT RECOGNITION" International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012 DOI : 10.5121/ijcseit.2012.2106 57

[7] MUDHOLKAR S.S.*, SHENDE P.M., KHARAT V.P. AND KHODWE S.S. "FINGERPRINT RECOGNITION SYSTEM FOR INTRUSION DETECTION "Journal of Pattern Intelligence ISSN: 2230-9330 & E-ISSN: 2230-9349, Volume 2, Issue 1, 2012, pp.-22-25.

[8]]Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega-Garcia "Fingerprint Liveness DetectionBased on Quality Measures" Biometric Recognition Group–ATVS, EPS, Universidad Autonoma de Madrid,C/ Francisco Tomas y Valiente 11, 28049 Madrid, SpainEmail: ƒjavier.galbally, fernando.alonso, julian.fierrez, javier.ortegag@uam.es

[9] Gian Luca Marcialis1, Aaron Lewicke2, Bozhao Tan2, Pietro Coli1, Fabio Roli1, Stephanie Schuckers2, Dominic Grimberg2, Alberto Congiu1, Alessandra Tidu1 and the LivDet 2009 Group* "First

[10] Hui Zhang1,2, Zhenan Sun2, Tieniu Tan2, Jianyu Wang1,2 1."Learning Hierarchical Visual Codebook for Iris Liveness Detection" Shanghai Institute of Technical Physics, Chinese Academy of Sciences 2.National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences {zhanghui,znsun,tnt}@nlpr.ia.ac.cn, jywang@mail.sitp.ac.cn