ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse52862019.pdf
https://doi.org/10.30534/ijatcse/2019/52862019

Developing the Security and Protection of the Electronic Passport

Dr. Omar Radhi Alzuobi [1], Dr. Bilal Radhi Alzuobi[2], Dr. Hamza A .Ibrahim[3], Marwan A. Al-Namari[4]

[1] College of Computer at Al-Gunfudah, Umm Al-Qura University, Saudi Arabia, orzubi@uqu.edu.sa
[2] College of Computer at Al-Gunfudah, Umm Al-Qura University, Saudi Arabia, brzoubi@uqu.edu.sa
[3]College of Computer at Al-Gunfudah, Umm Al-Qura University, Saudi Arabia, haibrahim@uqu.edu.sa
[4] College of Computer at Al-Gunfudah, Umm Al-Qura University, Saudi Arabia, manamari@uqu.edu.sa

ABSTRACT

Abstract— proposes to develop a security technique to be used with the e-passport in the airports to read its holder information by using Radio Frequency Identification technique (RFID). The proposed system concentrates on the security part of the e-passport. The code produced by the issuing country will be hidden in the passport photograph by using steganography mechanism. At the same time this code will be stored at the RFID tag. This code will be read by the control point in the airport using Nearest Field. The other part will be operated at the control point to make sure of the e-passport validity by checking the hidden code using NFC and verification it with the one in the RFID tag. The proposed method is one way in helping for the design of the E-passport to help in passing passengers through the control points in very fast and accurate way. This will help to control the crowded airports in processing the passage procedures.

Keywords: Nearest Field Communication, Radio Frequency Identification, and Epassport.

1. INTRODUCTION

E-passports composed of three technologies; Biometrics, Radio Frequency Identification technology (RFID) attached to the paper-style passport with connectivity using Public Key Infrastructure (PKI) to authenticate the reader devices in the control points and the RFID chip, and to secure the communication between the chip and the reader device. The personal credentials and bearer's biometric data that are saved in the chip must be encrypted using cryptography methods to secure them against any unauthorized readers.

The characteristics and specifications of e-passport are documented and proposed by International Civil Aviation Organization (ICAO)(Kundra &et al., 2014).

2. UNITS

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary.

2.1 Figures and Tables

The proposed schema in (Saeed &et al., 2009) take benefit of the optional data capacity of the standard format of MRZ (location 29-42).Firstly, create string S1 which equals Document Number || Date of Birth Date of Expiry. Then, encrypt it with the private key stored in the Tag and print the most significant 14 hexadecimal characters of the resulted ciphertext at the location 29-42 of MRZ. The corresponding check digit is also calculated and could be printed at location43.

At the access control, the resulted ciphertext is read optically by the reader to derive the BAC keys (KENC and KMAC). After reading the ciphertext, it interpreted as an ASCII code and converted to its corresponding binary code to form a 14 bytes sting. Each byte will be compressed by the reader to form 4-bits of data hence the resulted data is a 7 bytes long of string. Finally, the resulted compressed string is used to calculate SHA-1 hash code and the most significant 16 bytes are selected as K seed which in turn used to create the BAC keys.

The first advantage of ACASP that it has no link to the data of the EF.COM file, which can be amended and then the AA can be by passed. Therefore, the ACASP can fights strongly against chip cloning, and the AA can be omitted. The second advantage of ACASP is that it can with stand the skimming threat using BAC keys generation process. The computational load of the public key encryption is reduced in both the reader and the Tag. [1]

The authors of (Ghatak, Nayak & Sindhura, 2013) proposed a method for securing the traditional passport without the need for using electronic chip. Their method is based on visual cryptography for verification and uses Palm Vein for authentication of the passport holder at the checkpoints. The visual cryptography method encrypts the cover image into several shares.

In pre-processing module, a global threshold algorithm is applied to the scanned copy of the signature image. The threshold algorithm follows the equation 2.1.

$$g(x,y) = \begin{cases} 1 & if\ f(x,y) \geq T \\ 0 & otherwise \end{cases}$$

…… 2.1

Where $g(x,y)$ is the threshold version of $f(x,y)$.

A special pre-processing technique is then applied to the thresholder signature image and cover image in which the two images are divided into 2 × 2 block size. Then, for each block, the block with Hamming Value H(v) {3} is converted into block with H(v) {4} and the block with H(v) {1} is converted into block with H(v) {0}.

