Detection of Malware Entry with High Security

S. Divya & Md. Hameed Pasha

[1] S. Divya, Dept of ECE, Jayamukhi Institute Of Technological Sciences, Narsampet(V), Warangal(V),Telangana, India.

[2] MD. Hameed Pasha, Ph D, Assistant Professor , Jayamukhi Institute Of Technological Sciences, Narsampet(V), Warangal(V),Telangana, India.

Abstract: *In this Paper, the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding livens assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.*

Keywords: *Microcontroller, Fingerprint, GSM….*

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, 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.

The Hardware System

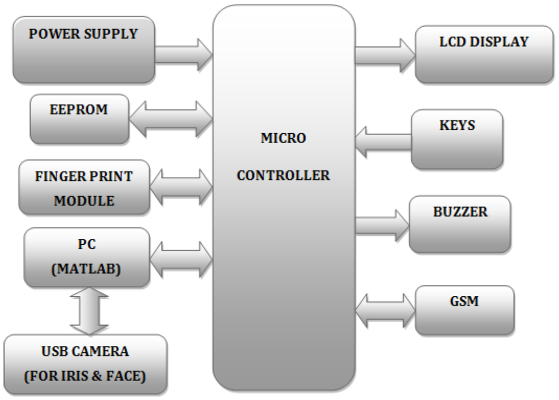


Fig.1.Block diagram

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 recognisation 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.

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.

Board Hardware Resources Features

Finger Print Module:

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 the interpapillary (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 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). Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs.

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

GSM:

An embedded system is a special-purpose system in which the computer is completely encapsulated by or dedicated to the device or system it controls. Unlike a general-purpose computer, such as a personal computer, an embedded system performs one or a few pre-defined tasks, usually with very specific requirements. Since the system is dedicated to specific tasks, reducing the size and cost of the product. Embedded systems are often mass-produced, benefiting from economies of scale. Global System for Mobile Communication (GSM) is a set of ETSI standards specifying the infrastructure for a digital cellular service. The standard is used in approx. 85 countries in the world including such locations as Europe, Japan and Australia.

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 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.

Fig:3: Types of Buzzers

CAMERA:

"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.

Fig:4: Webcam

DC Motor:

A DC motor relies on the fact that like magnet poles repels and unlike magnetic poles attracts each other. A coil of wire with a current running through it generates an electromagnetic field aligned with the center of the coil. By switching the current on or off in a coil its magnetic field can be switched on or off or by switching the direction of the current in the coil the direction of the generated magnetic field can be switched 180°.

Fig: 5:DC Motor

Motor driver (L293D):

DC motors are typically controlled by using a transistor configuration called an "H-bridge". This consists of a minimum of four mechanical or solid-state switches, such as two NPN and two PNP transistors. One NPN and one PNP transistor are activated at a time. Both NPN and PNP transistors can be activated to cause a short across the motor terminals, which can be useful for slowing down the motor from the back EMF it creates. H-bridge. Sometimes called a "full bridge" the H-bridge is so named because it has four switching elements at the "corners" of the H and the motor forms the cross bar. The switches are turned on in pairs, either high left and lower right, or lower left and high right, but never both switches on the same "side" of the bridge. If both switches on one side of a bridge are turned on it creates a short circuit between the battery plus and battery minus terminals. If the bridge is sufficiently powerful it will absorb that load and your batteries will simply drain quickly. Usually however the switches in question melt.

Conclusion

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this “*quality-difference*” hypothesis, in the present research work we have explored the potential of *general* image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing).For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris,the fingerprint and 2D face, using publicly available databases with well defined associated protocols. This way, the results GALBALLY *et al.*: IQA FOR FAKE BIOMETRIC DETECTION 723 are reproducible and may be fairly compared with other future analogue solutions.Several conclusions may be extracted from the evaluation results presented in the experimental sections of the article:

i) The proposed method is able to consistently perform at a high level for different biometric traits (“multi-biometric”);
ii) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection (“multi-attack”);
iii) The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios;
iv) The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions;and
v) in addition to its very competitive performance, and to its “multi-biometric” and “multi-attack” characteristics, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system

