

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

RFID Based Advanced Access System using Image Comparison Technique

S.Fayaz Begum¹, U.Snehitha²

Assistant Professor, Department of ECE, Annamacharya Institute of Technology & Sciences Rajampet, India¹

PG student (Embedded systems), Department of ECE, Annamacharya Institute of Technology & Sciences
Rajampet, India²

ABSTRACT: The conventional ID password system fails at stop the theft in industries. In biometrics basic traits of human is matched to the existing data and depending on result of matching identification of a human being is traced. Facial features are extracted and implemented through algorithms which are efficient and some modifications are done to improve the existing algorithm models. Face detection and recognition is used in many places nowadays. Features extracted from a face are processed and compared with similar faces which are existing in our database. If input face image matches with the image present in the databases then it is known as person is recognized otherwise it is known as person is unrecognized. However, while using the facial recognition system searching the corresponding image of an user in a large set of images is complex and also time consuming, by using a new approach along with RFID we can distinguish each user with his/her corresponding card and thus we can resolve the issue. So here we introduced a new approach with multi biometric system for industrial security applications using both the facial features and RFID card of each person. We use Eigen detection for face recognition in MATLAB communicating with the RFID through RS232.

KEYWORDS: Security, Face recognition, RFID, Eigen detection, MATLAB.

I. INTRODUCTION

Traditionally, passwords and ID cards have been used to restrict access to secure systems. However, security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor. Furthermore, simple passwords are easy to guess by an impostor and difficult passwords may be hard to recall by a legitimate user. Biometric systems are being deployed in various applications including computer logins, ATMs, grocery stores, airport kiosks, and driver's licenses. The successful installation of biometric systems in these applications does not imply that biometrics is a solved problem. In fact, there is significant room for improvement in biometrics as suggested by the error rates. Biometric systems installed in real-world applications must contend with a variety of problems. Among them are: *Noise in sensed data*. A fingerprint with a scar and a voice altered by a cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors (for example, accumulation of dirt on a finger print sensor) and unfavorable ambient conditions (for example, poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges. Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. There is empirical evidence that about 4% of the population may have poor quality fingerprints that cannot be easily imaged by some of the existing sensors. To avoid this problem here we introduce a new technique for person authentication, using RFID and face recognition system to avoid the false recognition in high sensitive areas.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

The article is organized as follows. The system architecture is discussed in Section II, followed by system description in Section III. The system implementation and Experimental work are presented in Section IV and Section V with result respectively. Finally, Section VI draws conclusion.

II. SYSTEM ARCHITECTURE

The Access management system reported that, the system consisting data base of images and card numbers. After running the program the video is started until the user input (face) is fetched, and system waits for the RFID input. If the user RFID and the corresponding image in the database is matched. This situation is called the authenticated case where the individual is identified and attendance is saved.

When a person tries to access the system with the ID card of his friend, then his image will be mismatched with the actual user of the card. This case is called the unauthenticated stage. After each successful authentication of each user, his/her attendance is saved in the form of a MATLAB report for the purpose of future access. After the periodical intervals of time the percentage of each student is intimated through an SMS.

III. SYSTEM DESCRIPTION

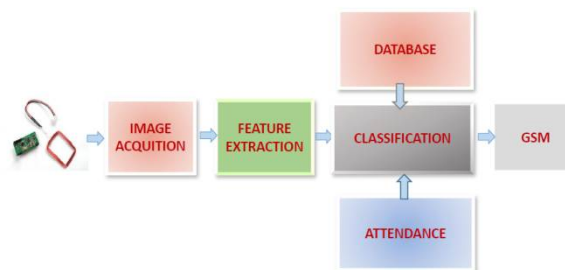


Fig 1: Layout of the proposed system

The description of the modules which are used in the system is as follows.

(i) QHML CAMERA

Quantum 495-LM PC camera is connected to computer and using USB cable. It has 25MP (interpolated) sensor and 6 white lights. These lights help you go that extra stride by performing in an all impressive manner even in dark. The webcam comes equipped with USB 2.0 interface and has a maximum frame rate of 30fps. It sports a focus range of 4-cm to infinity and has an integrated microphone.



Fig 2: QHML pc cam

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

(ii) **RFID**

This is a low frequency (125 KHz) RFID reader with serial output with a range of 8-12cm. It is a compact unit with built in antenna and can be directly connected to the PC using RS232 protocol.



Figure 3: RFID reader module

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes: active and passive. Active tags require a power source they're either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo. One example of an active tag is the transponder attached to an aircraft that identifies its national origin.

Transponders (tags) of passive RFID system don't have power supply. This is why they are called passive. Passive tags are powered from electromagnetic field generated by reader antenna. Reader antenna has to transmit enough power to provide enough energy to tag so it could to transmit back data. Because of this reading distance is very limited – up to several centimeters.

