International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-3, May, 2019

New Anti-Spoofing Approach for Biometric Device with Liveness Detection

SushmaChowdaryPolavarapu
Assistant Professor, Dept. of EIE, V.R. Siddhartha Engg. College, Vijayawada, Krishna Dist., A.P
sushmachowdaryp@gmail.com

UmamaheswariKunduru
Assistant Professor, Dept. of EIE, V.R. Siddhartha Engg. College, Vijayawada, Krishna Dist., A.P
kunduru.uma@gmail.com

Sri HariNallamala
Assistant Professor, Dept. of CSE,
DVR &Dr.HS MIC College of Technology,
Kanchikacherla, A.P.
nallamala.srihari@gmail.com

Abstract: The deployment of fingerprint sensors is increasingly becoming common and has now gained high user acceptance. However, fingerprint sensors are susceptible to spoofing using artificial materials or in worst case to the dismembered fingers. This paper proposes a new method of anti-spoofing using reliable liveness detection. The proposed method of liveness detection is based on the pulse sensor and changes in the volume of blood in an organ are measured by the changes in the intensity of the light passing through that organ, determines the liveness of the enrolled biometric. Our experimental results demonstrate that the developed prototype can successfully thwart the spoof attacks (those based on dismembered fingers).The GSM module is used for notification of authorized or unauthorized access of fingerprint system.

Keywords: Biometrics, Biometric Identification System, Finger Print, Spoofing Methods, Anti-Spoofing Methods.

I. INTRODUCTION

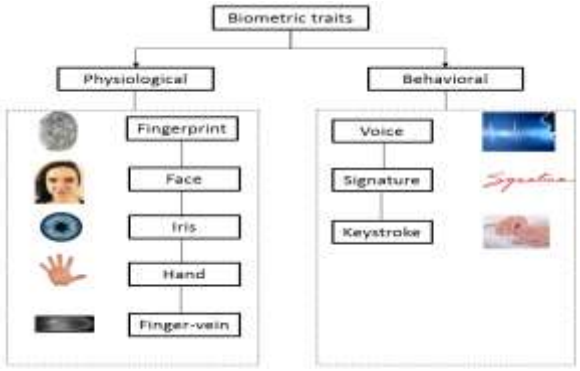
Biometrics systems aim to determine or verify the identity of an individual from their behavioural and/or biological characteristics. Biometrics already forms a significant component of current and emerging identification technologies [1]. Despite significant progress, some biometric systems fail to meet the multitude of stringent security and robustness requirements to support their deployment in some practical scenarios. Despite their appeal, however, biometric systems are vulnerable to malicious attacks. Among them are spoofing attacks, also referred to as presentation attacks, which refer to persons masquerading as others in order to gain illegitimate access to sensitive or protected resources.

A. BIOMETRIC IDENTIFICATION SYSTEM

Biometric Identification System is widely used for unique identification of humans. Biometrics is used as a form of identity access management and access control. Applications include criminal identification, airport checking, computer or mobile device log-in, transaction authentication, voice mail and secure tele-working.

BIOMETRIC MODALITIES

Each biometric information that can discriminate individuals is considered as a biometric modality. An example of biometric modalities is presented in fig. 1.1



Ideal biometric information should respect the following properties as shown in table 1.1:

- Universality (U): All individuals must be characterized by this information.
- Uniqueness (N): This information must be as dissimilar as possible for two different individuals.
- Permanency (P): It should be present during the whole life of an individual.
- Collectability (C): it can be measured in an easy manner.
- Acceptability (A): it concerns the possibility of a real use by users.

Table 1.1: Evaluation of biometric modalities

Information	U	N	P	C	A
DNA	Yes	Yes	Yes	Poor	Poor
Gait	Yes	No	Poor	Yes	Yes
Keystroke dynamics	Yes	Yes	Poor	Yes	Yes
Voice	Yes	Yes	Poor	Yes	Yes
Iris	Yes	Yes	Yes	Yes	Poor
Face	Yes	No	Poor	Yes	Yes
Hand geometry	Yes	No	Yes	Yes	Yes
Fingerprint	Yes	Yes	Yes	Yes	Fair

FINGERPRINTS

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life. Ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction. Figure 1.2 illustrates an example of a ridge ending and a bifurcation. In this example, the black pixels correspond to the ridges, and the white pixels correspond to the valleys as shown in figure 1.2.

