ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

A FLAWLESS PASSPORT VERIFICATION SYSTEM AND E-TRACKING OF LUGGAGE USING BIOMETRIC AND RFID TECHNOLOGIES

Dr. P.Gnanasundari, Ph.D., HoD/ECE, SNS College Of Engineering
A.Arokiyadass, M.Gowtham Karan, S.Vijay Ganesh
Department Of Electronics And Communication Engineering
UG Scholar, SNS College Of Engineering
Email id: hod.ece.snsce@gmail.com, malardass2000gmail.com, gowthamkaran07@gmail.com, vijayvicky2011@gmail.com,

ABSTRACT:

The main aim of this project is innovative hardware and which deals with passport authority management. The of the project is to simplify the job of the security people and to have a flawless passport verification system. In project are using a new technique that is a combination of RFID and Biometrics. By using this technique the details of the person will be stored and recognized by the fingerprint organization system and information will be stored in the microcontroller's memory. Person details will be checked by using fingerprint module and RFID. Then the corresponding information will be displayed on the LCD and is sent to the immigration room through wireless technology to verify for safety purpose of passengers. These include the implementation of the RFID luggage tracking system in airports. This project is used to announce the name of the particular person to collect their luggage at the luggage counter. Nowadays the luggage will be moving on a conveyor belt and the concern person will watch for their respective bags and collect them. This project instead, automatically announces the name of the particular person to collect it. In announcing the passenger name we have used anAPR9600 chip. The mode Selection key is used to change demonstrations mode.

Keywords: 1) Clone passport verification

2) E- tracking of luggage.

1. INTRODUCTION:

Electronic passports have known a wide and fast deployment all around the world since the International Civil Aviation Organization the world has adopted standards whereby passports can store biometric identifiers. The use of biometrics for identification has the potential to make the lives easier, and the world people live in a safer place. The purpose of biometric passports is to prevent the illegal entry of traveler into a specific country and limit the use of counterfeit documents by more accurate identification of an individual. This project instead, automatically announces the name of the particular person to collect it. So that the persons need not stand at the conveyor. This helps to reduce the congestions at the luggage counter and the time of the passengers to avoid the smuggled goods in luggage

Even now a days in India also using to implement the electric passport to all the old written passport holder to change as a electric passport the aadhaar card information feed into biometric e-passport because here the aadhaar card have a every individual person of biometric information stored in aadhaar card though who are living in Indian country So that the persons need not stand at the conveyor. This helps to reduce the congestions at the luggage counter and the time also. The RFID tag is attached to every baggage. The RFID reader is fixed on the conveyor.

So when the luggage comes near the reader, its code is read by the reader and it checks the database for the name of the particular person and announces it through the speaker..

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

2. EXISTING SYSTEM:

In airport now a day's they are using the biometric verification for individual details of security purpose. It is stored in computer system but not available in online process.

The order is not necessarily valid in all events. Sometimes a border control is not necessary or the passenger travels without baggage and does not need a baggage drop-off. For an easy overview a simplified process chain is shown which includes all major steps. For a better understanding a departure process flowchart is given below as figure 2.1.

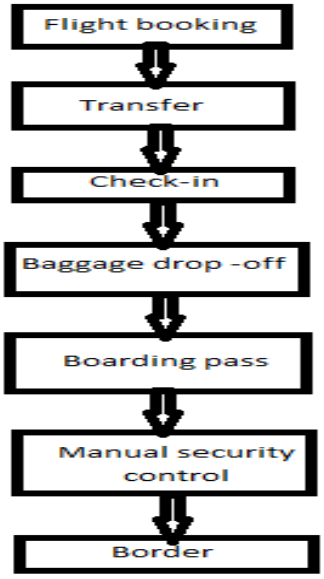

Figure: 2.1 Simplified departure process chain

Registration, seat allocation and confirmation passenger details e.g. passenger with reduced mobility, special meals, unaccompanied minor, etc. Passenger ID verification by manual, Travel document verification including payment verification, Baggage suitability size, weight/pieces, security questions, Baggage labelling and drop-off, Boarding Pass Control, required security search processes include the use of metal detectors and X Ray systems. Existing security processes are sometimes augmented by explosive trace detection systems (ETDS) as well as random hand search. Border Control Passenger boarding (registration passenger on board). The boarding time no need to take a heavy luggage for every were the luggage or drops in immigration check-in and drop the baggage in the conveyor to take while travelling to move into the flight means only hand luggage need to have with the passengers direct move to get a boarding pass and move to manual security control to check the hand luggage finally the passengers are border to get in the flight for travel the designation