In the second module, Master share generation, the idea is to permute the columns of the matrix M = [1 1 0 0] to select blocks of size 2 × 2 randomly. The result of this module is as depicted in Figure 1.

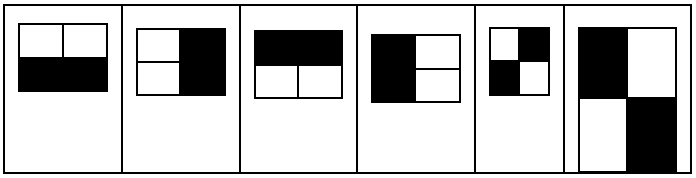

Figure 1: Resulted blocks of Master Share generation

In the final module, a block of size 2 × 2 is fetched from the cover, signature and the master share. The blocks of the innocent general share are constructed from the fetched combination of the Hamming weights for the pre-processed cover image, signature image and the master share. The master share and the resulted general share are then stacked using OR operation, and the general share and master share are stored in the central database. [2], [3]

In the second phase, depending on the provided passport number in the booked ticket, the necessary information, like palm vein, stacked master share and stacked general share, for the passport owner is travelled from the central database to the check point's fragmented database. At the passport holder arrival time, the attached hard copy of the general share is scanned and extracted at the check point, and the master share is fetched from the check point data base and stacked using OR operation with the scanned general share. Finally, if the new stacked share is identical with the original stored stack share, the passport is valid. Otherwise, the passport is not valid and must be blocked.

According to the passport holder, after verification result of the passport is positive (valid passport), the passport holder authentication process can be achieved using his palm vein authentication at the check point.

(Wang, Yang, Cheng & Ding, 2013) proposed a method for e-passport verification depending on watermarking which is composed of multimodal biometric feature and the parity check code of those multimodal biometric feature. The need for the multimodal biometric feature is to verify the passport owner, and the parity check code is for the verification of the integrity of the passport itself.

In the enrollment phase, the face image is decomposed into four sub-bands; the low frequency sub-band LL is used as the embedding region for watermarking components. According to the size of the image (which is mx n), the size of LL is $\frac{m}{2} * \frac{n}{2}$. So LL is segmented into sub-blocks LLij(i = 1, 2, · · · $\frac{m}{2k}$; j = 1, 2, · · · $\frac{n}{2k}$). Finally, the watermarking wijis embedded into each pixel of the corresponding sub-block LLij.

In the authentication phase, a watermarking extraction process is done by decomposing the watermarked face image into four sub-bands; and the low frequency sub-band LL is obtained and segmented into k×k sub-block LLij.

(Butt &et al., 2013) suggested a protocol to ensure non duplication of e-passport the European Union. The goal of this protocol is to prevent the issuance of fake and duplicated passports among the European Union states by using distributed databases of alphanumeric data and multimodal Biometric features.

3. STATEMENT OF PROBLEM

The purpose of this research is to develop the security and protection of e-passport epassport. And find a solution to increase the number of passengers in all the world and maintain security inside the airports and make sure the owner of the passport accurately and high speed

4. THE PROPOSED SOLUTION

The aim of this research is to find a software method and Diffie-Hellman key exchange algorithm to share a private key between the mark and the IS system to ensure that passengers are monitored.

NFC technology allows us to identify passenger data through RFID data and through this data can identify all the passenger information and compare them with the information on the device and make sure this data is done quickly and effectively references [4], [5]

The best type to be used in e-Passport is the Passive RFID Tags because of their low cost, low power consumption, and short read ranges (use of 13.56MHz radio frequencies for communication). According to ICAO standards, the Logical Data Structure (LDS) for the storage of RFID Tags in e-passport is composed of 16 data groups ranging from DG1 to DG16. These 16 groups are write protected, and only can be written at the time of issuing of the e-passport. The first fifteen data groups store different types of data such as the encoded headshot, fingerprint, public keys, etc. Table 3.1 presents the data to be stored in each DG.

