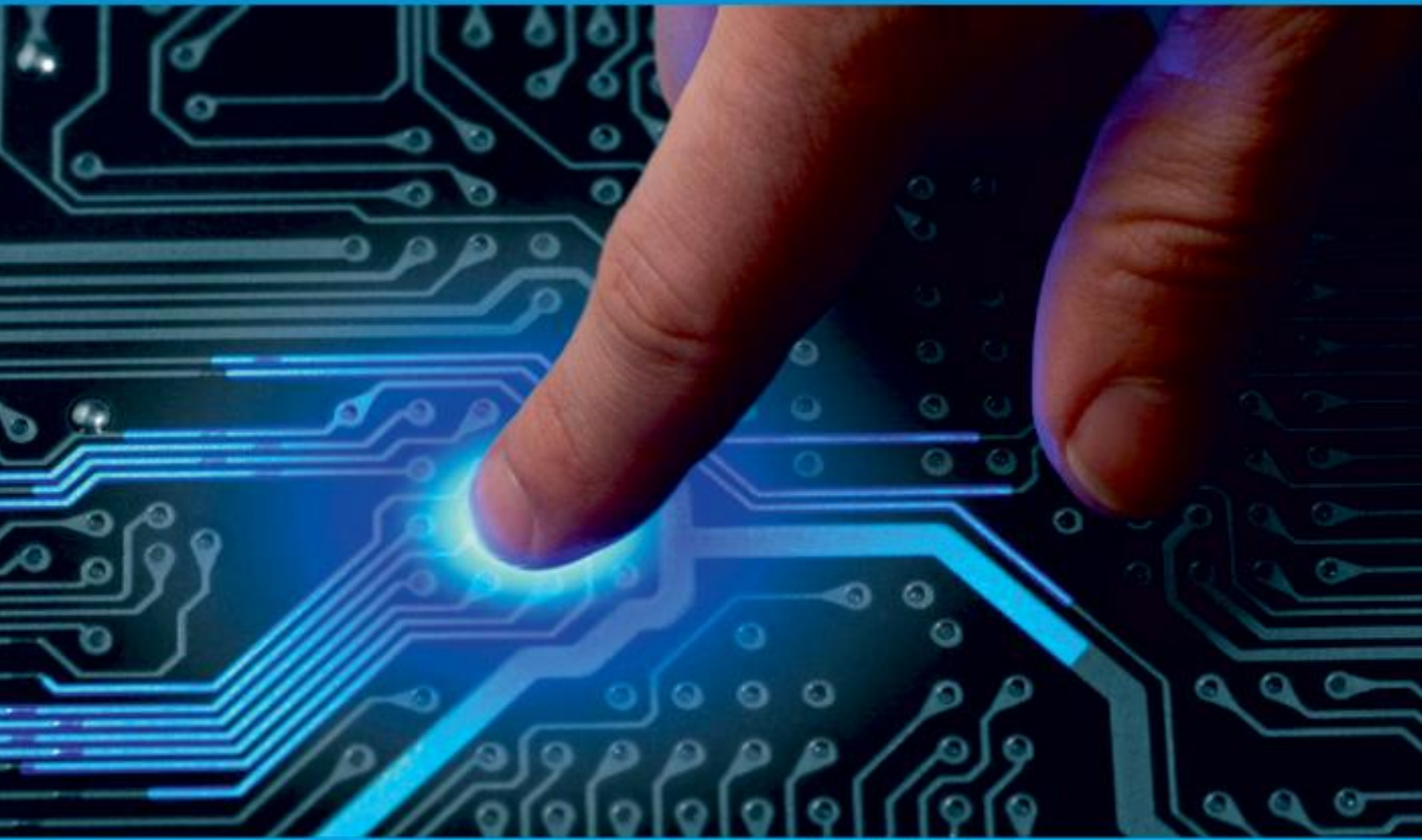
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004022 |

