Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 6 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhancing Security to Protect E-Passport against Photo Forgery

By Prof. Dr. Alaa Hussein Al - Hamami & Muna Amin Alabed Alhafez
Amman Arab University Amman

Abstract- Electronic Passport (e-passport) is one of the results of the electronic revolution in the World; since the passport is the document of the person in terms of identity and nationality and is the property of the country. One of the most important challenges is to protect this document from forgery. The common forgery for the passport is replacing its holder photo. The proposed system concentrates on the security part of the e-passport. It consists of two parts; the first part is hiding of the security code by using steganography and storing the same code in the RFID tag by the issuing country of the e-passport. The other part will be operated at the control point of the destination country to make sure of the e-passport validity by checking the hidden code using NFC and verify it with the one in the RFID tag. If the two values are equal, then the system will compute a key using Diffie-Hellman Key Exchange. This key will be used to read the secret information in the tag.

Keywords: *steganography, nearest field communication, radio frequency identification, and epassport.*

GJCST-E Classification : *D.4.6, H.2.7, K.4.4, I.4.8,*

ENHANCINGSECURITYTOPROTECTE-PASSPORTAGAINSPHOTOFORGERY

Strictly as per the compliance and regulations of:

Enhancing Security to Protect E-Passport against Photo Forgery

Prof. Dr. Alaa Hussein Al - Hamami [α] & Muna Amin Alabed Alhafez [σ]

Abstract- Electronic Passport (e-passport) is one of the results of the electronic revolution in the World; since the passport is the document of the person in terms of identity and nationality and is the property of the country. One of the most important challenges is to protect this document from forgery. The common forgery for the passport is replacing its holder photo. The proposed system concentrates on the security part of the e-passport. It consists of two parts; the first part is hiding of the security code by using steganography and storing the same code in the RFID tag by the issuing country of the e-passport. The other part will be operated at the control point of the destination country to make sure of the e-passport validity by checking the hidden code using NFC and verify it with the one in the RFID tag. If the two values are equal, then the system will compute a key using Diffie-Hellman Key Exchange. This key will be used to read the secret information in the tag.

Keywords: steganography, nearest field communication, radio frequency identification, and epassport.

I. Introduction

Speed, time and security components have become the most important success factors in any developed system and at the same time number of travellers around the world is increasing continuously. Since the airports are the main ports of the States, the movement of passengers through the gates in order to verify the identity of travellers requiring high accuracy to make sure that no forgery and no impersonate the passport holder.

E-passport technology (Kundra & et al, 2014) has become an important substitution of the traditional passports in the access controls intended for travel around the world since the authentication of the passenger using it becomes faster, more secure, and more preserving of the privacy of passengers (Juels& et al, 2005). In addition, the forgery processes of the traditional passports are not available in the e-Passports.

Some of these challenges are cloning, and spoofing of RFID. Other challenges are the impersonation and eavesdropping attacks on the reader devices. The communication between the Tag and inspection system are controlled by the cryptography techniques to overcome these types of attacks.

II. Literature Reviews

An Anti-Cloning and Anti-Skimming Protocol (ACASP) (Saeed & et al, 2009) has been proposed to counter the vulnerabilities of Basic Access Control and Active Authentication with respect to RFID chip skimming, and cloning. It takes advantage of public-private key pair stored in the chip and the optional data storage capacity in Machine Readable Zone (MRZ) of the passport. An advantage of ACASP is that it can be implemented without any modifications in the hardware of the reader and the Tag. And there is no need to make changes in the Logical Data Structure (LDS) of the RFID chip.

(Benssalah et al., 2012) proposed an authentication algorithm based on elliptic curves ElGamal encryption (ElGamal, 1985). The main benefits of this protocol are that fights against four types of security threats; Simple power analysis and timing analysis, Passive attacks, Man-in-the middle, and Replay attack.

Al-Hamami (Al-Hamami & Al-Anni, 2005A) suggested some new authentication method by using a firm authentication method by extracting some features for the original name of the holder with the passport number and digest them in a form, by applying some techniques, that can be hidden in the passport's photo.

A method for e-passport verification depending on watermarking (Wang & et al, 2013) has been proposed which is composed of multimodal biometric feature and the parity check code of that 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.