Table 1:e-Passport Logical Data Structure

Data Group (DG)	Data element
DG1	Document Details
DG2	Encoded Headshot
DG3	Encoded fingerprint
DG4	Encoded Iris
DG5	Displayed Portrait
DG6	Reserved for Future Use
DG7	Signature
DG8 – DG10	Data Features
DG11 – DG13	Additional Details
DG14	CA Public Key
DG15	AA Public Key
DG16	Persons to Notify
SOD	Security Data Element (SOD)

Details recorded in MRZ	DG1	Document type
		Issuing state or organization
		Name (of holder)
		Document number
		Check digit doc number
		Nationality
		Date of birth
		Check digit DOB
		Gender
		Date of Expiry
		Check digit DOB/VUD
		Optional data
		Check digit optional data field
		Composite check digit

Encoded identification features	Global interchange feature	DG2	Encoded headshot
	Additional features	DG3	Encoded fingerprint
		DG4	Encoded iris
Displayed identification features	DG5	Displayed portrait	
	DG6	Reserved for future use	
	DG7	Displayed signature or usual mark	
Encoded security features	DG8	Data features	
	DG9	Structure features	
	DG10	Substance features	
	DG11	Additional personal details	
	DG12	Additional document details	
	DG13	Optional details	
	DG14	Reserved for future use	
	DG15	Active Authentication public key info	
	DG16	Persons to notify	

Figure 2: Logical Data Structure of e-passport chip

The Security Data Element (SOD) stores the hash of data groups DG1 - DG 15 which must be signed by the issuing country.

Hiding the value A in e-passport photo using steganography mechanism

The process of hiding the value A inside the photo should be embowered by using password for encoding and also for decoding at the airport. Using the password makes the steganography more secure; because it makes sure that the only validated and authorized reader can read the RFID data, and authenticate the RFID tag and guarantees that the tag was not cloned by an adversary and the headshot was not replaced.

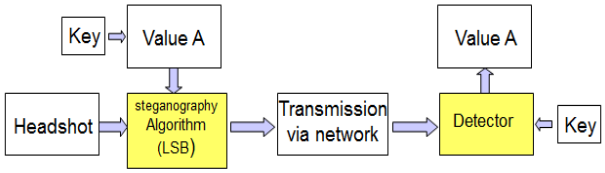

Figure 3: encoding and decoding in the steganography process

5.STEGANOGRAPHY PROCESS

In this step, and as we mentioned before, we decided to use the Open Puff tool. references [6], [7]

Figure 4: Open Puss steganography tool

By clicking on Hide button, the screen for hiding the value (A) will appear

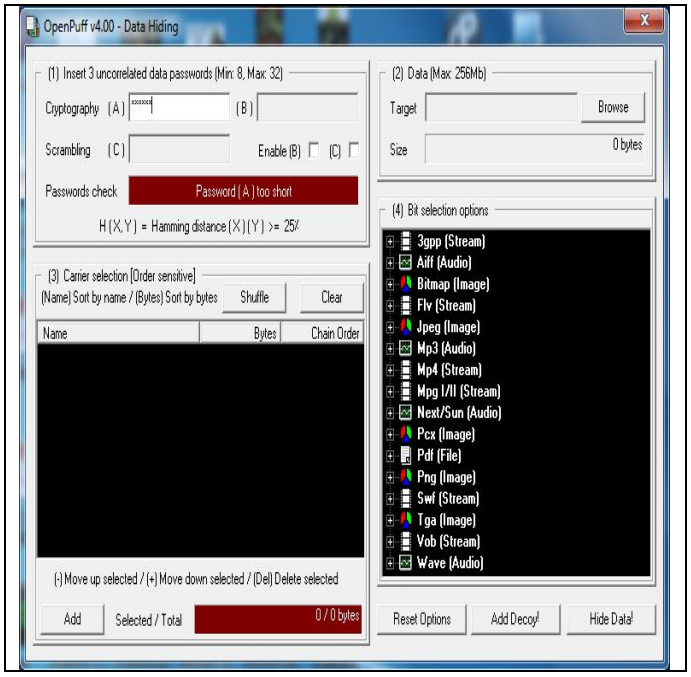

Figure 5: Main screen for hiding data in the headshot

In step one of this screen, the password (r) will be used in the cryptography (A) field, it will be 629441535 as shown in Figure 3.