E-Passport Fraud Detection using IOT

Shivani Balasaheb Irole, Anjali Pandit Patil, Vaishnavi Rajendra Ghule, Harsh Rajendra Baviskar, Prof. Somnath Lomte

Dept. of Computer, KSOE, Pune, Maharashtra, India

Dept. of Computer, KSOE, Pune, Maharashtra, India

Dept. of Computer, KSOE, Pune, Maharashtra, India

Dept. of Computer, KSOE, Pune, Maharashtra, India

Dept. of Computer, KSOE, Pune, Maharashtra, India

ABSTRACT: A unified structure which provides a higher security level to e-passports is put forward. This structure corporateface and fingerprint images. It require three layers of security: the first layer maps a biometric depiction to another biometric depiction which is called biostego depiction. Three mapping strategy are proposed: the first strategy maps single biometric depiction to single biostego depiction, the second strategy maps dual biometric depiction to single biostego depiction, the third scheme divides the biometric depiction into segment and maps each segment to different biostego depiction.

A mapping function maps the potency value of each pixel in the biometric depiction to pixels with same potency in the biostego depiction. A representative pixel is randomly picked from the set of pixels, and its coordinates are recorded in the location map of the biometric depiction. In the second layer, the location map is encoded using fingerprint fuzzy vault. In the third layer, the encoded location map is hidden in the biostegodepiction using steganography technique. The biostego depiction which contains the encoded location map is stored in the epassport's memory. Keeping the mapping plan, the proposed application provides higher level of defence against fraud.

KEYWORDS*:* Fingerprint Scanner, RFID Card, RFID Reader.

I. INTRODUCTION

Advancements in technology have produce the chance of huge assurance of correct travel document assest, however, some issues relating to security and productive-ness stay unevaluated. Electronic passports have remarkable a fine and rapid readying all around the world past the International Civil Aviation Organization the sphere have modified calibre whereby passports will store biometric modifier. The em- ployment of life science for recognition has the probable to create the lives easier, and therefore the world people board a safer place. The aim of biometric with RFID Tag recommed that e-passports are to stop the misappropriated entrance of a person into a choosed country and limit the employment of counterfeit documents by a lot of correct regonization of a person. This paper analyses the fingerprint biometric e- passport style. These papers focus on the privacy and private security of bear-ers of e-passports, the particular security profit specific countries obtained by the introduction of e-passports victimization fingerprint regonization systems. The research worker recogonized its main crypto graphical features; the fingerprint life science presently used with e-passports and regarded the encompassing procedures. Research worker- centered on exposedago anyone willing to bypass the system would select a constant application. On the opposite, only desire on them could create a possibility that didn't survive with forgoing passports and border controls. The paper jointly pro- vides a security examination of the e-passport victimization fingerprint biometric with RFID tags that are assume to produce better security in shielding biometric info of the e-passport bearer.An E-Passport is an ID document that keeping connected biometric data of its bearer. It's embedded in the RFID tag that is achieved by crypto graphical possibility. The triple-crown execution of biometric techniques in documents like E-Passports aims to the strength of border security by lessen the chance of the document's holder. The e-passport additionally provideconsiderable edges to the rightful holder by providing a lot of refined proposed that of confirming that the passport belongs thereto person which it's genuine, while not privacy. The states square compute presently supplying e-Passports, which corelate to quite five-hundredths of all passports being issued worldwide. This represents an aliveequal in national and international security because it make better the integrity of passports by the one written within the document and to the physical attribute of the holders, and allowed machine-assisted verification of biometric and account data to confirm the identity of travellers.

II. MOTIVATION

In the case of normal passports which are we using nowadays, to establish a positive compare between the travel document and the person who presents it, there are four typical applications:

1. Each time a traveller enters or exits a State, his identity can be verified against the depiction created at the time his travel document was issued. This will secure that the holder of a document is the authorized person to whom it was issued and will increase the productive of any advance passenger information (API) system.