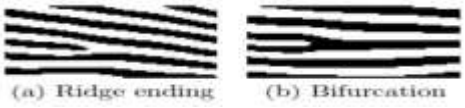


Figure 1.2: Example of ridge ending and bifurcation

IMPORTANCE OF FINGERPRINTS

Fingerprints are considered to be the best and fastest method for biometric identification. They are secure to use, unique for every person and do not change in one's lifetime. Besides these, implementation of fingerprint recognition system is cheap, easy and accurate up to satisfactory. Fingerprint recognition has been widely used in both forensic and civilian applications. Compared with other biometrics features, fingerprint-based biometrics is the most proven technique and has the largest market shares [2]. Not only it is faster than other techniques but also the energy consumption by such systems is too less.

PATTERNS OF FINGERPRINTS

The fingerprint patterns could be described as having three basic patterns as shown in figure 1.3.The ridges of the finger run continuously from one side of the finger to the other and make no backward turn [3].

Figure 1.3: Patterns of fingerprints

IDENTIFICATION OF FINGERPRINT

The fingerprint can be identified based on various minutiae as illustrated in figure 1.4.

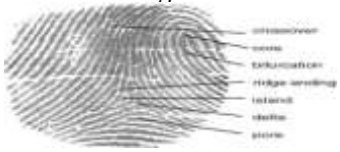


Figure 1.4 Fingerprint

B. SPOOFING METHODS

The method of attacking fingerprint systems by presenting artificial objects tothe sensor is known as spoofing. There are two main methods for fingerprint spoofing

CO-OPERATIVE SPOOFING

In co-operative spoofing, we have "Direct mold spoofing method". In this method, the spoof is formed using a live finger mold. We can use plastic material to obtain the mold and gelatine for the cast. The spoof fingerprints are usually made up of materials (like play-doh, clay, and gelatine) which are easy to scan by commercial fingerprint scanner. This duplication of fingerprint is a co-operative process as the real owner participates in creation as spoof finger prints[4].In Direct mold, the finger is pressed on a surface and negative impression of fingerprint is fixed and mold is taken. The mold is then filled with moisture based material and spoof is formed.

NON CO-OPERATIVE SPOOFING

There are four types of non co-operative spoofing as shown in figure 1.5.

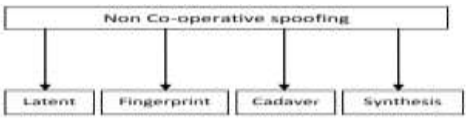


Figure 1.5: Types of non co-operative

- **Latent Fingerprint**

  These are the impressions which are produced by the rigid skin known as friction ridges on human finger. They are the marks left at the area and may not be visible with the naked eyes[5]. To flash them, the surface on which the fingerprint is left is powdered with the brush. The background powder is removed and the lifted print is placed on the sensor and exposed to UV Light.

- **Fingerprint Reactivation**

  In this method, graphite powder is brushed on the sensor, where the latent fingerprint is deposited on the sensor is reactivated.

- **Cadaver**

  This method uses dead finger for spoofing.

- **Fingerprint Synthesis**

  In this method, the fingerprint image is reconstructed using templates like minutiae points on the fingerprint and a digital image is captured which can be transferred to the spoofing artefact[6].

C. ANTI-SPOOFING METHODS

Characterizing a live fingerprint from an individual with some other sources is known as Spoof Detection. The detection techniques address the issues of liveliness and can be based on two major types

HARDWARE BASED SPOOF DETECTION

These techniques accomplish the individuality of vitality such as Pulse, Temperature, Electrical Conductivity, Skin resistance etc[7]. But these methods require additional hardware and make the device expensive .The limitation of the few methods are tabulated below as shown in table 1.2.

Table 1.2: Limitation of hardware based spoof detection

Liveness Detection Technique	Limitation
Temperature	Lack of ability to detect the wafer thin silicon rubbers.
Electrical Conductivity	Can be fooled by some saliva on the silicon artificial fingerprint.
Skin resistance	Can be fooled by artificial fingerprint with same type of requirements for original fingerprints

SOFTWARE BASED SPOOF DETECTION:

These methods are based on two mains techniques as shown in figure 1.6.

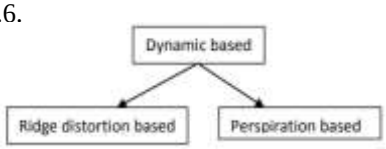


Figure 1.6: Types of dynamic based

Dynamic based

These are derived by processing multi-frame of same fingerprint in two successive images which are captured within a finite time interval.

