Vol. 6, No. 10, October 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Universal Developing of Persons Identification Based on RFID

[1] Ghazi Ibrahem Raho, [2] Muzhir Shaban Al-Ani, [3] Alaa Hussein Al-Hamami, [4] Raed Kanaan
Amman Arab University, Jordan
Anbar University, Iraq
[1] larsa_rr@hotmail.com, [2] muzhir@gmail.com

ABSTRACT

The forged passports become one of the important challenges facing the world, because each country has its own specifications about their passport and passport is the property of the country. The proposed system tries to integrate many factors to develop an efficient system. The main objective of this system is to compare, update the data continuously and to predict accurate new features for future. The proposed e-passport system can be used easily, adapted to different environment, and it is a secure system. The e-passport system based on the generation of an encrypted key depending on the combination of passport number, birth date and country code. This generated key is watermarked via the image posed at the passport.

Keywords: *E-passport, watermarking identification, secure passport, standard passport, secure key.*

1. INTRODUCTION

Mahmoud Al-Mabhouh was assassinated at 19 January 2010 in Dubai. In the framework of international interactions European Union of Al-Mabhouh deplored the use of the killers Al-Mabhouh forged passports from countries member of the Union. This international incident leads to big alert in forged documents, and one of these international documents is the passport which is an international personal identification with different forms.

In 1968 the International Civil Aviation Organization (ICAO) has been developed an efficient passports. This organization determines the beginning of an adequate document such as a passport card, an identity card with the requirements of document control. The best type of electronic system procedures and the device use for the indicated documents that are introduce in the available resources of Member States; the stander document feasibility of the needed information and ways of introducing this information through automated processes, considering that these methods would in phase with the security and privacy requirements and the required speed of the procedure [1].

Basic access control is the implemented method applied to cancel unauthorized disclosure of digital data that stored in the environment of e-passport and biometric e-passport (fingerprint and face). Optical scanner is used to read indicated zone from the data page of the e-passport.

The required data including, birth date, the number of passport and the expiry date of passport, these information are used to calculate a required key. Then the encryption process for the information is started using the generated key of e-passport so it is difficult to skim of data [2,3].

Step by step, the world becomes digital including e-government, e-monument, e-business, e-identification, and e-learning. One of the most important activities is e-passport in which we need to manage many factors such as quality, security, speed, as well as privacy.

2. E-PASSPORT

Traditional passports are used to identify human persons. These passports are replaced by e-passport (electronic passport) that including many privacy and security aspects according to the developed technologies.

E-passports contain memory chip that stored personal documents of the individual. The International Organization generates global standard e-passports. This organization established two e-passport standards to help countries to implement passport documents as shown in figure (1) [4].

- **Basic Access Control (BAC):** it is a first-generation biometric e-passport applied via Radio Frequency Identification (RFID).
- **Extended Access Control (EAC):** it is a second generation of biometric e-passports applied via Radio Frequency Identification (RFID).

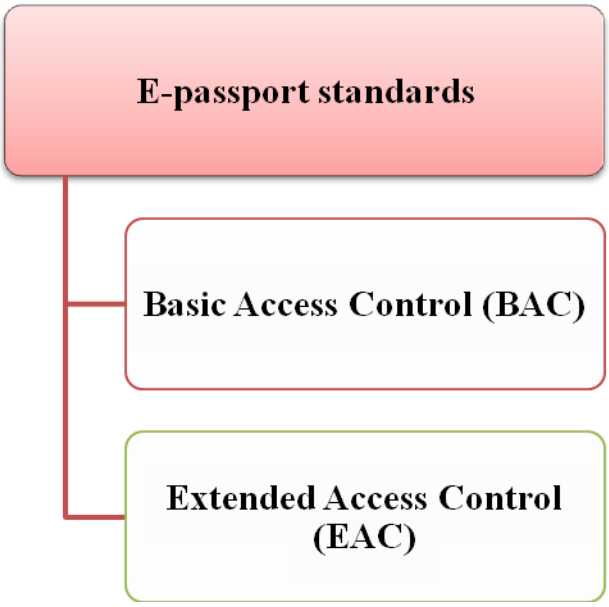

Figure 1: E-passport standards

3. RELATED WORKS

Many literature reviews are published to design and implement human identification as e-passport as below:

Gildas Avoine et al. (2008) proposed a secure e-passport that provides the basic encryption key and in addition that in 2003 Belgian passport recipient Interpol which denoted as the most secure passport in the world [5].