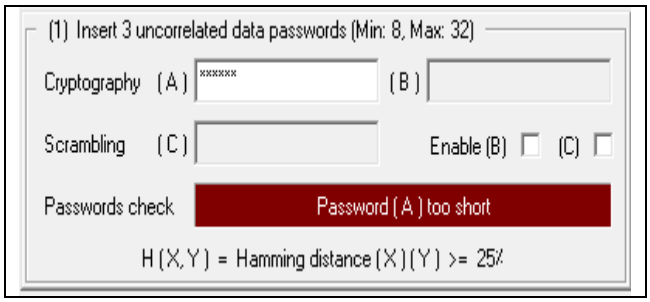

Figure 6 : Step one of steganography process (enter the password (r))

In step two, we have to choose the public key (A) value to be stored in the headshot.

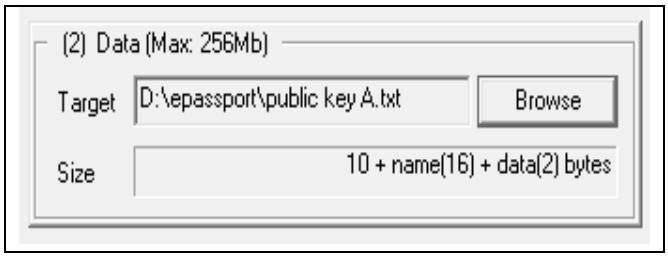

Figure 7: Step two of steganography process (selecting the identification data to be hide)

In step number three, we have to choose the headshot.

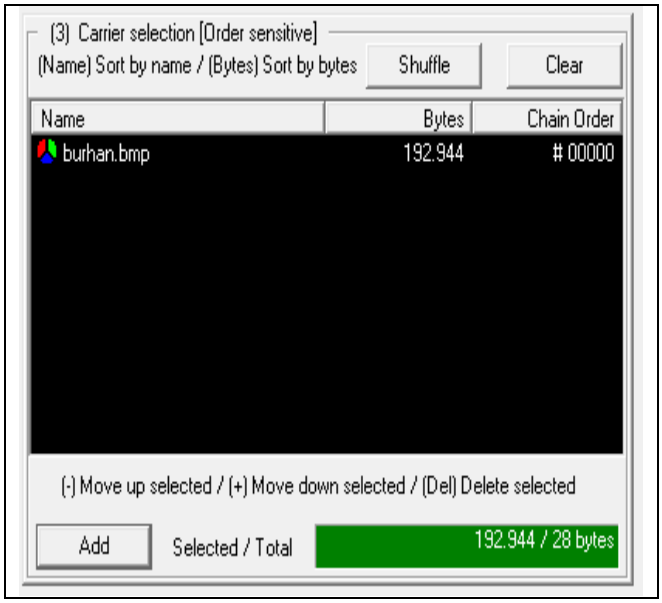

Figure 8 : Step three of steganography process (selecting the headshot)

Finally, we have to select the bit selection type and press Hide Data button. We decided to select the Bitmap type. [8]

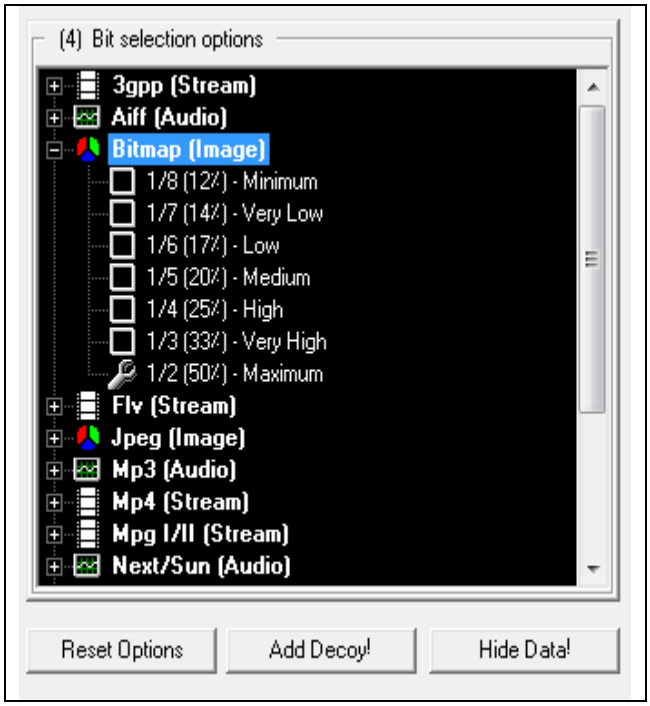

Figure *9*: Step four of steganography process (choosing the bit selection type)