- Ridge Distortion based

The distortion produced by a real finger when pressing and moving on a scanner is more than a spoofed finger. These distortions are analyzed by processing a sequence of frames at a very high frame rate[8]. The finger is assumed to be non-distorted at the beginning and its movements are analyzed using optical flow. The result and performance of this method depends on precision of minutiae extraction and pairing.

- Perspiration based

It uses live finger. It is based on detecting perspiration between human skin and other material, as the sweat starts from pores and diffuses along the ridges; it makes the region between pores darker[9].The resultant moisture pattern can be captured. Live fingerprints exhibit non-uniformity due to perspiration, where as spoof fingerprints show high uniformity.

Static based

These are analyzed using single fingerprint impression and compared with others. These methods are cheaper and fast than compared with dynamic features[10]. These features consider textural characteristics, skin elasticity, perspiration based or combination of these features as shown in figure 1.7.

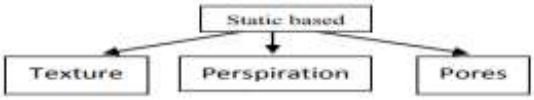


Figure 1.7: Types of static based

II. SPOOFING DETECTION HARDWARE

BLOCK DIAGRAM

The block diagram of Anti-Spoofing Approach For Biometric device with Liveness detection system is given in figure 2.1.

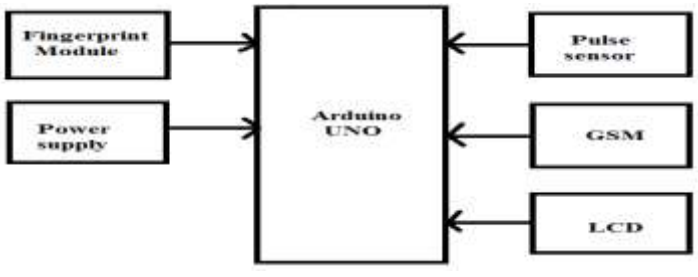


Figure 2.1: Block diagram of spoofing detection system

The necessary components required for Spoofing Detection system are described below:

FINGERPRINT MODULE (R305)

R305 fingerprint module shown in figure 2.2 is a fingerprint sensor with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3.3v or 5v microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port as shown in figure 2.2. Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as access control, attendance, safety deposit box, car door locks.

Figure 2.2: R305 fingerprint module

Biometric identification from a print made by an impression of the ridges in the skin of a finger is often used as evidence in criminal investigations [8]. The same biometric identification technique is used to build the projects like a biometric authenticator/access control system with the help of readily-available Fingerprint Identification Modules. Fingerprint processing includes two parts, fingerprint enrolment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger to capture the image. The system will then processes the finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library.

The fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometric used to identify individual's ad verify their identity. The fingerprint consists of four processes as given below:

Image Acquisition, Image Enhancement, Edge Detection, Extraction of Miniature Points and Matching.

ARDUINO UNO

The Arduino UNO shown in figure 2.3 is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits [9]. The board has 14 Digital pins, 6 Analog pins, and programmable with the Arduino IDE (Integrated Development Environment) via a type B USB cable. It can be powered by a USB cable or by an external 9-volt battery, though it accepts voltages between 7 and 20 volts.

Figure 2.3: Arduino UNO board

PULSE SENSOR

Figure 2.4: Pulse sensor

The principle behind the working of the Pulse Sensor is Photoplethysmograph as shown in figure 2.4. According to this principle, the changes in the volume of blood in an organ are measured by the changes in the intensity of the light passing through that organ. Usually, the source of light in a heartbeat sensor would be an IR LED and the detector would be any Photo Detector like a Photo Diode, an LDR (Light Dependent Resistor) or a Photo Transistor.

With these two i.e. a light source and a detector, we can arrange them in two ways: A Transmissive Sensor and a Reflective Sensor.

- In a Transmissive Sensor, the light source and the detector are place facing each other and the finger of the person must be placed in between the transmitter and receiver.
- Reflective Sensor, on the other hand, has the light source and the detector adjacent to each other and the finger of the person must be placed in front of the sensor.