(iii) **AT89S52**

Microprocessors and microcontrollers are widely used in embedded systems products. Microcontroller is a programmable device. A microcontroller has a CPU in addition to a fixed amount of RAM, ROM, I/O ports and a timer embedded all on a single chip. The fixed amount of on-chip ROM, RAM and number of I/O ports in microcontrollers makes them ideal for many applications in which cost and space are critical. The Intel 8052 is Harvard architecture, single chip microcontroller (μ C) which was developed by Intel in 1980 for use in embedded systems.



Figure 4: AT89S52 controller

8052 is an 8-bit processor, meaning that the CPU can work on only 8 bits of data at a time. Data larger than 8 bits has to be broken into 8-bit pieces to be processed by the CPU. The present project is implemented on Keil μ Vision. In order to program the device, proload tool has been used to dump the program onto the microcontroller.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

(iv) GSM

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation. Cellular is one of the fastest growing and most demanding telecommunications applications. Cellular systems using a digital technology will become the universal method of tele-communications.



Figure 5: GSM Module

Mobile to Base Transceiver Station (uplink): 890-915 MHz

Base Transceiver Station to Mobile (downlink):935-960 MHz

Bandwidth: 2 * 25 MHz

A GSM network is made up of multiple components and interfaces that facilitate sending and receiving of signaling and traffic messages. It is a collection of transceivers, controllers, switches, routers, and registers. The Subscriber Identity Module (SIM) is a small smart card which contains both programming and information. The SIM card provides the actual identity for the subscriber. During initial registration all the relevant subscriber data are inserted into the SIM card and the activity is known as personalization.

IV. EXPERIMENTAL RESULTS

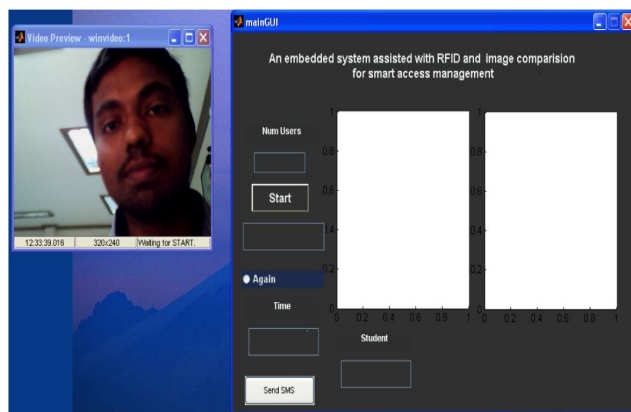


Figure 6: Initial stage where video is running and waiting for RFID input

After running the program the video is started until the user input is fetched. The above figure shows the case where the video is running and waiting for the RFID input.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

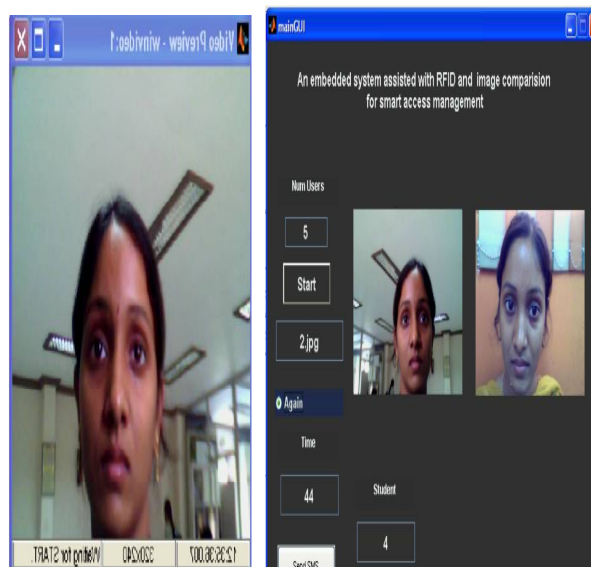


Figure 7: Graphical User Interface (GUI) representing the person is authenticated

Above figure explains the case where the user RFID and the corresponding image in the database is matched. This situation is called the authenticated case where the individual is identified and attendance is saved.

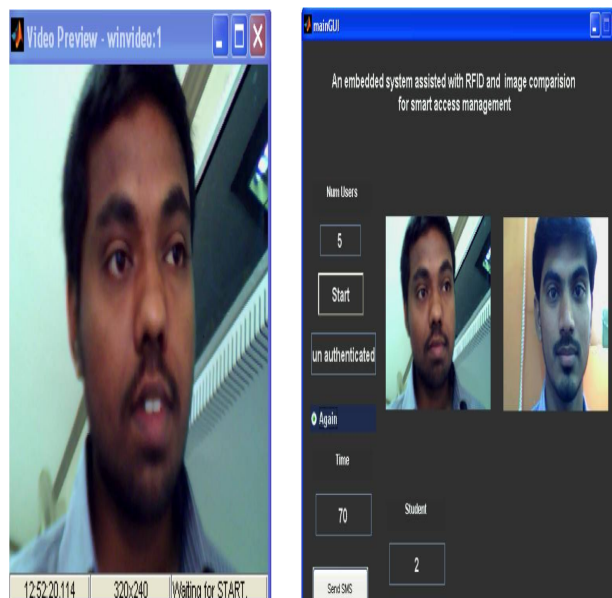


Fig 8: Graphical User Interface (GUI) representing the person is unauthenticated

When a person tries to access the system with the ID card of his friend, then his image will be mismatched with the actual user of the card. This case is called the unauthenticated stage. The above figure explains the scenario.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

