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, Issue 7, July 2017

SMART BANK LOCKER SECURITY SYSTEM USING MULTIMODEL BIOMETRICS& GSM TECHNOLOGY

Samreen Talha[1]and T Sreenivasulu[2]

[1] M. Tech Student and Guide [2]

Department of ECE, Kakatiya University College of Engineering & Technology,
Kakatiya University Campus, Warangal, Telangana, India.

Abstract: Biometrics technology is an automated recognition system which enables the authentication of individual based on biological and behavioural characteristics such as face, iris, voice, fingerprints etc. Biometric methods are supposed to be a set of secure methods for Identification and authentication of an individual as it has makeable advantages as compared with other methods. But at the same time biometric systems may be vulnerable to attacks, at each level such as biometric sensor level, data communication, database etc. The most Vulnerable part of a system is its acquisition sensor, attackers have mainly focused on direct spoofing. 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 using Respberry Pi. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveners assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. Here we are interfacing camera to Micro controller. The camera will capture face image of a person and send to controller. The controller will recognize the face and iris of the particular person from the image. The finger print module will take the finger print from the person and send to controller. The controller will recognize the finger print of particular person from the data base. If they are matched then it will display the data on display unit. Otherwise it will send the message to the police or authorized one about wrong accessing. Using this biometric system we are designing an application where we are using biometrics like fingerprint, face and iris using this we will access the our application which is ATM system And we will detect the fake accessing by spoofing detection

Keywords:*Microcontroller,Fingerprint,GSM,USB Camera….*

Introduction

The existing self-banking system has got very high popularity with 24 hours service. Use of Bank Locker is helpful for money or gold storage.by submitting the proper documents,bank management will give you authorization on bank locker,so that anyone can use locker system. Butthis system is not safe to use because anybody can access the system if they have the details and fake proofs like we share our details to our friends who may miss use it. This is the main disadvantage of existing system.Traditional Bank locker systems authenticate the method has some

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, Issue 7, July 2017

defects. Using identity card and proofs of documents cannot verify the client'sidentity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated, which has offered newverification means for us, the original password authentication method combined with the biometric identification technologyverify the users identity better and achieve the purpose that use of Bank lockers improve the safety .In the proposed system we are trying to remove disadvantages of existing system. So security over money Transaction is ourprime concern. In traditional system client has to carry documents or identity cards with him to verify his identity. This identity cardmay lose, so instead of traditional identification we are using biometric identification. Fingerprint recognition has gotcontinuously updated algorithm in recent years which mean perfect biometric identification. The aim of the project is to designa model to give high security while storage in the Bank Locker's. Main objective of this project is to develop a system by whichthe authentication is being provided by making use of unique code and Face Recognition.

The Hardware System

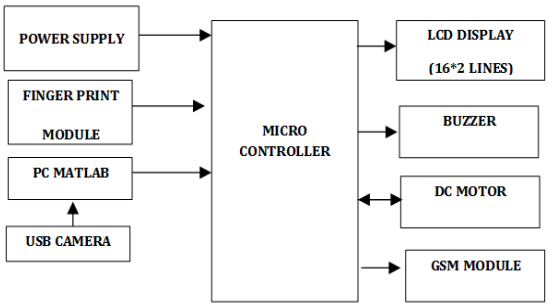


Fig.1.Block diagram

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: It 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.

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, Issue 7, July 2017

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.

Power Supply: This module basically consists of a transformer to step down the 230V ac to 12V ac followed by regulators and diodes. Here diodes are used to rectify the ac to dc. After rectification, the obtained rippled dc is filtered using a capacitor Filter.

A positive voltage regulator is used to regulate the obtained dc voltage.

Photograph of power supply module

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 primatehand. 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

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, Issue 7, July 2017

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).

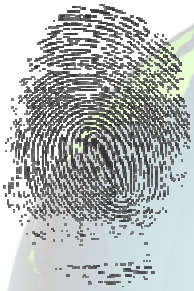


Fig: fingerprint created by the friction ridge structure.

Finger print scanner interfaced to the PC for getting fingerprint recognition. This module can be used for registration of all the concerned of their finger print

Photograph of fingerprintmodule

GSM: Anembedded 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, design engineers can optimize it, 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 Maximwas 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

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, Issue 7, July 2017

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.