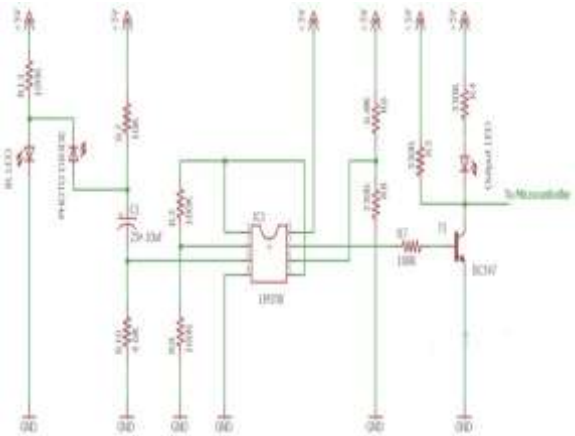


Figure 2.5: Circuit diagram of pulse sensor and control unit

The output of the first op-amp is given as one of the inputs to the second op-amp, which acts as a comparator as shown in figure 2.5. The output of the second op-amp triggers a transistor, from which, the signal is given to a Microcontroller like Arduino. The op -amp used in this circuit is LM358. It has two op-amps on the same chip. Also, the transistor used is a BC547. An LED, which is connected to transistor, will blink when the pulse is detected.

LIQUID CRYSTAL DISPLAY (LCD)

LCD screen is an electronic display module and find a wide range of applications. A 16x2 LCD display shown in figure 2.6 is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on. A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix.

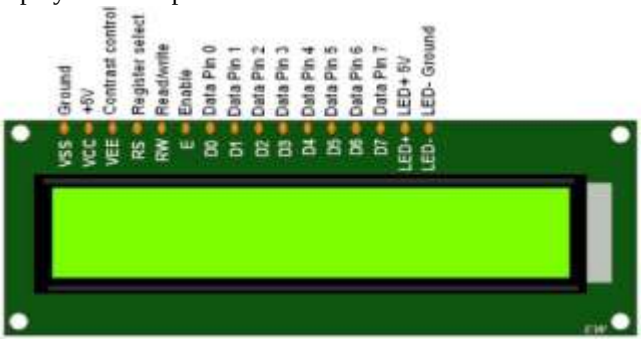


Figure 2.6: 16x2 LCD display

GSM (GLOBAL SYSTEM FOR MOBILE)

The GSM system is the most widely used cellular technology in use in the world today. It has been a particularly successful cellular phone technology for a variety of reasons including the ability to roam worldwide with the certainty of being able to be able to operate on GSM networks in exactly the same way - provided billing agreements are in place.

Figure 2.7:GSM modem

The GSM system was designed as a second generation (2G) cellular phone technology as shown in figure 2.7. One of the basic aims was to provide a system that would enable greater capacity to be achieved than the previous first generation analogue systems. GSM achieved this by using a digital TDMA (time division multiple access approach). By adopting this technique more users could be accommodated

within the available bandwidth. In addition to this, ciphering of the digitally encoded speech was adopted to retain privacy.To transmit data using GSM Modem, there are various methods that can be used, such as:SMS, CDS or HSCSD, GPRS / UMTS

GSM MODEM

A GSM modem is a device which can be either a mobile phone or a modem device which can be used to make a computer or any other processor communicate over a network.

A GSM modem requires a SIM card to be operated and operates over a network range subscribed by the network operator. It can be connected to a computer through serial, USB or Bluetooth connection.A GSM modem can also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on your computer. GSM modem is usually preferable to a GSM mobile phone. The GSM modem has wide range of applications in transaction terminals, supply chain management, security applications, weather stations and GPRS mode remote data logging.

Figure 2.9: SIM card slot

III. SOFTWARE

ARDUINO IDE

A program for Arduino hardware may be written in any programming language with compilers that produce binary machine code for the target processor. The Arduino integrated development environment (IDE) is a cross platform application (for Windows, macOS, Linux) that is written in the programming language Java. The Arduino IDE supports the languages C and C++ using special rules of code structuring [10]. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub main() into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution.

A program written with the Arduino IDE is called a sketch. Sketches are saved on the development computer as text files with the file extension.ino. Arduino Software (IDE) pre-1.0 saved sketches with the extension.pde.