The main idea in (Peeters et al., 2014) is to use mutual authentication protocol pattern instead of bootstrap from the low entropy value in MRZ. In order to protect the e-passport holder's privacy, terminal authentication takes place first, and then the e-passport authentication which uses Sigma-I or IBIHOP+.

(Al-Hamami & Al-Anni, 2005B) suggested a protocol to solve the problem of e-passport verification and authentication. (Al-Hamami & Al-Anni, 2005) suggested to use an invisible watermark to be hidden in the passport headshot to solve the problem of the passport verification, and they also suggested to use Diffie–Hellman to solve the problem of mutual

Author α: Faculty of Computer Sciences and Informatics, Amman Arab University Amman, Jordan.
Author σ: Faculty of Computer Sciences and Informatics Amman Arab University Amman, Jordan. e-mail: muna_hafiz83@yahoo.com

authentication between the e-passport and the inspection system.

III. Statement of Problem

The aim of this paper is to propose a method to enhance the security part of the epassport. Since the epassport is an international issue, we tried to use an international security method. This will be done by using an international prime number code assigned for each country, using a secret code for every country for privacy, and using unified methods Diffie-Hellman key exchange to create the exchanged key and steganography method to hide the secret code for privacy and authentication (Hariri & et al, 2011).

IV. The Proposed Solution

This paper aims to use a global method for greater security of epassport at airports check points. This depends on giving each country its own prime (what's wrong in this key? The main idea of Diffie-Hellman and ElGamal is to use a large prime number) number. This number should be a prime number or it will be converted to a prime number so that it can be used in the proposed framework of scrutiny and increased passport security.

In general, the proposed method is to use Diffie-Hellman key exchange Algorithm to share a private key between the Tag and the Inspection System (IS). The inspection system will use NFC technology in the reader devices which allows the reader to communicate with RFID Tag without needing to touch the devices together or go through multiple steps setting up a connection and allows the exchange of information between devices through short-range waves about four centimeters a maximum so as to prevent contact by mistake to other devices.

A calculated value will be hidden in the passport photo by using steganography method. When, the passport holder arrives the access control, and during the Diffie-Hellman key exchange process, the reader obtains a value from the Tag. Then, the reader scans the passport photo and compares the value hidden in the photo with the obtained value; if they were identical, the reader can make sure that the Tag is not cloned and it is authenticated.

After the mutual authentication process between the Tag and the reader, and after each of them calculates the secret key using Diffie-Hellman, the Tag sends the identification data (which are stored in plaintext format) of the passport holder using asymmetric encryption algorithm (ElGamal encryption system) to convert the plaintext into cipher-text and then the reader reconverts the cipher-text into plaintext. Figure 1 explains the proposed framework.

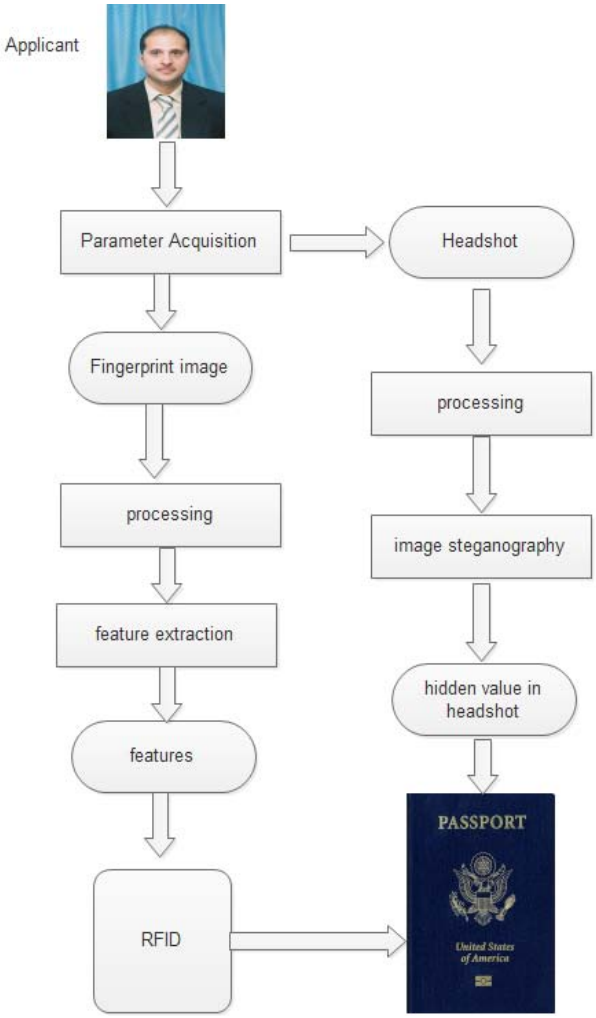

Figure 1 : A Phase one (e- passport generation)