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.

Types of Buzzers

WEB 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

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, Issue 7, July 2017

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 toappear.

Photograph of 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: 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 melts. [7] discussed about a project, in this project an automatic meter reading system is designed using GSM Technology. The embedded micro controller is interfaced with the GSM Module. This setup is fitted in home. 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, Issue 7, July 2017

energy meter is attached to the micro controller. This controller reads the data from the meter output and transfers that data to GSM Module through the serial port. The embedded micro controller has the knowledge of sending message to the system through the GSM module. Another system is placed in EB office, which is the authority office. When they send "unit request" to the microcontroller which is placed in home. Then the unit value is sent to the EB office PC through GSM module. According to the readings, the authority officer will send the information about the bill to the customer. If the customer doesn't pay bill on-time, the power supply to the corresponding home power unit is cut, by sending the command through to the microcontroller. Once the payment of bill is done the power supply is given to the customer. Power management concept is introduced, in which during the restriction mode only limited amount of power supply can be used by the customer.

SYSTEM INTERFACING & TESTINGSTEPS

The procedure adopted for the various modules interface and testing is as follows

Power supply of 5V has been given to micro controller to initialize the operation.

LCD has been connected to display the data related to the working status of proposed design.

At initial stage, LCD shows "Welcome to the Project" & "Keep finger and press Enter".

Fingerprint section is to be initialized by enrolment process.

Function key section has been placed to enroll the finger. Here we have 3 keys (Increment, Decrement and Enter).

process to Enroll the Finger on Fingerprint Sensor:

RST button has been soldered at ARM Board. long press the RST Button and then Enter button.

Release the RST Button and then release the Enter, Then LCD Shows "Enrolment started" and "Enter person Number".

Then place the Finger on Fingerprint module. Enter the person Number 1 by using the functional keys.

This is the procedure for Enrollment of Finger on Finger print module.

Whenever LCD asks to "Keep finger and press enter", then we have to place the finger on Finger print module and long press Enter. LCD shows "Valid person 1".

Then it asks"waiting for iris".

In the above if the finger print is not matched then it displays on LCD. And buzzer will turn On, A message can be sent to the mobile says "Finger is not matched

RECOGNISATION OF IRIS:

Open "Mat lab" Software on PC. Run the code given in iris locate "irislocate.m"

It shows the window on which predefined iris and user defined iris is to be matched.

Connect USB Camera to the CPU USB Slot. Then click on "Read Image" on window. Then look into camera for capturing the iris. In window it appears as predefined image. Wait for freeze the iris image. Then save it with Name like "Image 1".

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, Issue 7, July 2017

Then click on "Read image" for capturing the different iris to compare with "image 1". After taking the another iris it has to

compared with image1 by clicking the "Recognize"