IV. IMPLEMENTATION OF SPOOFING DETECTION SYSTEM

The testing of the spoofing detection system firstly includes the interfacing of hardware and software to the Arduino UNO board. The following connections are made to interface the hardware components to the Arduino:

- Connect the fingerprint R305 module Rx (yellow) pin to the 0th pin andTx (blue) pin to the 1th pin on the Arduino board respectively.
- Connect the fingerprint R305 module GND and Vcc to the GND and5V on the Arduino board respectively.
- Then connect the 11th pin of the Arduino board to the Rx pin on the GSM Modem for serial transmission using software serial function.
- The LCD of 4th and 6th pins are connected to the D7 and D6 on the Arduinoboard respectively.
- The 11,12,13,14 pins(Data pins) of LCD are connected to the D5,D4,D3,D2 Pins on the Arduino board respectively.
- The A0,A1,A2(Analog pins) of the Arduino board are connected to the Switches for the Enroll,Delete,Search functions.
- The power supply for the components is taken from the combinedcentre tapped secondary transform and positive voltage regulator.

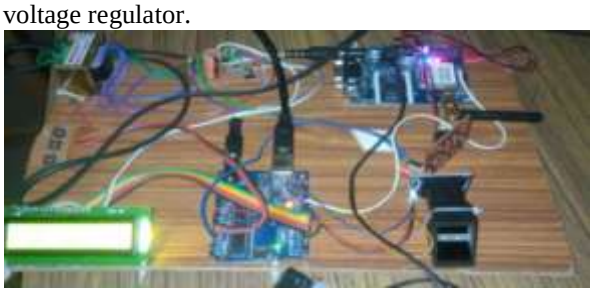


Figure 4.1: Assembly of spoofing detection system

V. RESULTS

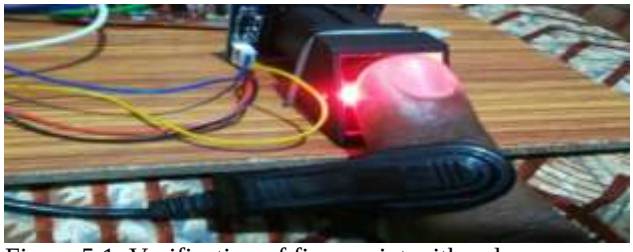


Figure 5.1: Verification of fingerprint with pulse sensor

Figure 5.2 Authorized access

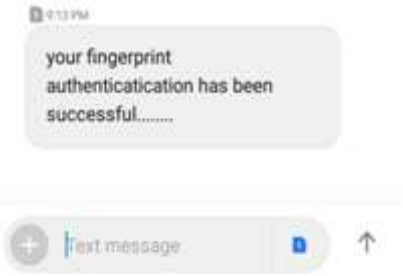


Figure 5.3: Authorized access alert

The verification of the fingerprint with pulse sensor as shown in figure 5.1.If person have the pulse is detected by the pulse sensor and recognize as live person and allowed to access the system or data. The authentication access by user message will send to the mobile as shown in figure 5.2.

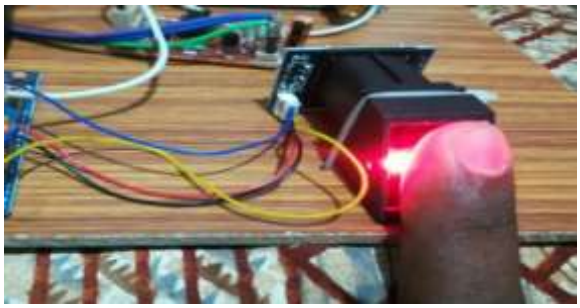


Figure 5.4: Verification of fingerprint without pulse sensor

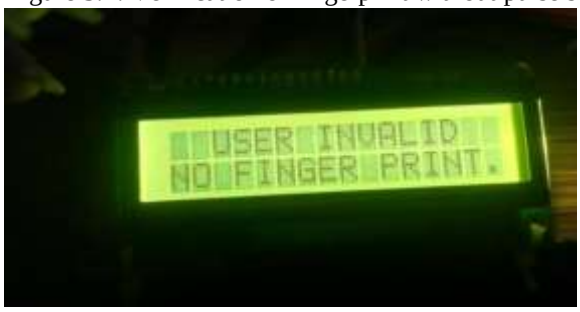


Figure 5.5: Unauthorized access

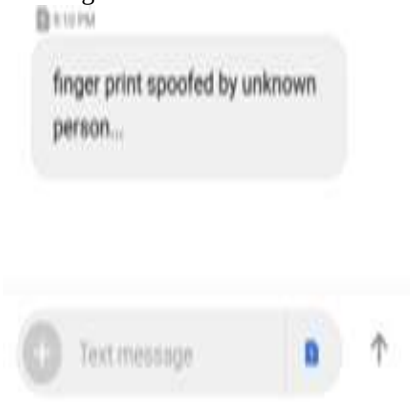


Figure 5.6: Unauthorized access alert

The unauthorized access by user the system or data cannot access because the pulse sensor can't detect the pulse from the user and send alert message.