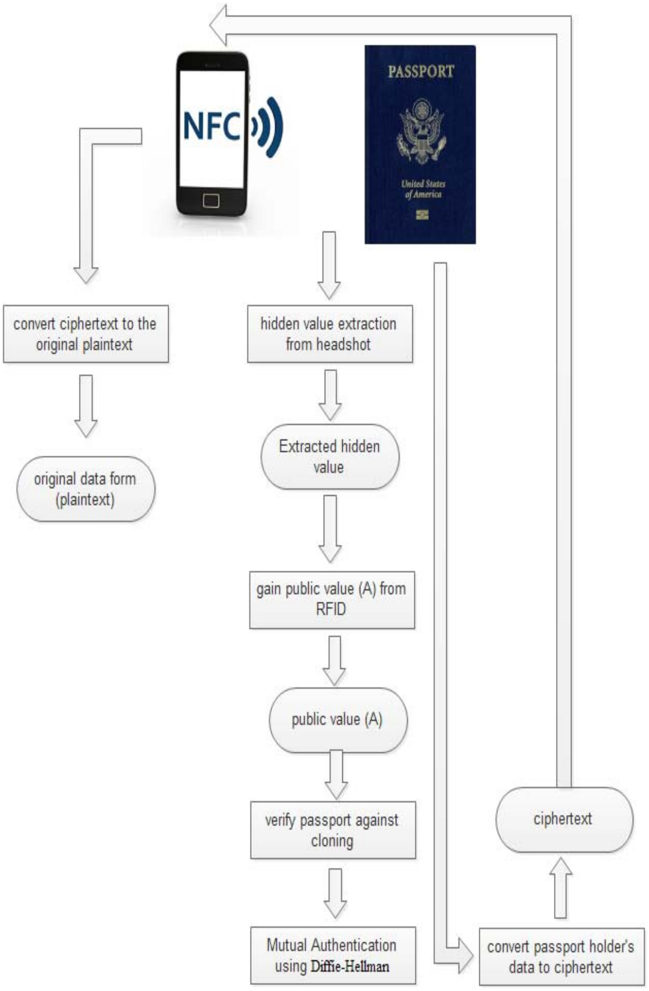
NFC
PASSPORT
United States of America
convert ciphertext to the original plaintext
original data form (plaintext)
hidden value extraction from headshot
Extracted hidden value
gain public value (A) from RFID
public value (A)
verify passport against cloning
Mutual Authentication using Diffie-Hellman
ciphertext
convert passport holder's data to ciphertext

Figure 1 : B phase two (e-passport (verification and mutual authentication)

The proposed method consists of two phases; e-passport generation phase, represented in Figure 1.A, and e-passport verification and mutual authentication, represented in Figure 1.B.

a) Phase one is composed of three algorithms. Each one is responsible for one type of processes. These algorithms have to be performed by the originator country.

V. Algorithm One (Parameter Acquisition)

a) Read the applicant identification data.
b) Validate entries.
c) Store the entries in the e-passport chip.

VI. Algorithm Three (Text Steganography)

a) Using Diffie-Hellman algorithm, generate the public key (A).
b) Generate a random number (r) and store it in the Tag.
c) Scan the headshot of the applicant.
d) Hide the generated public key (A) in the headshot using Least Significant Bit encoding (LSB) steganography technique. Use the random number (r) as a password for the steganography process.
e) Phase two is composed of four algorithms. These algorithms have to be performed by the access control country.

VII. Algorithm One (Mutual Authentication)

Continue the Diffie-Hellman algorithm, which has been started in step (a) of algorithm three of phase one, in order for the chip and the reader to obtain a shared secrete key (K).

VIII. Algorithm Two (E-Passport Chip Verification)

a) Using ElGamal algorithm, obtain the random number (r).
b) Extract the hidden value from the headshot, and use the value (r) as the password for that.

Obtain the public key value (A) from the chip during Diffie-Hellman algorithm.

Compare the extracted value in step (b) with obtained value in step (c); if they were identical, so the chip is the original one and not cloned. Otherwise, the chip is cloned and the e-passport holder must not pass the access control, and there is no need to perform the algorithms two, three, and four.

Identification and Biometric Data Conversion to Cipher (Using ElGamal Encryption)

Use ElGamal decryption algorithm to convert the identification and Biometric, which were stored in the chip, into cipher text. Send the cipher text to the reader device.

X. Decryption of the Cipher Text (using Elgamal Decryption)

a) Receive the cipher text from the e-passport chip.
b) Use ElGamal encryption algorithm to convert back the cipher text to its original plaintext value.

Example for non-forged passport

Suppose that the value of the automatically generated prime number (p) is 23, the value of the modular number (g) is 5, the value of (p) and (g) are common between the RFID and the reader. Suppose also the secret number of the RFID (a) equals 6, and the secret number of the reader device (b) equals 15. Now these values have to be followed across the overall process.

At the passport side, it calculates the public key (A). (A = g^a mod p), (A) = 8. On the other hand, the reader device calculates its public key (B). (B = g^b mod p), (B) = 19.

After generating the public key (A), it will be hidden in the headshot of the passport bearer. When the passenger arrives to the access control of the destination country communication between the E-Passport and the inspection system carries on. The RFID sends the value A to the reader, and the reader sends the value B to the RFID. Based on Diffie-Hellman algorithm, when the E-Passport calculates its secrete key K_{RFID} = B^a mod p (K_{RFID} = 19^6 mod 23=2).and the reader calculates its secrete key K_{Raeder} = A^b mod p (K_{Raeder} = 8^{15} mod 23=2), and after checking the equality state of them, if they were identical, a message saying that Mutual authentication passed will appeared. Now the system will Extract the hidden value (A) from the headshot, and compare it with obtained value from the RFID chip; if they were identical, so the chip is the original one and not cloned.

After the passport authentication and verification, it has to encrypt the identification data using ElGamal encryption algorithm in order to send them to the reader device. The final step happens in the access control country in which the reader needs to decrypt the encrypted identification data sent to it from the E-Passport.

X. Conclusion

The use of e-Passport is technology increasingly used in different countries overall the world. It aims to fight against the forgery activities of the traditional passports. This paper proposed to develop a security technique to be used with the e-passport in the airports to read its holder information by using Radio Frequency technique (RFID).

The proposed security method proved that it works correctly in identifying the forgery if it is existed. The authentication of the validity of the epassportis confirmed by the double checking for the hidden code. The proposed security method kept the privacy of each country in dealing with its secret code.

References Références Referencias

1. A. Al-Hamami, S, Al-Anni (2005 A). A new approach for authentication technique, Journal of Computer Science, Vol. 1, No. 1, P. 103-106, NY, USA.
2. A. Al-Hamami, S, Al-Anni (2005 B). A Proposal for comprehensive Solution to the problems of Passport's Authentication. Information Techno logy Journal, 4(2): P. 146-150, Asian Network for Scientific Information.
3. M. Benssalah, M. Djeddou, K. Drouiche (2012). RFID authentication protocols based on ECC encryption schemes. Paper presented at the RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on.
4. T. ElGamal (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. Paper presented at the Advances in cryptology.
5. M. Hariri, R. Karimi, M.Nosrati (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. A. Juels, D. Molnar, D. Wagner (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 on.
7. S. Kundra, A. Dureja, R .Bhatnagar, (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.
8. R.Peeters, J.Hermans, B.Mennink (2014). Speedup for European E-Passport authentic-cation. Paper presented at the Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the.
9. M. Saeed, A. Masood, F. Kausar, (2009). Securing E-Passport system: a proposed anti-cloning and
10. anti-skimming protocol. Paper presented at the Software, Telecommunications & Computer Networks, 2009. SoftCOM 2009.17th International Conference on.
11. Z. Wang, , L. Yang, Y. Cheng, Q. Ding, (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 on.