Result

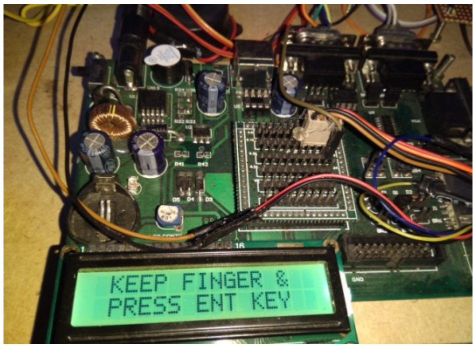


Fig:5: first we have place our finger and has to press enter key

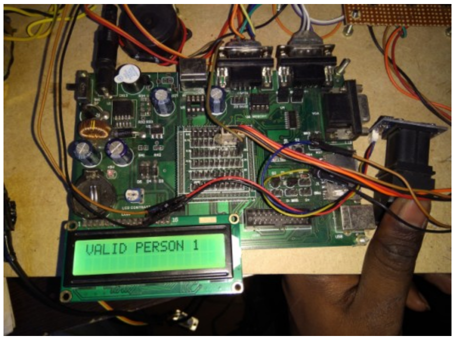


Fig:6:finger print is valid then it shows valid person number

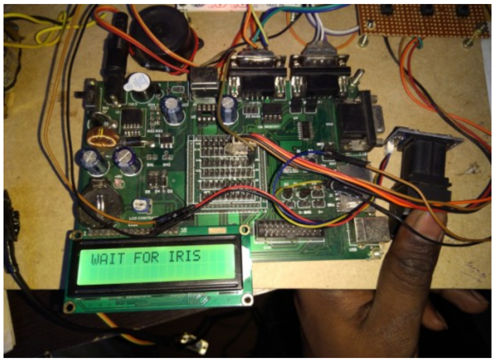
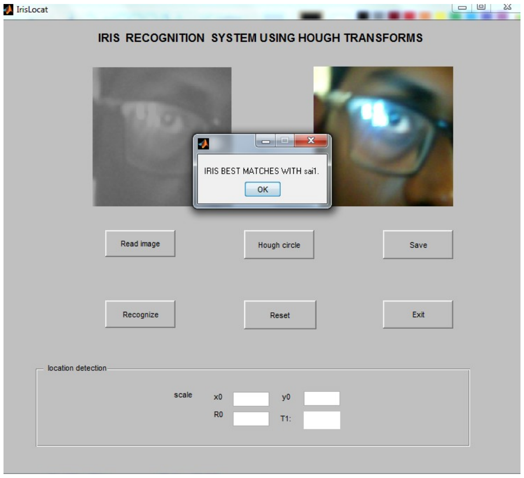


Fig7:after validting finger print waits for iris recognation


IrisLocat

IRIS RECOGNITION SYSTEM USING HOUGH TRANSFORMS

IRIS BEST MATCHES WITH sai1.

Fig:8:iris matches it shows iris is matched

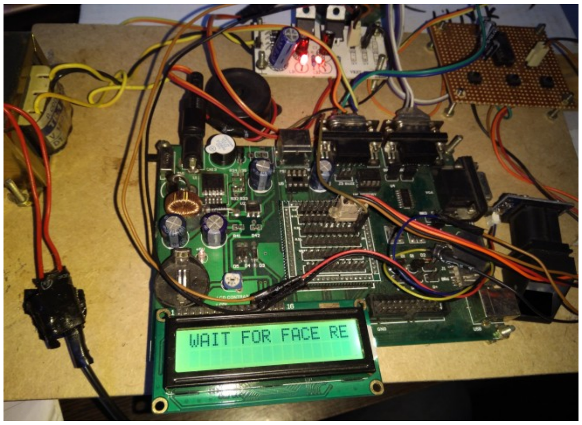
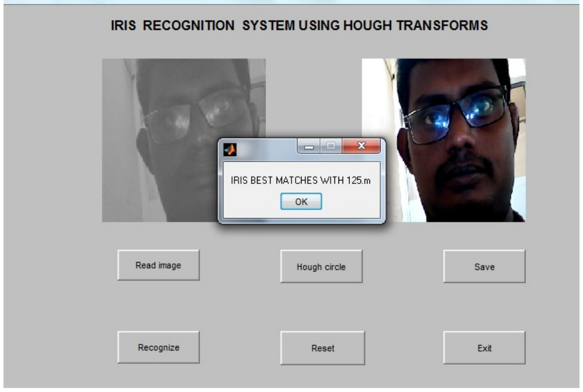


Fig:9:after matchinf of iris it will waits for face recognation


IRIS RECOGNITION SYSTEM USING HOUGH TRANSFORMS

IRIS BEST MATCHES WITH 125.m

Fig:10:if was matched

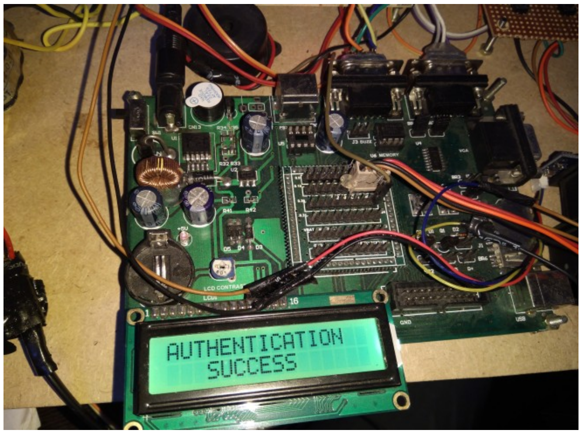


Fig:11:if all the three conditons fingerprint,iris,face recognation was success then it gives access and displays autentication success.

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.

[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] 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.

[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.