2. Two-way check The travellers current captured biometric depiction data and the biometric device from his travel document (or from a central database), can be verified to confirm that the travel document has not been change.

3. Three-way check The travellers current biometric image data, the depiction from his travel document and the depiction stored in a central database can be verified (by making biometric templates of each) to confirm that the travel document has not been change. This technique verify the person with his passport and with the database recording the data that was put in that passport at the time it was delivered.

4. Four-way check A fourth confirmational check, although not an electronic one, is plainly verify the results of the three-way check with the digitalization photograph on the data page of the travellers passport.

In the second case application for an Epassport there are two basic applications:

1) The end users biometric data, generated by the entrance process, can be used in a search of one or more biometric databases (recognition) to determine whether the end user is known to any of the comparable systems (for ex- ample, holding a passport under a different recognition, having a criminal record, holding a passport from another State).
2) When the end user collects the passport or visa (or presents himself for any step in the issuance process after the starting application is made and the biometric data is captured) his biometric data can be taken again and verified against the initially captured biometric data.

The primary reasons for worldwide compliance of E-passports over the standard passports are:

1) Secure Recognition of the passport holder.
2) Minimal chances of fake of biometric information stored in the passport.
3) Improve privacy safeguard.
4) Greater safeguard against identity theft.
5) Respite of handling entry and exit at border controls with automatic passport readers.

III. PROJECT SCOPE & LIMITATIONS

To design a illustration that will reduce fake, duplication of data entry, look-alike fraud, photo exchange, which may be done by any holder of a standard passport booklet. To come up with a more structured travel document with less human interference eliminating the fraud associated with a paper passport. This system will allow the biographic information such as family name, date of birth, gender, ID number of the bearer to be electronically stored in the system. This can also result in faster action at the border controls as the holder just have to tap their RFID cards in front of the card readers and if the fingerprint scanner is present then their fingerprints can be taken there one real-time basis to capture if the ones taken presently will depiction the fingerprints already stored in a template in the database.

- Firstly, the early adopters - countries that transitioned to the e-passport system ten years ago will prepare themselves for a technology update in order to include some of the newest features into their citizens travel document, such as biometrics.

- Secondly, the introduction of a microprocessor or chip-based passport is changing border control operations, for the better. Governments around the world are now progressively provide with e-passport scanners, fingerprint reading machines, and even automatic check-in systems, accelerating the speed at which passengers are verified. E-Passports will continue to facilitate smooth, compatible, and secure authentication of travellers in the near future.
- Thirdly, thanks to the infinite of security features embedded in the e-passports, governments will send on them more and more as international travel expands. Today, as the threat of terrorism looms large, a top priority of the border control offices is to recognize and stop high risk particular from passing through. By exploit advanced technology featured in e-passports, border control authorities can enhance the accuracy of verification and imaginably reduce the bypassing of high risk particular into the border.
- Last but not least, e-passports are fast turning into a medium for countries to showcase their classical landmarks and unique citizens symbols on paper. On that note, governments will have higher design assumption for future e-passports. So far, many countries have been able to deliver unique travel documents that in time became works of art and symbols of joy in the hands of their national.

IV. HARDWARE COMPONENTS

- **Biometrics:**

Biometrics is the automatic measurement of biological or behavioral features that identify a person The major components of biometric system used in E-passport are:

1. Capture
2. Extract
3. Create Template
4. Compare

The fingerprint identification technique is used to implement and understand this project.