Luis Teran et al. (2009) depend on the characteristics adapted by International Civil Aviation Organization they implemented biometric passport applets with efficient security. The developed system can apply the communication between the implemented system and the cards that implemented using Java [6].

Pravir Chawdhry et al. (2010) implemented e-passport as a international aspect trust between real time and offline environments. The implemented architecture is done for a network based digital identification system to support e-government services, high private services and e-commerce [7].

V.K. Narendira Kumar and B. Srinivasan (2011), gave a scope of challenges arise in electronic biometric passports. This work concentrated on security and privacy factors of electronic passports. This system is introduced many biometric features as face, fingerprint, and iris. The implemented system deals with good results of recognition and identification [8].

4. PROPOSED STANDARD E-PASSPORT

The proposed system can be divided into the following parts:

1. Identification Unit, this unit contains 15 digits as the following:

   - One digit for passport type.
   - Three digits for country identification.
   - Eleven digits for passport number.

The proposed architecture as shown in figure (2) is able to recover all the population growth during the next 100 years.

Type	Country no.			Passport no.										
1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th

Figure 2: Passport number construction

2. Physical design card unit, this unit relates to the physical card dimension (8*4) cm, person name, picture name and plastic cover.

3. Image processing unit, this unit relates to face identification, verification and prediction, then passport number recognition and identification, in addition a hidden number recognition.

4. Memory specification unit, this unit relates to prepare a memory RAM of 1 Mbytes that can be read/write with special secure device, in which saved the required information.

Vol. 6, No. 10, October 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

5. Network Unit, this unit concerns with the connections of all departments sites, airports, borders, etc. this units serves sharing of information all over the world via secure high speed Internet.

6. Database unit, this unit concern with huge repository distributer all over the world. The required algorithms are implemented to collect, refine and retrieving adequate information.

7. RFID unit, this unit prepares tags for passports that deal with identification numbers and reader that situated at airports, borders, etc.

4.1 Proposed Standard E-Passport Units

To validate the functionality of the overall system, we can divide the standard e passport into four main units:

First unit is the physical identification card (passport document) that including a ministorage device contains the electronic information about the passport and information that identify the specific person. This information deals with:

- Passport number (primary key).
- New picture of the related person.
- Birth date (2 digits for day, 2 digits for month & 4 digits for year).
- Person mane (1st name, 2nd name, 3rd name & family name).
- Originator country (name of the country).
- Passport generation date.
- Passport expiry date.

Second unit is the hidden information that storage on a mini secured read/write storage device that is out of management of any human being, this storage device are partitioned into isolated parts each part is responsible only on one specific information as the following:

- Visa (permission to enter the destination country), that can be passed from any gate on the frontiers or agencies.
- Normal information about the related person that is mentioned above that can be read only from any gate on the frontiers or agencies.
- Secured information those are hiding via the coded image that can be read only from any gate on the frontiers.

Third unit is the reader device which situated at the gate of all departments sites, airports, borders, etc. This device is an e passport reader device, which can read all documents of the passport including the hidden information. Also, this device can mark up a sign for a person passed the airport gate, and this sign contains date and time. In addition, this device works automatically (person monitoring) and gives a silence alarm when some is wrong.

Fourth unit is the communications unit which including a transceiver in each side of the system (passport side and reader side). This unit consists of two parts; one is RFID active tag, which is mounted on the passport and other part is the RFID reader, which is situated at the gate site.

