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 2, January 2017

SECURED AUTHENTICATION SYSTEM USING FACE SCRAMBLING WITH PRIVACY PROTECTION

M RAVI KIRAN REDDY [1], D. SHEKAR GOUD [2],

[1]PG Scholar, Dept. of ECE, Ellenki College of Engineering and Technology, Sangareddy Dist, Telangana, India.

[2]Assistant Professor, Dept of ECE, Ellenki College of Engineering and Technology, Sangareddy Dist, Telangana, India.

Abstract:

In present days world authentication is provided using various technologies . With advent of internet remote surveillance and authentication is possible. In our system video streaming of area is done through which unauthorized entry can be prevented by alerting, authentication is provided by face recognition using face scrambling technique which have huge advantages over existing system. The goal of this to improve the frameworks of security in bio metric recognition , by providing live assessment in a user-friendly,quick and through the assessment of image quality . USB camera is interfaced to RAPBERRY-PI. The camera will capture face image of a person and send to RASBERRY-PI. The RAPBERRY-PI will recognize the face of the particular person from the image. If they are matched then it will display the data on display unit and send to email. Otherwise it will send the message to the police or authorized one about wrong accessing and send to email. This system handles chaotic signals and improves significantly the accuracy in recognition. With this advantages our method can be implemented in providing authentication and secure bio metric verification in various applications.

Keywords:*USB camera,LAN,Raspberry-pi.*

Introduction:

Authentication is provided using various bio-metric systems with different technologies to recognize. Bio metrics can be refers to measure features related to individuals. Bio metrics authorization in many systems is used as one method to identification and provide access . It will also be used in identify persons in group that are under observation. Bio metric measurends are the unique, measurable features helps to identify and label individuals. Bio metric parameters are often divided as behavioral and physiological parameters. Physiological parameters are compared to body ire shape. Different examples included are unlimited to palm veins ,fingerprint, face identification,iris identification, odor/scent and retina . Behavioral parameters are compared to patterns of actions of individuals, included but unlimited to gait ,voice and typing rhythm. Some people have termed the behaviometrics to classify the bio-metrics.Various different features of individual behavior or chemistry,physiology could be utilized for bio metric systems for authentication. For selecting a authentication system using bio metric systems various factors has to be taken for specific application. Apt bio metric usage depends on

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 2, January 2017

application. Many bio metric are better and powerful than others required on feasibility and security levels. All possible application cannot be designed by a

particular bio metric system.With advent in IOT and technology in various IOT systems targeted for video sharing scrambling o face is proposed to protect privacy. Because of these result in IOT based applications,recognition using bio metric identification has a demand or scrambling which has has challenging task for face identification. This experiment output successfully shows how the system can reliably handle and improve the accuracy in recognition ,which makes a promising method for safe bio metric identification.

LITERATURE SURVEY

Fake biometrics means by using the real images like iris images captured from a printed paper or fingerprint captured from a dummy finger of human identification characteristics create the fake identities like fingerprint on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication. There is no such technology to provide security for fake users. In the proposed method, 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 liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. Here we are interfacing camera to ARM RAPBERRY-PI. The camera will capture face image of a person and send to RASBERRY-PI. The RAPBERRY-PI will recognize the face of the particular person from the image. If they are matched then it will display the data on display unit and send to email. Otherwise it will send the message to the police or authorized one about wrong accessing and send to email.

PROPOSED SYSTEM

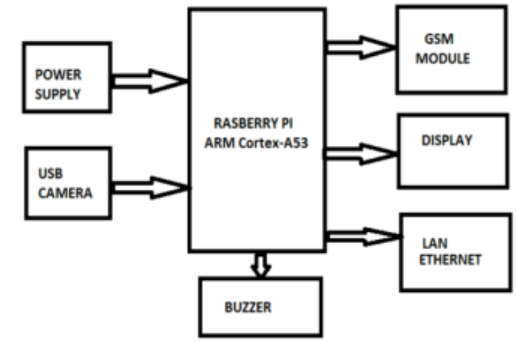


Fig:1:Block diagram

METHODOLOGY

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.