- **SCENARIO IN WHICH MULTI-CORE, EMBEDDED AND DISTRIBUTED COMPUTING USED:**

  - **Arduino Uno board**

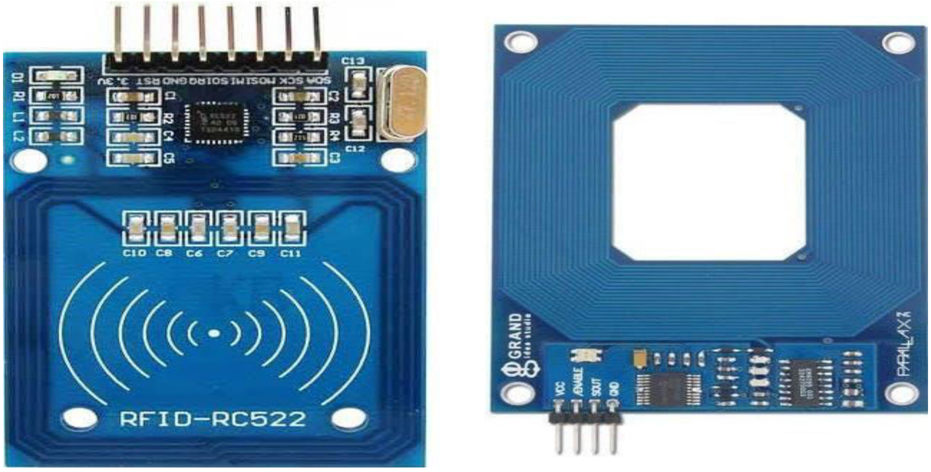
These days many people try to use the arduino because it makes things simple due to the simplified version of C++ and the already made Arduino microcontroller that you can programme, erase and reprogramme at any given time.

- **Fingerprint Scanner**

To inspect biometrics we are using fingerprint scanner.Fingerprint scanners have distinctive patterns/design that can be used to unique one scanner from another one. The pattern/design, which we call scanner pattern, stems from the flexibility of device characteristics at silicon level and is generate by defect of the change from the input to the scanner (i.e., the object applied to it) to its output (i.e., the digital image).

- **RFID Scanner/Reader**

  The RFID reader is also known as an interrogator, it supply the connection between the tag data and the software that require the information.



V. RELATED WORKS

The e-passport possesses two feature of technology which are RFID and biometrics all incorporated so as to securely recognize and verify the agent possessing that journey document. In this part of chapter one the writer will plot, acknowledge and repeat similar works that have been done on the e-passport in hug and also state how this project is going to be distinguish from all these works.

1) E-passports are already accessible and in use in various European countries and variousinvestigation have been conducted around the world following their categorization in these countries.[5] Kumar et. al discussed the efficient execution of e-passports scheme using cryptographic security along with manybiometrics.In this article he states that an e-passport is an recognition document which possesses necesscary biographic and biometric details of its bearer on paper and also has this detail embedded on an RFID chip which is capable of

cryptographic functionality. However this project speak to eliminate the design of having a passport booklet with an RFID chip embedded on it but rather just make use of an RFID card with all the details stored on that card.