VI. CONCLUSION

Spoofing is a substantial challenge in fingerprint recognition systems. With the advancements in biometric technology, the attacks on fingerprint systems have also become sophisticated over the past few years. Therefore, it is extremely important to develop robust liveness detection or anti-spoofing mechanisms in order to maintain the integrity of fingerprint biometric systems. A robust and accurate method for fingerprint spoof detection is critical to ensure the reliability and security of the fingerprint authentication systems. This paper has presented liveness detection for the cadaver method using pulse detection.

VII. SCOPE FOR FUTURE WORK

The functionalities of the system can be further enhanced by interfacingthe system to the GPS module which will locate and navigating towards the position where the spoofing is executed.

REFERENCES

[1] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. Biometric authentication.Encyclopedia of Information Science and Technology, pages 346–354, 2008.
[2] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints",IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 8,pp. 1010-1025, August 2002.
[3] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, "Determination of vitality from a noninvasive biomedical measurement for use in fingerprintscanners", Pattern Recognition
[4] Sousedik, C.; Busch, C., 12 2014 "Presentation attack detection methods for fingerprint recognition systems: a survey," in Biometrics, IET.
[5] Mojtaba M, Wamadeva B, Jan 2010Liveness and Spoofing in FingerprintIdentification Issues and Challenges, School of Engineering &DesignBrunelUniversityUxbridge, Middlesex.
[6] Annalisa F,Davide M,2008,Fingerprint Synthesis and Spoof Detection,Springer London.
[7] Emanuela M, Arun R, 2014. A Survey on Anti-Spoofing Schemes for FingerprintRecognition Systems ACM Comput. Surv.47, 2, Article A,36 pages.
[8] Javier G,Julian F, Javier, Raffaele C,2014,Fingerprint Anti-spoofing inBiometric Systems, Springer London..
[9] Shahzad M, April 2012, Novel Active Sweat Pores Based Liveness Detection Techniques for Fingerprint Biometrics, Brunel University. School of Engineering and Design
[10] MaltoniD,Maio D, Jain A K, PrabhakarS,2003,Handbook of FingerprintRecognition,New York, Springer Verlog.

AUTHOR'S BIOGRAPHIES

Mrs.SushmaChowdaryPolavarapu received her B.Tech degree in Electronics and Instrumentation Engineering from V.R. Siddhartha Engg. College, Vijayawada, A.P in 2008 and M.Tech

degree in ECE with Electronics and Instrumentation Engineering Specialization from University College of Engineering, Andhra University, Visakhapatnam in 2011. She has 10 years of experience in teaching. She had published number of papers in reputed journals and presented several papers at international & national conferences. At present she was working as an Assistant professor in V.R Siddhartha Engineering College, Vijayawada, Andhra Pradesh.Her interested domains are Image Processing, Sensors, Robotics and IoTs.

Mrs.UmamaheswariKundurureceived her B.Tech Degree in Electronics and Instrumentation Engineering from Bapatla Engineering College, Bapatla, A.P in 1998 and M.Tech Degree in Digital Systems and Computer Electronics Specialization at Narayana Engineering College, Nellore, A.P in 2012. She has 12 years of experience in teaching. She had published number of papers in reputed journals and presented several papers at international & national conferences. At present she was working as an Assistant professor in V.R Siddhartha Engineering College, Vijayawada, Andhra Pradesh.Her interested domains are Image Processing, Robotics and IoTs

Mr. Sri HariNallamala received his B.Tech degree in Computer Science and Engineering from JNT University Engineering College, Hyderabad in 2007 and M.Tech degree in CSE from RRSCET, JNT University Hyderabad in 2010. He was doing his PhD at KLEF (Deemed to be University), Guntur in the Data Mining domain and it was in the completing stage. He has 10 years of experience in teaching. He had published more than 10 papers in reputed journals and presented several papers at international & national conferences. He became as Reviewer for 3 International Journals and many on pipeline. Presently he was doing his services as an Assistant Professor at DVR &Dr.HS MIC College of Technology, Kanchikacherla, Krishna Dist., Andhra Pradesh. His interested domains are Data Mining, Cloud Computing, Image Processing, Robotics and Internet Technologies.