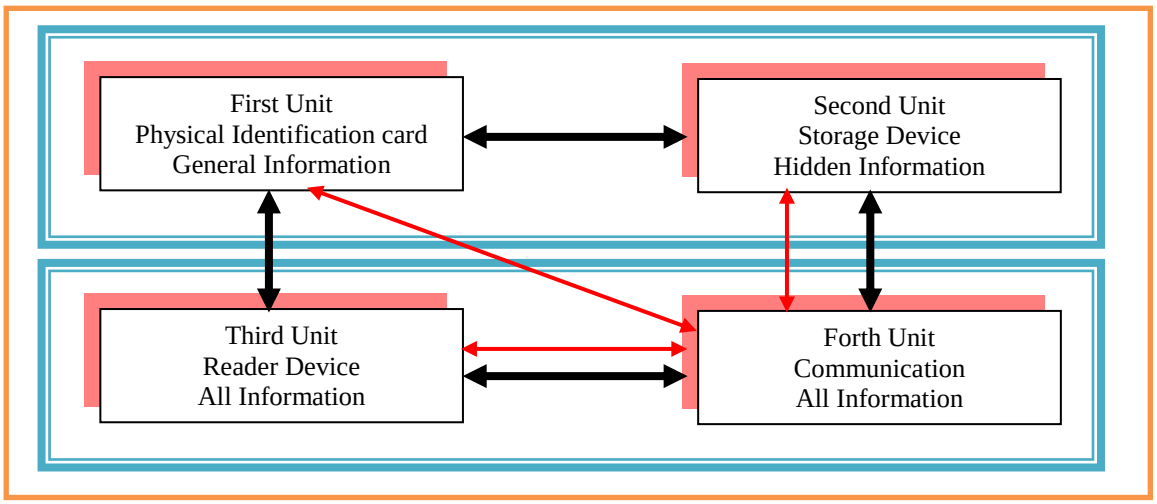

Figure 2: E-passport system units

4.2 Proposed Standard E-Passport Gates

When the system is implemented all over the world and two gates are required in each airport apart of 5m between gates. The system operation started when the person stand in front of the first gate situated at the airport (for example). These two gates operated as the following:

First gate order the coming person to stop and order the camera to take a face image to the person in

Vol. 6, No. 10, October 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

front, then the identification process start to perform all document stored at the passport.

Second gate starts operation when it received the order from the first gate. This gate open the door when all documents are right, but when there some think wrong, an alert appears to indicate that this person must be checking other time and this door not open.

4.3 Proposed E-Passport System Infrastructure

The infrastructure of the e-passport system is constructed of many data acquisition devices, computers and networks and their supported devices as shown in figure (3). Considering that these devices are labeled and updated to avoid the damage that may be occurred during the heavy duty working.