Raspberry Pi :

The Raspberry Pi delivers 6 times the processing capacity of previous models. This second generation Raspberry Pi has an upgraded Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor that runs at 900MHz. 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 2, January 2017

board also features an increase in memory capacity to 1Gbyte.

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.

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.

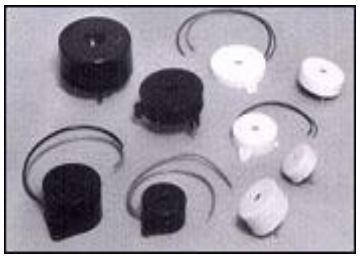


Fig:2: Types of Buzzers

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

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 2, January 2017

mega pixels, are available and higher frame rates are starting to appear.

Fig:3: Webcam

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 orPAL.Support electronics are present to read the image from the sensor and transmit it to the host computer. The camera pictured to the right, for example, uses a Sonix SN9C101 to transmit its image over USB. Some cameras - such as mobile phone cameras - use a CMOS sensor with supporting electronics. [7] discussed about a method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

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

SM 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 class of attacks, each of them aiming a different part of the network.

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 2, January 2017

Fig:4: GSM Module

Ethernet:

Ethernet is a family of computer networking technologies for local area networks (LANs) and metropolitan area networks (MANs). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3, and has since been refined to support higher bit rates and longer link distances. Over time, Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET. The primary alternative for contemporary LANs is not a wired standard, but instead a wireless LAN standardized as IEEE 802.11 and also known as Wi-Fi.The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet uses coaxial cable as a shared medium, while the newer Ethernet variants use twisted pair and fiber optic links in conjunction with hubs or switches. Over the course of its history, Ethernet data transfer rates have been increased from the original 2.94 megabits per second (Mbit/s) to the latest 100 gigabits per second (Gbit/s), with 400 Gbit/s. Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model, Ethernet provides services up to and including the data link layer.

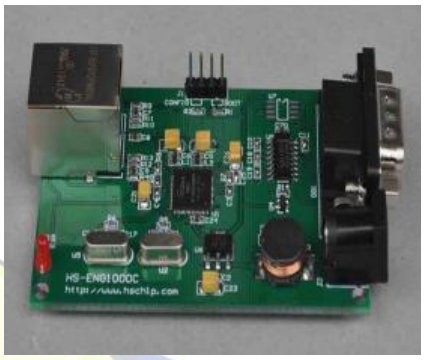


Fig:5: Ethernet module

FEATURES:

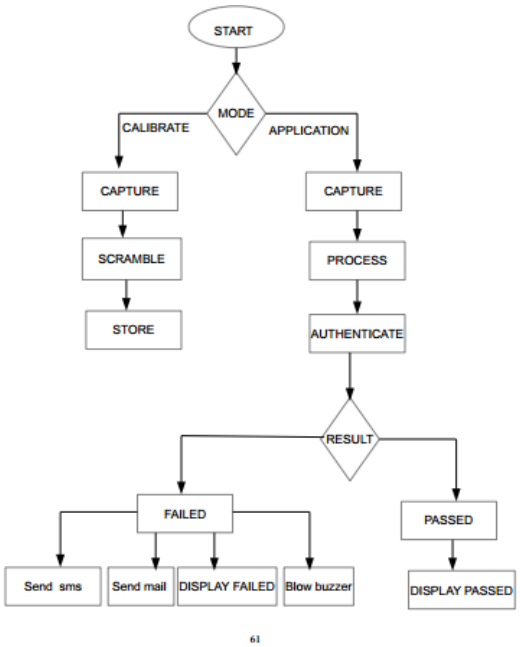
- Smallest wireless video & audio camera
- Wireless transmission and reception
- High sensitivity
- Easy installation & operation
- Easy to conceal
- Light weight
- Low power consumption
- Small size

SPECIFICATIONS:

- Output frequency: 900MHZ 1200MHZ
- Output power: 50mW 200mW
- Power supply: DC +6~12v
- Distance covered: 10m

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 2, January 2017

FLOW CHART



61

RESULT

Fig:6:project hardware

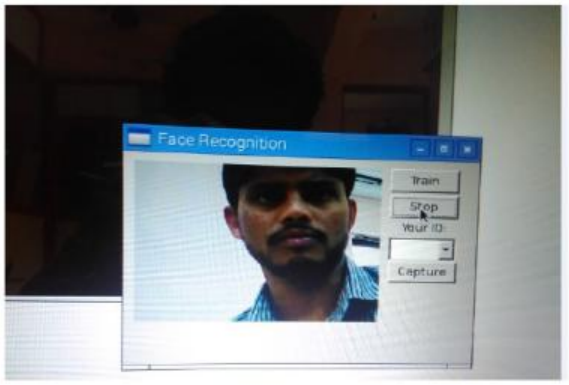


Fig:7:user interface

CONCLUSION

As a conclusion, the objectives of this project have been achieved successfully where this project was able to develop a secured authentication system that can protect privacy. Implementation of authentication system have is developed using raspberry-pi and various modes of communication to pass authentication information have been implemented. The project implementation will help in protecting privacy of individual and also does not compromise on reliability and security.

REFERENCES

[1] Singh, A. ; Karanam, S. ; Kumar, D. "Constructive Learning for Human-Robot Interaction", IEEE Potentials, Vol 32, Issue 4, 2013, Page(s): 13 – 19.

[2] Jayatilake, D. ; Isezaki, T. ; Teramoto, Y. ; Eguchi, K. ; Suzuki, K. "Robot Assisted Physiotherapy to Support Rehabilitation of Facial Paralysis", IEEE Trans Neural Systems and Rehabilitation Engineering, Vol. 22 , Issue 3,

[3] McDuff, D. ; Kaliouby, R.E. ; Picard, R.W. "Crowdsourcing Facial Responses to Online Videos",

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 2, January 2017

IEEE Trans Affective Computing, Vol 3, Issue 4, 2012 , Page(s): 456 – 468

[4] Fleck, S.; Strasser, W. "Smart Camera Based Monitoring System and Its Application to Assisted Living", Proceedings of the IEEE, On page(s): 1698 - 1714 Volume: 96, Issue: 10, Oct. 2008

[5] A. Melle, J.-L. Dugelay, "Scrambling faces for privacy protection using background self-similarities," Proc. 2014 IEEE International Conference on Image Processing (ICIP), 2014, pp.6046-6050.

[6] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, "Privacy-Preserving Face Recognition," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (PETS '09), 2009, pp.235-253.

[7] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., "Network Fault Correction in Overlay Network through Optimality", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22

[8] A. Erdlyi, T. Bart, P. Valet, T. Winkler, B. Rinner, "Adaptive Cartooning for Privacy Protection in Camera Networks". Proc. International Conference on Advanced Video and Signal Based Surveillance, 2014, pp.6.

[9] F. Dufaux, T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," Proc. 2006 Conference on Computer Vision and Pattern Recognition Workshop, Washington, DC, USA, 2006, pp.106-110.

[10] F. Dufaux, "Video scrambling for privacy protection in video surveillance: recent results and validation framework," Proceedings of SPIE, Vol. 8063, 2011, pp.14.

Author's Profile

M. Ravi kiran Reddy is pursuing M.Tech(Embedded Systems) in prestigious Ellenki College of Engineering and Technology, Hyderabad. He obtained B.tech from Vignana Bharathi Institute of Technology.

D.Shekar goud, M.tech(E.S) he is currently working as Assistant Professor in department of Electronic and communication of . Ellenki College of Engineering and Technology He guided for more than 15 projects to final year B.E/B.Tech students and guided for M.Tech students with good teaching experience. His Areas of interest in Embedded System R & D, DSP, Microprocessors and Microcontrollers.