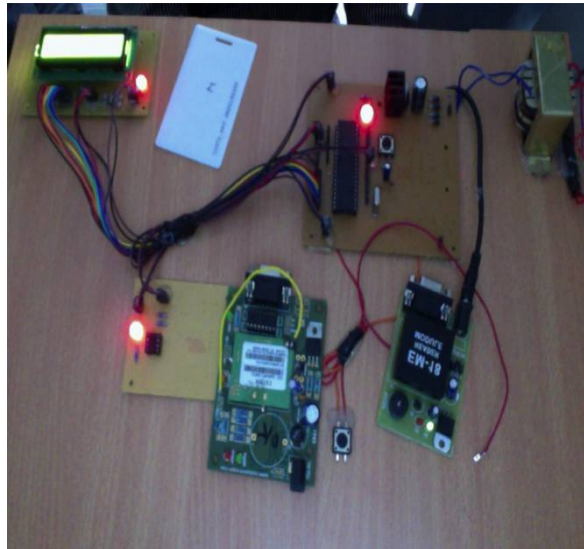


Fig 9: Experimental setup

The above figure shows the picture of the total experimental setup containing RFID card, reader and a GSM module along with the LCD display and the Microcontroller.

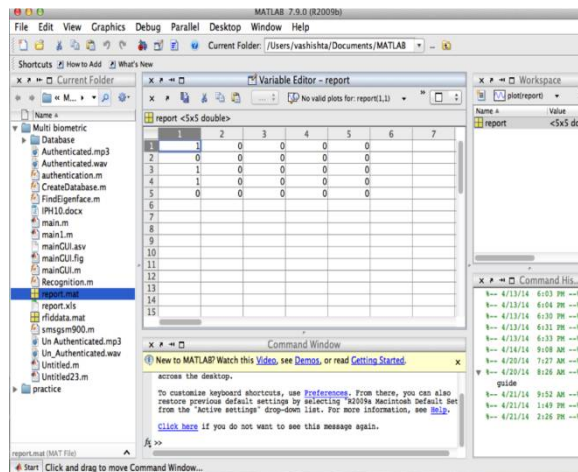


Fig 10: The report with the details of student's attendance

After each successful authentication of each user, his/her attendance is saved in the form of a MATLAB report for the purpose of future access. Above figure is the attendance report of the individual students for each class.

V. CONCLUSION

We used the Eigen faces to represent the features vectors for human faces and the corresponding faces of the user are stored in the database, later and these images are matched along with the RFID cards of each user for the

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

purpose of authentication and their respective attendance saved in a report. After the periodical intervals of time the percentage of each student is intimated through an SMS.

By using databases, the data is more organized. This system is also a user friendly system as data manipulation and retrieval can be done via the interface, making it a universal attendance system. Thus, it can be implemented in either an academic institution or in organizations. However with the increase in number of users the coding part increases which in turn makes the whole process slow. This problem can be rectified by using a dedicated database tools like MySQL or Oracle.

REFERENCES

TEXTBOOKS:

- [1] Ononiwu G, Chiagozie, Okorafor G. Nwaji. "Radio Frequency Identification (RFID) Based Attendance System With Automatic Door Unit". in *Academic Research International*, ISSN-L : 2223-9553. 2012; 2(2).
- [2] ZatinSinghal and Rajneesh Kumar Gujral. "Anytime Anywhere- Remote Monitoring of Attendance System based on RFID using GSM Network". in *International Journal of Computer Applications* (0975-8887). 2012; 39(3).
- [3] Herdawatie Abdul Kadir, MohdHelmyAbd. Wahab, ZarinaTukiran, Ariffin Abdul Mutalib. "Tracking Student Movement using Active RFID". in *9th WSEAS International Conference*, ISSN : 1790-5117.
- [4] ElisabethIlie-Zudor, ZsoltKemeny, Peter Egri, Laszlo Monostori. "The RFID Technology and its Current Applications" in *MITIP-2006*.
- [5] Mohd. Firdaus Bin Mahyidin. "Student Attendance Using RFID System". in *University Malaysia, Pahang*, May- 2008.

WEBSITES:

www.ieeexplore.com
www.google.com
www.mathworks.in