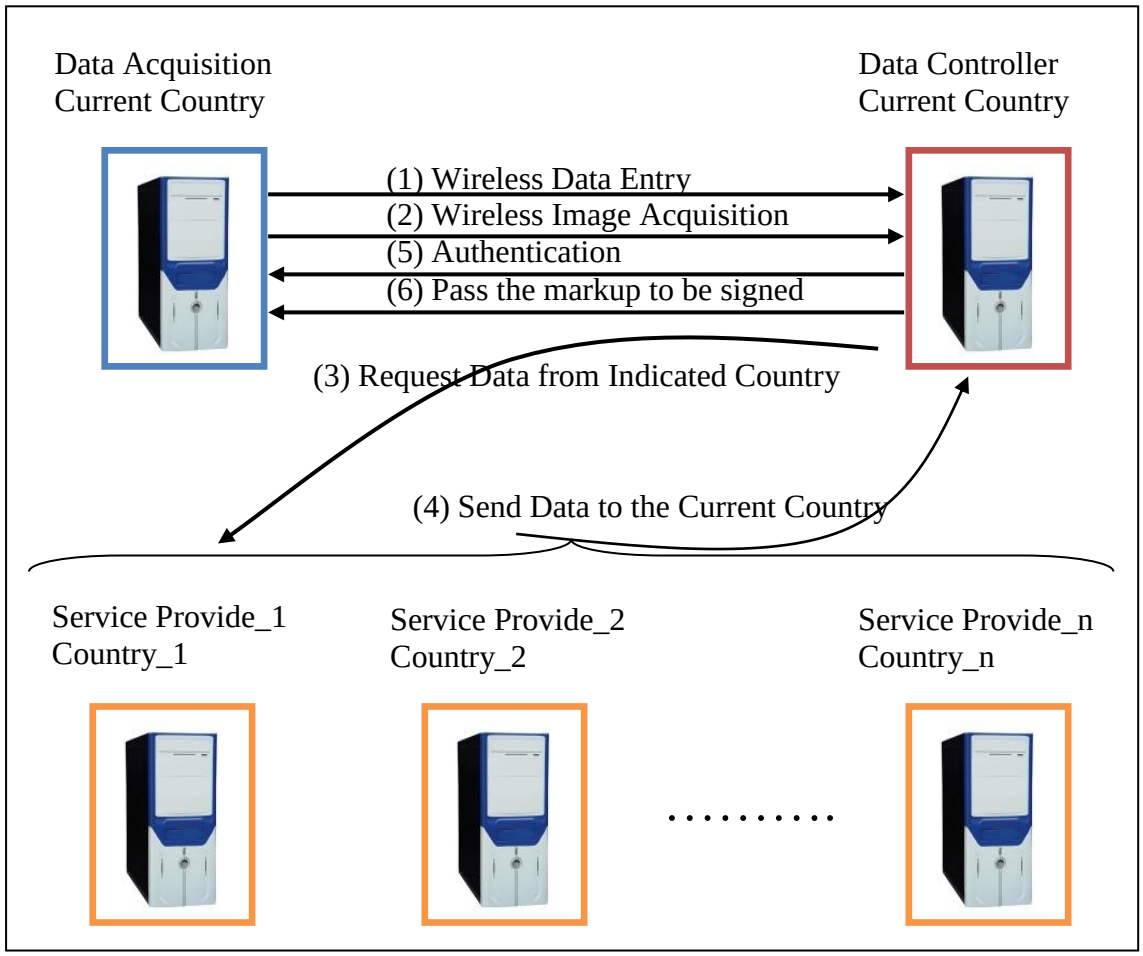

Figure 3: E-passport system infrastructure

4.4 Proposed Standard E-Passport Operations

The system operations can be performed as the following steps:

First step starts when the traveler started to pass the first gate which does many functions:

- A sensor located in front of the first gate activates a camera.
- Compare the taken picture to the stored one.
- Compare the stored information of the passport to validate the passport.
- Open the first gate to pass the passenger to the second gate.

Second step starts when the passenger pass the first gate toward the second gate (all documents are OK) which do many functions:

- Mark up the entry information when the passenger arrives.
- Mark up the departure information when the passenger leaves.

4.5 Security in the Proposed Standard E-Passport

Many operations must be taken in consideration to evaluate an efficient secure method, these points are mentioned below:

- **Begin**, the tag of Radio Frequency Identification Device begins to work when the traveler is standing near first gate of the system.
- **Encryption**, a key number is generated and encrypted from mixing of many factors depend on human specification.

- **Watermarking**, the encrypted number is used for watermarking process via the image fixed on e-passport.
- **Comparison1**, comparison operations implemented between the extracted face processing with the data covered-passport.
- **Comparision2**, comparison operations implemented between the extracted iris processing with the data covered e-passport.

In addition, when there is any mismatching of the information or any doubt, an interrupt stop the procedure and then the passenger is out of permission to pass.

4.6 Passport Construction Approach

The passport construction algorithm is very important case to validate the passport therefore it must be sure that all documents are correct and valid at that time, and also it must be sure that the indicated person has no other passport. After that you can pass to the passport construction algorithms which encrypt the generated key via the introduced data that watermarked in the passport.

4.7 Passport Information Retrieval Approach

The passport information retrieval algorithm is an authentication case to validate the passport and to insure that all documents are correct and valid at that time, and also insure that the indicated person is the same as indicated at the passport. The passport information retrieval algorithm which used to compare the watermarked key with the generated key to decide the identification.