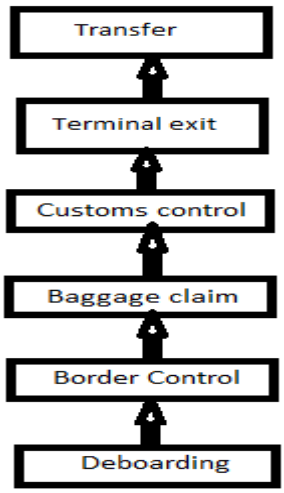

Figure: 2.2 Simplified arrival process chain

The simple view for an arriving passenger is explained in figure 2.2. Depending on the type of flight not every step is necessary. At a domestic flight the arriving passengers do not need to traverse the border and customs control.

Checking passport Checking travel document Visa, Immigration documents, etc. Collect baggage from baggage claim, bulk luggage return. Customs control by the authority of government to stop the illegal entry and baggage verification using RFID to avoid a Smuggled goods.

Disadvantage:

- Not able to find the smuggled luggage.
- It may be possible to thief the other person baggage.

3. PROPOSED SYSTEM:

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

The primary objective of the study is to produce new knowledge with respect to security of biometric techniques and RFID in a passport setting.

The results of the work should be useful for those making passport design decisions with respect to RIFD security and biometric technologies in a passport setting.

The purpose of biometric passports is to prevent the illegal entry of travelers into a specific country and to limit the use of fraudulent documents by more accurate Identification of individuals. It is interesting to find out to what extent the integration of RFID and biometric identification information into passports will improve their robustness against identity theft.

RFID tags come in three general varieties: passive, active, or semi-passive also known as battery assisted. Passive tags require no internal power source, thus being pure passive devices, they are only active when a reader is nearby to power them, whereas semi-passive and active tags require a power source, usually a small battery. To communicate, tags respond to queries generating signals that must not create interference with the readers, as arriving signals can be very weak and must be told apart. Besides backscattering, load modulation techniques can be used to manipulate the reader's field. Typically, backscatter is used in the far field, whereas load modulation applies in the near field, within a few wavelengths from the reader.

3.1BIOMETRICS IN PASSPORTS

Biometrics in passports complying with the ICAO standard consist of a mandatory facial image and fingerprints. While the former are used by a significant number of countries and thus information on them is widely available, the latter is currently used seldom. Therefore, this section only covers the vulnerabilities of (facial images, fingerprints, palm print and iris images).

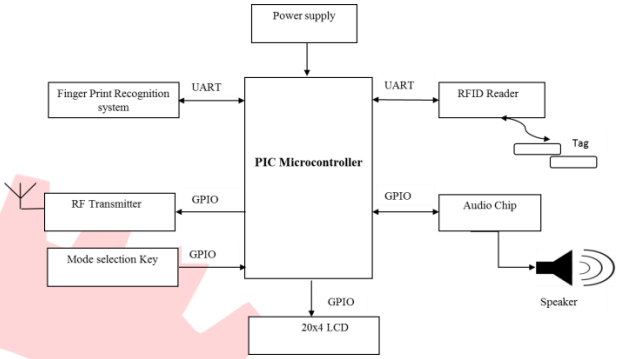

Figure: 3.1 Transmission section of the proposed system

3.2 BIOMETRIC PASSPORT SECURITY GOALS

Researcher analyzes e-passport protocols by first identifying their security goals. The researcher assumes that a country implements the highest level of Cryptographic security and multiple biometrics for the receiver section of the proposed system which is given below in the figure no 3.2.