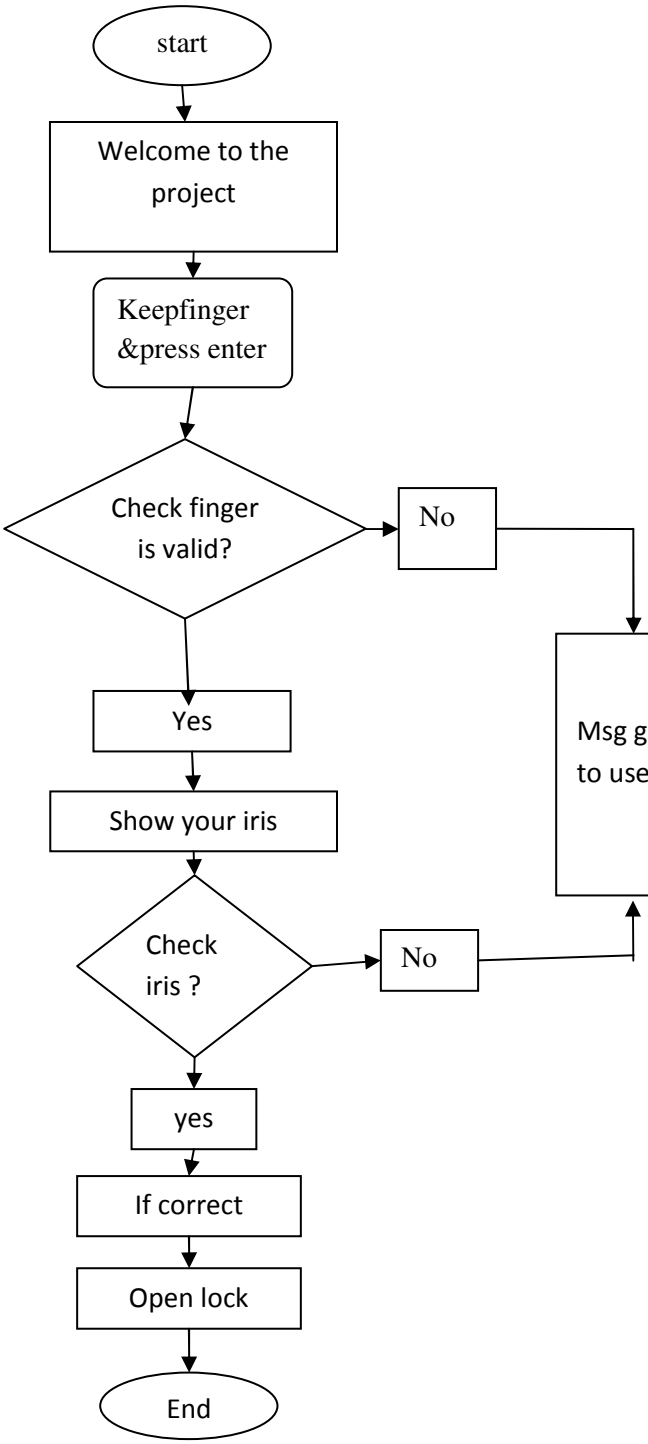
If it is matched with "image 1", then it displays "best matches found with image1", then motor will turn ON.

If it is not matched then it shows "Match not found". Then buzzer will turn On and message can be sent to the mobile. The message contains "IRIS not matched".

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, Issue 7, July 2017

SOFTWARE: FLOWCHART



SNAPSHOTS OF RESULTS

Fig : Initialization of LCD

Fig: Log in into the project

Fig :Checking the iris

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, Issue 7, July 2017

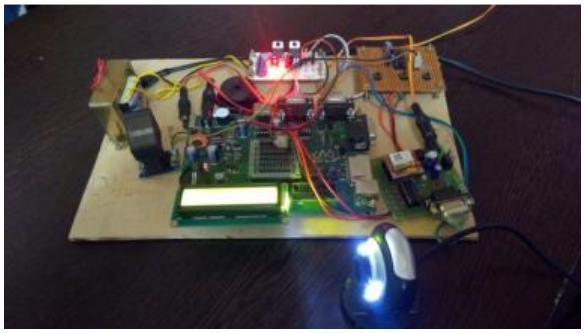


Fig: Proposed Design

APPLICATIONS:used in all banks for Lockers

- used in all bank ATMs,
- In houses Almarah,
- Schools treasury, Colleges treasury
- In industries
- VIP vehicle Security Applications
- In hospitals and
- Offices.

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 arereproducible 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.

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./Apr2003.

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, Issue 7, July 2017

[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, "Onthe 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 onquality 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] Christo Ananth, Kanthimathi, Krishnammal, Jeyabala, Jothi Monika, Muthu Veni, "GSM Based Automatic Electricity Billing System", International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Volume 2, Issue 7, July 2015, pp:16-21

[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: IEEEPress,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 facerecognition: A public database and a baseline," in *Proc. IEEE IJCB*,Oct. 2011, pp. 1–7.

[14] Biometrics Institute, London, U.K. (2011). *Biometric VulnerabilityAssessment 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 fakefingers 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 forgeryscenario 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*,

[20] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serialand parallel multibiometric

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, Issue 7, July 2017

systems under spoofing attacks," in *Proc.IEEE 5th Int. Conf. BTAS*, Sep. 2012, pp. 283–288.

[21] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of FingerprintRecognition*. New York, NY, USA: Springer-Verlag, 2009.

[22] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint imagereconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[23] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *Proc. IEEE ICIP*, Oct.2006,pp.317–320.

[24] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulationdetection,"*J. Electron.Imag.*, vol. 15, no. 4, pp. 041102-1–041102-17,2006.

[25] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 492–496, Sep. 2010.