4.8 Encryption Key Generation Algorithm

Encryption key generation algorithm is very important part of e-passport in addition to the validation of the collected data of the indicated person. The proposed algorithm depends on the following data:

- **Passport personal identification number (11 digits),** the passport is contained of 15 digits as mentioned previously; One digit for passport type, three digits for country identification, eleven digits for passport number. This number is Unique and can be used as primary key for any operation. In the encrypted side the passport personal identification number is resorted in a way to perform a part of the final key.

$$X= [x1\ x2\ x3\ x4\ x5\ x6\ x7\ x8\ x9x\ 10\ x11] \quad (1)$$

- **Birth date identification number (8 digits),** this part identify 2 digits day, 2 digits month and four digits year, this number is not identical and may be repeated more than one times, and it used as a part of the final key.

$$Y=[y1\ y2\ y3\ y4\ y5\ y6\ y7\ y8] \quad (2)$$

- **Country identification number (3 digits),** as the last statistical survey there are 257 countries in the world, and 3 digits is sufficient to cover 999 countries. In the encrypted side the passport country identification number is resorted in a way to perform a part of the final key.

$$Z=[z1\ z2\ z3] \quad (3)$$

- **Image personal identification number (Passport Number) (11 digits)**, this number is generated using a feature vector of DWT of the personal stored image.

$$DWT=[dwt1\ dwt2\ dwt3\ dwt4\ dwt5\ dwt6\ dwt7\ dwt8\ dwt9\ dwt10\ dwt11] \quad (4)$$

- **Combining process,** this process follows the following procedure:
  Combine Y and Z as below:

$$YZ=[y1\ y2\ y3\ y4\ y5\ y6\ y7\ y8\ z1\ z2\ z3] \quad (5)$$

Combine X,YZ and DWT using the following equation:

$$K= \text{int}\ [(X+YZ+DWT)/3] \quad (6)$$

This final equation is used to generate the key, and then this key is encrypted and stored as watermarked key via the personal image at the e-passport.
The steps can be implemented perform the encryption algorithm.

4.9 Decryption Key Generation Algorithm

The most important part of the e-passport is how to retrieve the encrypted information to get the detailed information of the specific person. This algorithm is implemented using the following steps:

- **Key retrieving process**, this process retrieves the encrypted watermarked key from e-passport.
- **Decrypt the retrieved key,** this process backward the combination key K through a certain operations.
- **Comparing process,** this process compares the obtained key K with the values of X, YZ, DWT to verify the overall information of the passport.

5. CONCLUSIONS

Many factors are introduced to develop an efficient e-passport system. Many processes must be implemented to legalize and authorize e-passport system.

This system introduces a procedure to compare, update the data continuously and predict accurate new features for future aspects. The proposed e-passport system offered many advantages such as flexible, easy to use, updating, person tracking and it is difficult to copy.

The proposed e-passport based on the generation of an encrypted key depending on the combination of passport number, birth date and country code. This generated key is watermarked via the image posed at the passport. To facilitate the system operation, all access and operations to this system is done via wireless media using RFID technology.

REFERENCES

[1] Ruwantissa Abeyratne, "The use of forged passports of foreign nationals in international criminal activity", Journal of Transportation Security (2010) 3:127–145

[2] EleniKosta, Martin Meints, Marit Hansen and Mark Gasson, "An analysis of security and privacy issues relating to RFID enabled ePassports", International Federation for Information Processing (IFIP), vol. 232, 2007.

[3] Ghazi IbrahemRahoet al., "Signature Recognition Using Discrete Fourier Transform", IJBICT is published in cooperation with The American Society for Competitiveness March 2015, Vol.1, No.1-2

[4] Bob Carter, Chairman Brussels Interoperability Group, "Government Entrust ePassport Security Solutions", http://www.entrust.com/government/e-passport.htm, accessed at 1/11/2010.

[5] GildasAvoine et al., "ePassport securing International Contacts with Contactless Chips", FC 2008, LNCS 5143, PP141-155, 2008.Springer-Verlag Berlin Heidelberg 2008.

[6] Luis Teran et al., "On Development of Inspection System for Biometric Passports Using Java", BioID-MultiComm2009, LNCS 5707, PP260-267, 2009.Springer-Verlag Berlin Heidelberg 2009.

[7] Pravir Chawdhry et al., "Use of ePassport for Identity Management in Network-Based Citizen-Life Processes", Privacy and Identity, IFIP AICT, PP 122-133, 2010. Springer-Verlag Berlin Heidelberg 2010.

[8] V.K. Narendira Kumar and B. Srinivasan, "Design and Implementation of E-Passport Scheme Using Cryptographic Algorithm Along with Multimodal Biometrics Technology", International Journal of Advanced Information Technology (IJAIT) Vol. 1, No. 6, December 2011.