2) In the e-passport design Kumar also talks of the certification whereby the authentication methodincludes two processes which are Registration and Verification whereby throughout the former step the candidate registers their biometric under human administration and the information is stored on the passport tag. However the e-passport designed in this project vary in the sense that rather of having the data stored on the tag to be duplicated on the paper passport, the details should be stored in a centralised system database which is only accessible to the authorised person at border controls. Such that the border formal will have to physically check what the system is showing with the physical appearance in-front of them to see if it similar.
3) In a thesis note by BC Vollmer in 2006 titled Biometrics, RFID technology and the e-passport he states that the American e-passport will have an RFID chip embedded interior the back cover of the passport folder and it will save the same data that is printed on the bio-data page of the passport booklet/folder. This project hold that if the passport booklet and the chip are both save with the similar information why then not resort to only one thing the RFID card which will saveall thedata because RFID cards are easy to replace if lost and they are portable (easy to shift around with or carry with you all time) than a passport folder. Note that the RFID card and the Chip use the similar principle of working and same technology. No doubt that this RFID card then must incorporate powerful security characteristic to protect against remove and information altering.
4) Vollmer as well states that the RFID chip develop in the e-passport is a passive, write once, read many version of an RFID chip technology. Whereas this project would like to observe the chance of note on the RFID card many times so as to constantly improve the photographs of the passport holders in the system after a certain period of time so as to keep them improve as possible. With the American e-passports chips can’t be altered after manufacture. The writer Vollmer introduce also of the read range of this American e-passport which is about 121.9cm and it is the read scale when the passport is opened. Now with the RFID tags it will depend withtype which one is using but the ones appropriate for this project are the Less frequency RFID tags which have a low read range than that of chip. Since both use the RFID technology the Faraday Cage may be applied to shield the RFID cards or the chip from transmitting any farther than a some centi-metres.
5) An E-Passport holder holds an electronic chip such as RFIDs and fingerprint. The chip holds the samedetails that is noted on the passport data page such as the passport holders name and other information. An E-Passport holds a biometric recognition. The US needs that the chip should include a digital photograph of passport owner. All E-passport issued by Visa Waiver Program countries and the United States have security characteristics to prevent the unlicensed analysis or examining of data save on the E-passport chip.
6) This RFID and Biometrics technologies was suggest in paper. The study of recent technologies used in E-passport system. Personal capability and bearers biometric detail is stored on RFID chip which is used in verification process by border security officers. The next generation of e-passports will executemany advanced cryptographic mechanism, collectively known as an Extended Access Control, and in particular a protocol referred to as Chop Authentication that shield an e-passport will executemany advanced cryptographic mechanism, collectively known as expand Access Control, and in particular a protocol referred to as Chip Authentication that shield an e-passport against cloning and transferability attacks. The Ex- tended Access Control Suite of agreement has found minor attention in the literature until now.

   With these inner facts one can conclude that with the use of an RFID based e-passport it will be very hard for sophisticated counterfeiters to steal these RFID based e-passports cards and alter the data to match them. It should show to be impossible.

VI. CONCLUSION

The project has examine the great current and potential utilize of RFID in identifying documents. The important characteristics of this project is security and time wastage includes in validation of passports. Inclusion of RFID technology into machine readable documents will better their robustness opposed to identity theft.

| DOI: 10.15680/IJIRCCE.2022.1004022 |

REFERENCES

[1] KeertiSrivastava, Amit K. Awasthi andR.C.Mittal*Biometric based RFID tag mutual authentication protocol defending against illegitimate access* -2018, Malaya Journal ofMatematik[102-106].

[2] Gualberto Aguilar, Gabriel Sanchez, Karina Toscano, Moises Salinas, Mariko Nakano, and Hector Perez. 2007. *Fingerprint Recognition*.In Proceedings of the Second International Con- ference on Internet Monitoring and Protection(ICIMP '07). IEEE Computer Society, Washington, DC, USA, 32-. DOI: https://doi.org/10.1109/ICIMP.2007.18

[3] Y.A. Badamasi, *The working principle of an Arduino," 2014 11th International Conference on Electronics*, Com- puter and Computation (ICECCO), Abuja, 2014, pp. 1-4.URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?

[4] Ivanov, Vladimir I. and John S. Baras. *Authentication of fingerprint scanners.* 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). (2011): 1912-1915.

[5] S. Kundra, A. Dureja and R. Bhatnagar, *The study of recent tech- nologies used in E-passport system*, 2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS), Trivan- drum, 2014, pp. 141-146.

[6] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, "Untraceability in the applied pi-calculus," in Proceedings of the 1st Int. Workshop on RFID Security and Cryptography., 2009, to appear

[7] Piotr Porwik, "The Biometric Passport: The Technical Requirements and Possibilities of Using", Biometrics and Kansei Engineering, International Conference - ICBAKE on 2009, pp. 65.

[8] Dr Albert B. Jeng, Elizabeth Hsu, And Chia-Hung Lin Sponsor: "Should and How CC be used to evaluate RFID based Passports‖

[9] K. Nohl and D. Evans, "Privacy through noise: a design space for private identification," in Annual Computer Security Applications Conference (ACSAC 2009), 2009.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING