ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

# SPOOFING DETECTION IN IRIS, FACE AND FINGERPRINT RECOGNITION

**NISHA. S. KUMBLE [1] , DR. B. HARI KRISHNA [2] , C. ASHOK KUMAR[3]**

[1] Nisha. S. Kumble, M.Tech Student, Dept. of ECE, CMR Engineering College, Kandlakoya (V), Medchal, Telangana, India.

[2] Dr. B. Hari Krishna, PhD, Professor, Dept. of ECE , CMR Engineering College, Kandlakoya (V), Medchal, Telangana, India.

[3] C. Ashok Kumar, M.Tech, HOD & Professor, Dept. of ECE, CMR Engineering College, Kandlakoya (V), Medchal, Telangana, India.

**Abstract:** Biometric systems are used significantly for person identification and authentication. It has an important role in personal, national and global security. But these systems can be deceived or spoofed. With recent development in spoofing detection, existing solution often rely on specific biometric reading system.

In this project a software programming based fake identification system is designed which uses image acquisition method using MATLAB. It is used to identify real and fake actions. It has low level complexity, which makes it feasible for ongoing applications. General picture quality elements from the obtained picture is compared with existing picture in database for confirmation purposes to recognize real and imposter tests. The experimental results are data sets of fingerprint, iris and 2D face. Thus this show that the proposed method is highly competitive compared with other recent approaches.

The analysis of the biometric samples has highly valuable information which can be very efficiently used to discriminate from fake traits. The target of the proposed system is to improve the security of biometric used systems, by including liveliness appraisal in a fast, easy to use and non-intrusive manner, using quality assessment

***Keywords:*** *Microcontroller, Fingerprint, GSM*

## I. Introduction

Biometrics human characteristics and traits can successfully allow people identification and authentication and have been widely used for access control, surveillance, and also in national and global security systems [1]. In the last few years, due to the recent technological improvements for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition, and machine learning, several biometric modalities have been largely applied to person recognition, ranging from traditional fingerprint to face, to iris, and, more recently, to vein and blood flow. Simultaneously, various spoofing attacks techniques have been created to defeat such biometric systems. There are several ways to spoof a biometric system [2], [3]. Indeed,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

previous studies show at least eight different points of attack [4], [5] that can be divided into two main groups: direct and indirect attacks. The former considers the possibility to generate synthetic biometric samples, and is the first vulnerability point of a biometric security system acting at the sensor level. The latter includes all the remaining seven points of attacks and requires different levels of knowledge about the system, e.g., the matching algorithm used, the specific feature extraction procedure, database access for manipulation, and also possible weak links in the communication channels within the system.

## II. Hardware System

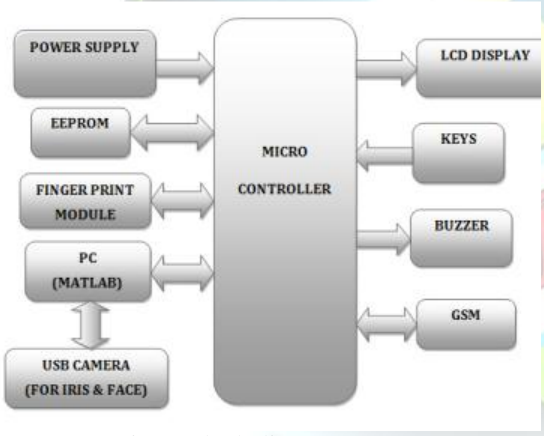


Fig.1: Block diagram

Experimental results illuminate the validity of this locker security system. In this proposed embedded locker security system, Finger print has been placed for detecting thumb recognition of the person & IRS (Iris recognition System) is used to detect the iris of the customer and compare it with the predefined iris. IRS compares the obtained image with the predefined images if the image doesn't match, then the information is sent to the owner through SMS and buzzer will turn ON. In our system the possibility of fraud is highly reduced. As facial recognition technique is nonintrusive and it also cost effective it helps to reduce overall cost of the project. The finger print scan provides very high accuracy to the system. It is one of the developed biometrics. It is easy to use so it will simplify the system at greatest extent. Biometric algorithm standardizes the system. [10] proposed a principle in which the division is the urgent stage in iris acknowledgment. We have utilized the worldwide limit an incentive for division. In the above calculation we have not considered the eyelid and eyelashes relics, which corrupt the execution of iris acknowledgment framework. The framework gives sufficient execution likewise the outcomes are attractive. Assist advancement of this technique is under way and the outcomes will be accounted for sooner rather than later. Based on the reasonable peculiarity of the iris designs we can anticipate that iris acknowledgment framework will turn into the main innovation in personality verification.In this paper, iris acknowledgment calculation is depicted. As innovation advances and data and scholarly properties are needed by numerous unapproved work force. Therefore numerous associations have being scanning routes for more secure confirmation strategies for the client get to. The framework steps are catching iris designs; deciding the area of iris limits; changing over the iris limit to the binarized picture; The framework has been actualized and tried utilizing

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

dataset of number of tests of iris information with various complexity quality.

**Micro controller:** This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

**ARM7TDMI:** ARM is the abbreviation of Advanced RISC Machines, it is the name of a class of processors, and is the name of a kind technology too. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs.

**Liquid-crystal display** (**LCD**) is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

## III. Board Hardware Resources Features

**Finger Print Module:**

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. FIM 30 has functions of fingerprint enrollment, identification, partial and entire deletion and reset in a single board, it does not require connection with a separate PC, thereby offering convenient development environment.

A **fingerprint** in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the foot can also leave an impression of friction ridges. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand or the sole of the foot, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and inter papillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges also assist in gripping rough surfaces, as well as smooth wet surfaces. Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the **eccrine** glands that are present in friction ridge skin, or they may be made by ink or other substances transferred from the peaks of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers. Fingerprint identification, known as dactyloscopy, or hand print identification, is the process of comparing two instances of friction ridge skin impressions (see Minutiae), from human fingers, the palm of the hand or even toes, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand. Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm (or toe or sole).

Fig.2: Fingerprint created by the friction ridge structure.

**GSM:**

Global System for Mobile Communication (GSM) is a set of ETSI standards specifying the infrastructure for a digital cellular service.

The network is structured into a number of discrete sections:

- Base Station Subsystem – the base stations and their controllers explained
- Network and Switching Subsystem – the part of the network most similar to a fixed network, sometimes just called the "core network".
- GPRS Core Network the optional part which allows packet-based Internet connections.
- Operations support system (OSS) – network maintenance.

GSM was intended to be a secure wireless system. It has considered the user authentication using a pre-shared key and challenge-response, and over-the-air encryption. However, GSM is vulnerable to different

**MAX-232:**

The MAX232 from Maxim was the first IC which in one package contains the necessary drivers (two) and receivers (also two), to adapt the RS-232 signal voltage levels to TTL logic. It became popular, because it just needs one voltage (+5V) and generates the necessary RS-232 voltage levels (approx. -10V and +10V) internally. This greatly simplified the design of circuitry. Circuitry designers no longer need to design and build a power supply with three voltages (e.g. -12V, +5V, and +12V), but could just provide one +5V power supply, e.g. with the help of a simple 78x05 voltage converter. The MAX232 has a successor, the MAX232A. The ICs are almost identical, however, the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

MAX232A is much more often used (and easier to get) than the original MAX232, and the MAX232A only needs external capacitors 1/10th the capacity of what the original MAX232 needs. It should be noted that the MAX 232(A) is just a driver/receiver. It does not generate the necessary RS-232 sequence of marks and spaces with the right timing, it does not decode the RS-232 signal, it does not provide a serial/parallel conversion. All it does is to convert signal voltage levels. Generating serial data with the right timing and decoding serial data has to be done by additional circuitry, e.g. by a 16550 UART or one of these small micro controllers (e.g. Atmel AVR, Microchip PIC) getting more and more popular.

**EEPROM:**

EEPROM (also written $E^2$PROM and pronounced e-e-prom or simply e-squared), which stands for Electrically Erasable Programmable Read-Only Memory, is a type of non-volatile memory used in computers and other electronic devices to store small amounts of data that must be saved when power is removed, e.g., calibration tables or device configuration. When larger amounts of more static data are to be stored (such as in USB flash drives) other memory types like flash memory are more economical. EEPROMs are realized as arrays of floating-gate transistors. In 1983, Greek American George Perlegos at Intel developed the Intel 2816, which was built on earlier EPROM technology, but used a thin gate oxide layer so that the chip could erase its own bits without requiring a UV source. Perlegos and others later left Intel to form Seeq Technology, which used on-device charge pumps to supply the high voltages necessary for programming EEPROMs.

**Buzzer:**

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave ovens, & game shows. The word "buzzer" comes from the rasping noise that buzzers made when they were electromechanical devices, operated from stepped-down AC line voltage at 50 or 60 cycles. Other sounds commonly used to indicate that a button has been pressed are a ring or a beep.

The "Piezoelectric sound components" introduced herein operate on an innovative principle utilizing natural oscillation of piezoelectric ceramics. These buzzers are offered in lightweight compact sizes from the smallest diameter of 12mm to large Piezo electric sounders. Today, piezoelectric sound components are used in many ways such as home appliances, OA equipment, audio equipment telephones, etc. And they are applied widely, for example, in alarms, speakers, telephone ringers, receivers, transmitters, beep sounds, etc.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

Fig.3: Types of Buzzers

**WEBCAM:**

"Webcam" refers to the technology generally; the first part of the term ("web-") is often replaced with a word describing what can be viewed with the camera, such as a netcam or streetcam. Webcams are video capturing devices connected to computers or computer networks, often using USB or, if they connect to networks, Ethernet or Wi-Fi. They are well-known for low manufacturing costs and flexible applications. Video capture is the process of converting an analog video signal—such as that produced by a video camera or DVD player—to digital form. The resulting digital data are referred to as a digital video stream, or more often, simply video stream. This is in contrast with screen casting, in which previously digitized video is captured while displayed on a digital monitor.

Webcams typically include a lens, an image sensor, and some support electronics. Various lenses are available, the most common being a plastic lens that can be screwed in and out to set the camera's focus.

Fixed focus lenses, which have no provision for adjustment, are also available. Image sensors can be CMOS or CCD, the former being dominant for low cost cameras, but CCD cameras do not necessarily outperform CMOS-based cameras in the low cost price range. Consumer webcams are usually VGA resolution with a frame rate of 30 frames per second.

Higher resolutions, in mega pixels, are available and higher frame rates are starting to appear. The video capture process involves several processing steps. First the analog video signal is digitized by an analog-to-digital converter to produce a raw, digital data stream. In the case of composite video, the luminance and chrominance are then separated. Next, the chrominance is demodulated to produce color difference video data. At this point, the data may be modified so as to adjust brightness, contrast, saturation and hue. Finally, the data is transformed by a color space converter to generate data in conformance with any of several color space standards, such as RGB and YCbCr. Together, these steps constituted video decoding, because they "decode" an analog video format such as NTSC or PAL.

Fig.4: Webcam

## IV. CONCLUSION

Spoofing is a significant test in biometric acknowledgment system. This paper has displayed distinctive satirizing procedures alongside different cutting edge databases. Parodying recognition and its sorts are additionally been inspected with relating

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

databases. A parodying related calculation needs a strong element extractor which separates the notable components from input pictures. A great deal of algorithmic work is should have been connected for parodying acknowledgment system in order to infer summed up strategies that are autonomous of particulars, necessities and results in expanded mocking acknowledgment rate.

Biometric verification systems are very powerless against advanced ridiculing assaults. To keep a decent level of security, solid mocking location devices are vital, ideally actualized as programming modules. .all the primary methods and capacities in this exuberance discovery region are incorporated into this paper. As appeared in this paper, there are a few distinct strategies and systems conflicting with current introduction assault situations productively. Here it must be specified that none of these procedures give a whole insurance to biometric system. Particularly, the identification of video assaults is a specific test. As a result, a mix of various energy discovery strategies is unequivocally prescribed. additionally, there are a few other identification strategies that ought to be utilized for identifying introduction assaults and ensuring against controls of biometric system to expand the general security .a great performing exuberance recognition system is not just equipped for working under various biometric system (multi biometric) and for assorted mocking situations, however it likewise gives a decent level of assurance against certain non-ridiculing assaults (multi-assault).The project has been effectively outlined and tried. It has been created by coordinating elements of all the equipment segments and programming utilized. Nearness of each module has been contemplated out and put precisely along these lines adding to the best working of the unit. Also, utilizing very advanced ARM7 board and with the assistance of developing innovation the project has been effectively actualized.

## V. 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] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks,"

*Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.

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

[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 Generat. Comput. Syst.*, vol. 28, no.

1,pp. 311–321, 2012.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

[6] 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.

[7] *ISO/IEC 19792:2009, Information Technology—Security Techniques—Security Evaluation of Biometrics*, ISO/IEC Standard 19792, 2009.

[8] *Biometric Evaluation Methodology. v1.0*, Common Criteria, 2002.[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, *Proceedings of the IEEE*

*Int. Joint Conf. on Biometrics*. Piscataway, NJ, USA: IEEE Press, 2011.

[10] Christo Ananth,"Iris Recognition Using Active Contours",International Journal of Advanced Research in Innovative Discoveries in Engineering and Applications[IJARIDEA], Volume 2,Issue 1,February 2017,pp:27-32.

[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,*et al.*, "Competition on countermeasures to 2D facial spoofing attacks," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–6.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz,"Evaluation of direct attacks to fingerprint verification systems,"*J. Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.

[13] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. IEEE IJCB*,Oct. 2011, pp. 1–7.

[14] Biometrics Institute, London, U.K. (2011). *Biometric Vulnerability Assessment Expert Group* [Online] Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-bvaeg.html

[15] (2012). *BEAT: Biometrices Evaluation and Testing* [Online]. Available:http://www.beat-eu.org/

[16] (2010). *Trusted Biometrics Under Spoofing Attacks (TABULA RASA)* [Online]. Available: http://www.tabularasa-euproject.org/

[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni,J. Fierrez, *et al.*, "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," *Pattern Recognit. Lett.*, vol. 31,no. 8, pp. 725–732, 2010.

[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in *Proc. IAPR ICB*,

vol. Springer LNCS-4642. 2007, pp. 366–375.

[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard,and M. Nixon, "Can gait biometrics be spoofed?" in *Proc. IAPR ICPR*,

2012, pp. 3280–3283.

[20] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *Proc.IEEE 5th Int. Conf. BTAS*, Sep. 2012, pp. 283–288.