http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 4 (2): 146-150, 2005
ISSN 1812-5638

A Proposal for Comprehensive Solution to the Problems of Passport's Authentication

Alaa H. Al-Hamami and Saad A. Al-Anni
Faculty of Information Technology, Al-Ahliyya Amman University,
P.O. Box 975, Swieleh, Amman, Jordan

Abstract: This research introduces a comprehensive solution for the passport authentication problem. It proposed to use an invisible watermark to be hidden in the passport's photo which is contain a digest value to be checked for the authentication. The construction of this watermark uses the idea of making a physical connection between the passenger characteristics (name) and passport's number and photo.The proposed system makes it easy to authenticate the passport in the originator country which issues the passport. The problem is how to authenticate the passport by another country (not the originator). Diffie-Hellman exchange key has been used by the proposed system to exchange a secret key for making the authentication process correct and simple. Each country will use its own secret key for developing its invisible watermark. The watermark retrieving process by any country will depend on its secret key and the exchanged of a secret key.

Key words: Watermark, secret key, authentication, Diffie-Hellman exchange key, passport authentication

INTRODUCTION

Steganography is the art and science of hiding the fact that communication is taking place. Steganographic systems can hide messages inside of images or other digital objects. To a casual observer inspecting these images, the messages are invisible[1].

The term "Information hiding" relates to both watermarking and steganography. There are three different aspects to aninformation hiding system that content with one another: capacity, security and robustness. Capacity refers to the amount of information that can be hidden, security to the inability of an eavesdropper to detect hidden information and robustness to the amount of modification the cover medium can withstand before the hidden information is destroyed.

In general, the primary goal of a watermarking system is to achieve a high level of robustness. That means it should be impossible to remove a watermark without degrading the quality of the data object[2].

The security of a classical steganographic system relies on the secrecy of the encoding system. Once the encoding system is known, the steganographic system is defeated. However, modern steganography should be detectable only if secret information is known, namely, a secret key[3].

When the watermark scheme is used between two parties, it is a simple task to preserve the properties of the information hiding technique. The problem arises when there are many parties sharing the same secret and to use the watermark in a proper manner. To solve the problem of distributing and managing watermark, it is possible to use a public key but this will direct the scheme to the cryptography technique.

This research suggests the key exchange method which proposed by Diffie-Hellmen to transfer the secret key and to apply the authentication method[5].

A firm authentication method was proposed by Al-Hamami and Al-Anni[4] and that by extracting some features for the original name of the holder with passport number and digest them in a form, by applying some technique, that can be hidden in the passport's photo as a watermark.

After using this technique, it is very simple to use the computer in scanning and verifying, at check point, that the passport's photo has been not replaced and that by comparing the invisible watermark with the digest name of the holder and passport's number.

The proposed method is secure and effective, but it works beutiffly for one National State and could be used between more than two states by transmitting copy of the passport between them for authentication. The copy of the passport must be sent to the originator country for this authentication.

This method of authentication is not suitable in these days where time is very important in addition it is vulnerable to the threats of integrity and security during

Corresponding Author: Dr. Alaa Hussain Al-Hamami, Professor, Faculty of Information Technology, Al-Ahliyya Amman University, P.O. Box 975, Swieleh, Amman, Jordan
Tel: 079 6789621 E-mail: alaa_hammami@yahoo.com

the transmitting process. It is preferable to do the authentication at once at the control point for the different types (origins) of the passport's originators.

This new method of authentication could be done but we must preserve the secret key of each country (originator) and use a shared method for issuing and authenticating passport by keeping the privacy of each country preserved.

This research tries to practice these ideas by suggesting a new method and technique for using watermark.

The proposed system: The proposed system includes a new method of constructing the invisible watermark, a new implementation of Diffie – Hellman key exchange and a new technique for applying authentication.

General overview: There are two major parts in the proposed system. The first one is the constructing of the watermark by using the passport's characteristics which are,the holder's name and the passport's number. Then hide the invisible watermark in passport's photo. The second part is about the passport's authentication and this could be done by using Diffie–Hellman key exchange algorithm.

The outline of the designed system is shown in Fig. 1.

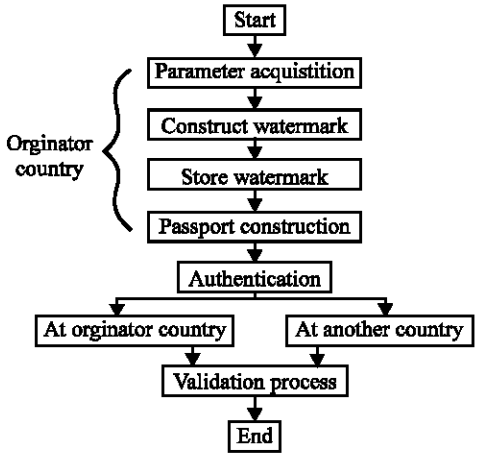
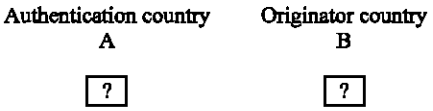


Fig. 1: The outline of the designed system

The proposed system consists of four algorithms. Each one is responsible for one type of process. All the required validation processes will be taken in consideration by the proposed method.

To show the algorithm processes consider the following figure:



where, A = Control point in the other countries
B = country of Passport's issue

There are two general algorithms that can be used by the originator and the authenticator country.

Algorithm one (Parameter Acquisition):

1. Read first, second, third and family name.
2. Read Passport Number.
3. Validate entries.
4. Assign each letter a number according to a table.
5. Keep each name's numbers.

Algorithm two (Convert):

1. Get the summation of the first name by adding the code of each character multiplied by the 2nd name character on a sequence manner.
   E.g, 1stname[1]*2ndname[1]+1stname[2]*2ndname [2]+…..
2. Consider the result as "row".
3. Repeat step (1) for the third name and family name.
4. Add the 3rd name, family name and the passport number and the result will be "column".

Hiding process: This process will be developed in the originator country, in this case is B and we will be used Diffie-Hellman exchange key in a different way. We will explain the new implementation of Diffie-Hellman method.

$$Y_B = \alpha^{XB} \bmod q$$

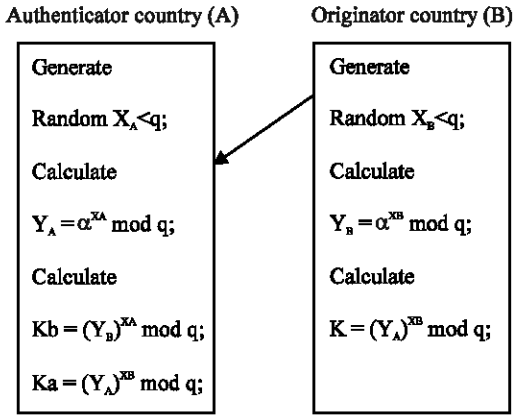
Where:

X_B = secret key for the originator country.
Y_B = A number which is publicly known.
α = A primitive root for q.
q = A prime number for the originator country.
$Y_A = \alpha^{XA} \bmod q$ used for the authenticator country.

To exchange the secret key (k):

$K = (Y_B)^{XA} \bmod q$
$K = (Y_A)^{XB} \bmod q$

This could be explained better by figure



Diffie-Hellman key exchange.

The third algorithm (Hide) will be used as follows:

Algorithm three (Hide):

1. Use algorithm one.
2. Use algorithm two.
3. Get Y_B value by using $Y_B = \alpha^{XB} \bmod q$.
4. Value = Y_B.
5. Read the value of the pixel on location (row, column) from the original Image.
6. Find the largest value of RGB color for that pixel and assign it to "large".
7. Divide "value" on "large" to get number of pixels.
8. Calculate the modulo of "value" over "large" and assign it to "color".
9. Calculate Ncolumn so that equals to "column" + "No.of pixels" + 1.
10. Get the pixel value in location (row, Ncolumn).
11. Replace the largest value of RGB for that pixel with "color".
12. Restore the pixel at the same location.

Figure 2 will explain the algorithm.

Authentication process: This process can be used by the originator country or by another country. Algorithm Four (Authenticate) can be used in this process. This algorithm consists of two parts. Part (A) authenticates the passport at the Control Point of the originator country and part (B) does the authentication at another country, other than the originator.

Algorithm four-A:

1. Calculate the new value of Y'_B.
   $Y'_B = \alpha^{XB} \bmod q$
2. Compare value which is equal to Y_B with the new value of Y'_B.

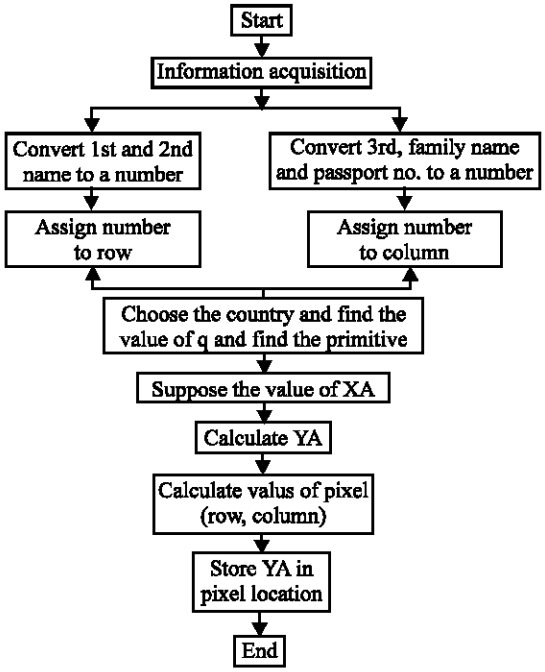


Fig. 2: The hiding algorithm

3. If they are equal, then the passport is O.K.
4. Exit.

Algorithm four-B:

1. Calculate X_B by using the equation $Y_B = \alpha^{XB} \bmod q$
2. Calculate k at the authenticator country $K_A = (X_A)^{XB} \bmod q$
3. Calculate k at the originator country $K_B=(Y_B)^{XA} \bmod q$
4. Compare K_A with K_B if they are equal then the passport is O.K.
5. Exit.

Figure 3 will give the details for this algorithm.

The implementation: To test the proposed system and to evaluate it we will take the following example:

Watermark construction: By using Algorithms (1, 2 and 3) to get passport's information and construct and hide the watermark. Figure 4 shows the construction and hiding process for the watermark. Also, make the process of changing the RGB value, to make the color matching perfect, is shown in the Fig. 5. The hidden value (Y_b) is equal to 2.

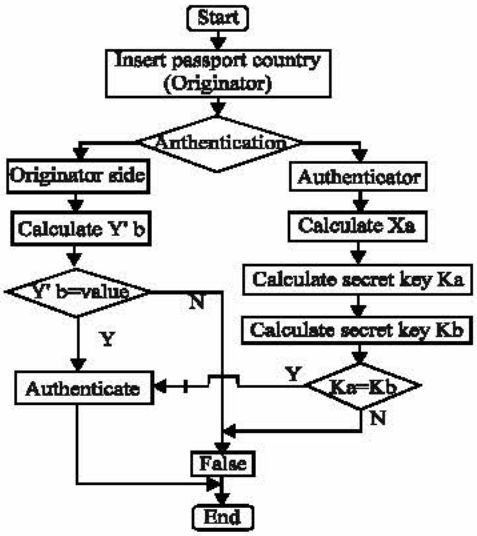


Fig. 3: The Authentication process

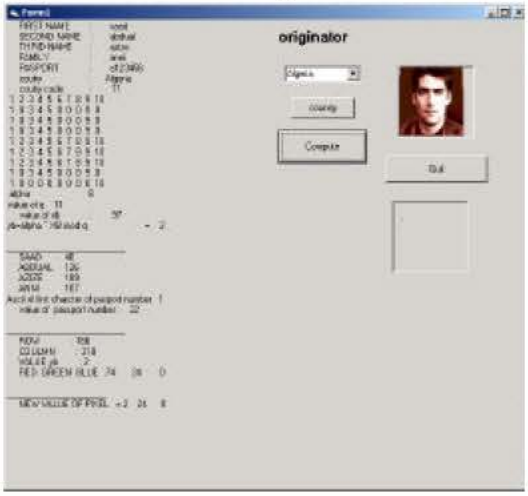


Fig. 4: Construct and hiding watermark

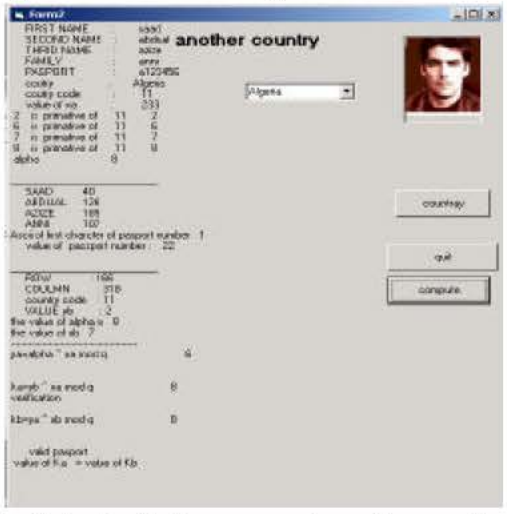


Fig. 5: Authentication process be another country

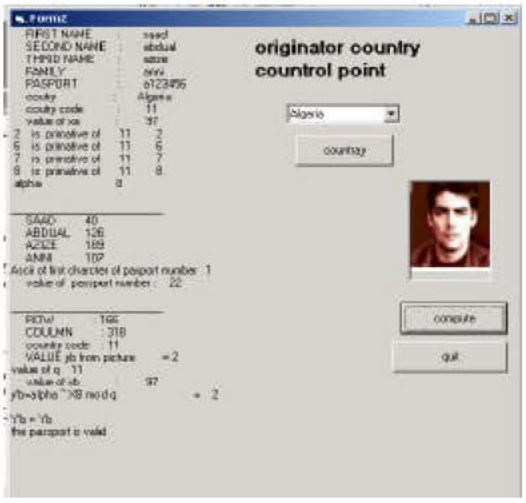


Fig. 6: Authentication process by the originator country

Authentication process by another country: The authentication process (by another country) is shown in Fig. 6. The value of Y_b is calculated which is equal to 2. The exchanged key is calculated (ka) and it must be equal to (k_b) validate the passport. In the example the value of Ka and K_b is equal to 8.

Authentication process by the originator country: Figure 6 shows the calculation of the hidden value which is equal to 2. Then the Y_b of the originator must be calculated. If the value of Y_b equals to the hidden value then the passport is valid.

DISCUSSION

The proposed system has suggested anew method of authentication. The suggested technique of the invisible watermark has connected physically the passport's characteristics with photo. The proposed invisible watermark has satisfied the invisibility, undetectibility and security requirements.

The problem of passport authentication has been solved by the proposed system and proves it's practically working correctly and simply by using different experiments assuming different countries applying this authentication.

The Diffie-Hellman method has been used in a convenient way to do the authentication and to keep the privacy of the secret key of each country. The parameters of the Diffie-Hellman algorithm have been chosen perfectly such as (q) which is mean the prime number of the originator country which is publicly known.

REFERENCES

1. Johnson, F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. IEEE Computer Magazine, 31: 26-34.
2. Provos, N. and P. Honeyman, 2001. Detecting steganography content in the internet. Center for Information Technology Integration, University of Michigan, USA.
3. Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House.
4. Wu, M. and B. Liu, 1998. Watermarking for image authentication, IEEE International Conference on Image processing (ICIP '98), Chigaco, USA
5. Al-Hamami, A. and S. Al-Ani, 2004. A new approach for authentication technique. J. Comp. Sci., No., 2004, NY, USA.