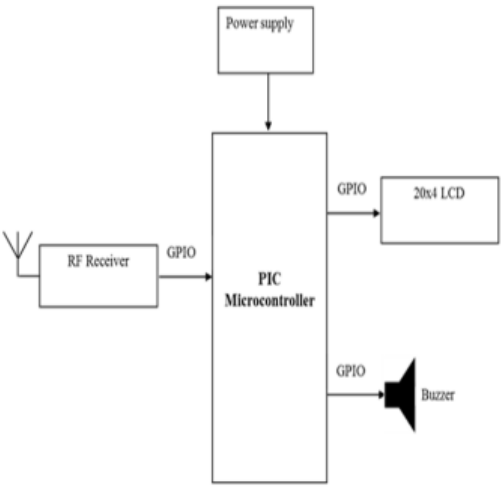

Figure: 4 Receiver section of the proposed system

3.3 RADIO FREQUENCY IDENTIFICATION

Chip is activated by a magnetic field from a reader and subsequently broadcasts the data that is stored in its memory. The fact that this personal information is being broadcast raises many questions about the use of this technology in such sensitive

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

areas such as passports. It seems that contact chip technology would be preferable. However, the International Civil Aviation Organization (ICAO), the organization that developed the standards for passports, analyzed these options and excluded contact chips for use in electronic passports. It was argued that contact chip technology, which is primarily used in card formats, would be difficult to put in a passport style document. Also, because contact chip technology requires exposed areas that require precise contact points with a reader, it was postulated that a contact chip document would not be able to function for the entire ten-year lifespan of a passport.

Therefore, a contactless chip technology, such as RFID is used in the electronic passports. The two security concerns with the use of an RFID chip in an electronic passport are skimming and eavesdropping. Skimming is the act of reading the data on a chip without the holder's permission. Eavesdropping is when a party monitors the information in the communication between a chip and an authorized reader.

ADVANTAGES:

More secure because of fingerprints which are unique for each and every person.

3.4 DISPLAY THE OUTPUT:

The output display is used with the authority of personal details in display to name and id numbers it is shown in figure 3.4

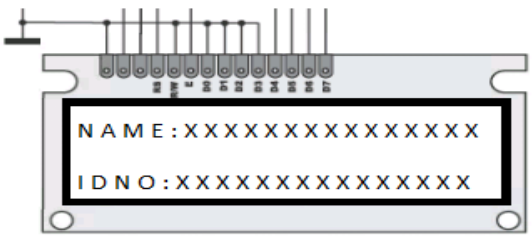

Figure: 3.4 LCD output

RESULTS

The operation of biometric passport systems depends highly on the results for existing biometrical technologies and components. These existing technologies as well as new solutions need to be evaluated on their passport system performance. An RFID chip will be embedded into the back cover of the luggage.

However, it is often forgotten that the biometric face, finger, iris, and palm prints are only one part of a fully deployed application. As biometric (sub) systems are often not designed with security and or privacy in mind, system integrators will need to address the requirements of the deployed application in this light. The fears and concerns of a significant segment of the user population need to be addressed as early as possible in the design process, to ensure that appropriate mechanisms are in place to reassure such users.

This system is also highly efficient because of baggage of the customus without manual interruption. It also makes the passengers to get alerted when the baggage arrive.

REFERENCES

1. Ari Jules, Paul Syverson, and Dan Bailey, "High-power proxies for enhancing RFID privacy and utility", Workshop on Privacy Enhancing Technologies (PET 2005), May 2005.
2. G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
3. G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol", In International Conference on Pervasive Computing and Communications, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press. 2006.
4. C.Hesher, A.Srivastava, G.Erlebacher, "A novel technique for face recognition using range images" in the Proceedings of Seventh

International Symposium on Signal Processing and Its Application, 2003.

5. G. Tsudik, "A family of dunces: Trivial RFID identification and authentication protocols", In Privacy Enhancing Technologies 7th International Symposium, PET 2007, Ottawa, Canada, June 20-22, 2007: Revised Selected Papers, volume 4776, page 45. Springer, 2007.
6. D. Monar, A. Juels, and D. Wagner, "Security and privacy issues in e-passports", Cryptology ePrint Archive, Report 2005/095, 2005.
7. HOME AFFAIRS JUSTICE, "EU standard specifications for security features and biometrics in passports and travel documents", Technical report, European Union, 2006.