Then we will get the following result, see Figure 9

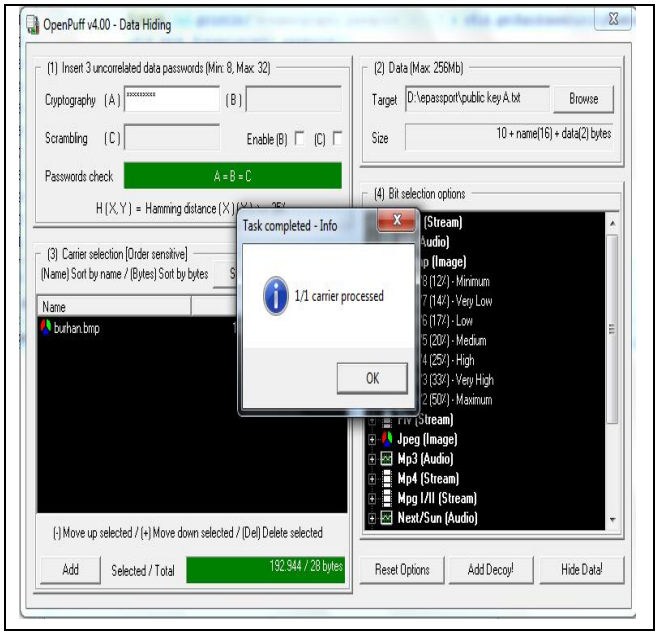

Figure 10: Information hiding success

6. CONCLUSION

The use of encrypted passport is a modern technology that is widely spread in the world and its goal is to maintain the confidentiality of data and speed in the itch of the passengers inside the airport and to dispense with traditional travel passports and the development of the use of modern technology (RFID). This technique has proven successful and has reduced the fraudulent use of passports. [10]

REFERENCES

1. Al-Hamami, Alaa. H&Al-Anni, Saad, A. (2005 A). A new approach for authentication technique, Journal of Computer Science, Vol. 1, No. 1, P. 103-106, NY, USA.
https://doi.org/10.3844/jcssp.2005.103.106

2. Al-Hamami, Alaa. H&Al-Anni, Saad, A. (2005 B). A Proposal for comprehensive Solution to the problems of Passport's Authentication. Information Technology Journal, 4(2): P. 146-150, Asian Network for Scientific Information.
https://doi.org/10.3923/itj.2005.146.150

3. Benssalah, M., Djeddou, M., &Drouiche, K. (2012). RFID authentication protocols based on ECC encryption schemes. Paper presented at the RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference .
https://doi.org/10.1109/RFID-TA.2012.6404575

4. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. Paper presented at the Advances in cryptology.
https://doi.org/10.1007/3-540-39568-7_2

5. Hariri, M., Karimi, R., & Nosrati, M. (2011).An introduction to steganography methods. World Applied Programming, 1(3), 191-195.
http://www.icao.int/about-icao/Pages/default.aspx, accessed on January 2016

6. Juels, A., Molnar, D., & Wagner, D. (2005). Security and Privacy Issues in E-passports. Paper presented at the Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005.First International Conference.
https://doi.org/10.1109/SECURECOMM.2005.59

7. Kundra, S., Dureja, A., &Bhatnagar, R. (2014). The study of recent technologies used in E-passport system. Paper presented at the Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS), 2014 IEEE.
https://doi.org/10.1109/GHTC-SAS.2014.6967573

8. Peeters, R., Hermans, J., &Mennink, B. (2014). Speedup for European E-Passport authentication. Paper presented at the Biometrics Special Interest Group (BIOSIG), 2014

9. Saeed, M. Q., Masood, A., & Kausar, F. (2009). Securing E-Passport system: a proposed anti-cloning and anti-skimming protocol. Paper presented at the Software, Telecommunications & Computer Networks, 2009. SoftCOM 2009.17th International Conference

10. Wang, Z., Yang, L., Cheng, Y., & Ding, Q. (2013). Two-stage verification based on watermarking for electronic passport. Paper presented at the Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference
https://doi.org/10.1109/IIH-MSP.2013.19