PASSPORT-G AUTHENTICATION METHOD BASED ON VAPOR-MARK BEARER'S PHOTO

Hiba Zuhair Zeydan
Al-Nahrain University.

Abstract

This research proposes a simple method for issuer's authenticity verification of the Iraqi new passport form that is publicly named as (passport-G). This authentication method is based on a digital watermarking technology that is named as (vapor-mark), and it involves two phases: the embedding phase and the authentication phase. During the embedding phase, a reference number is embedded as a watermark in a specific location entire the passport bearer's photo. This reference number and its embedding location are derived and encoded from the issuing authentication data such as: the date of issue, the date of expiration, and the passport number. During the authentication phase, the passport is digitally scanned and the embedded reference number is extracted from the bearer's photo. Then, a verification algorithm is applied to compare the extracted reference number with that number derived from the printed issuing authentication data. If they are identical, then the passport-G is said to be authentic. Otherwise, an unauthorized passport-G reproduction or forgery is detected.

Keywords: Passport Authenticity, Reference Number, Vapor-mark, Embedding Phase, Authentication Phase.

I. Introduction

Within the recent two years, Iraqi travelers are carrying a new form of passports that are publicly named as (Passport-G). The passport-G is the new travel document set by the Iraqi national authority to provide a specific level of security that reduces forgery by using a combination of some specific properties such as: high resolution modulation patterns of document structure, material and physical properties of the document paper, and biometrics (images of the bearer's face and fingerprint) that are included into the bio-data page of the passport. Because these properties can be penetrated by unlawful people, some threats against the passport-G security still raise and that will force the national authority to invent more secure mechanisms. Such threats are explored on the security aspects of passport-G issuer (authenticity, non-transferability, and integrity) [1]. Generally, A passport document is not authentic if the legitimate issuer is not the origin of the passport. If some one else other than the legitimate bearer, presents the passport as his/her own, the non-transferability of the passport is affected. The passport loses its integrity if its content can be modified or manipulated by unauthorized or fraud individuals [1]. Specifically, in passport-G, the security criterion of (non-transferability) is achieved by including images of bearer's face and fingerprint to identify the lawful passport bearer, as well as some personal details like: the bearer's full name, place and date of birth. The security criterion of (integrity) is obtained in passport-G by stamping and clamping the passport, so subsequent modifications may be made difficulty but not impossibly.

But the security criterion of (authenticity) requires more than resistance to tampering and forgery attacks; and the passport-G should be irrefutable pedigree with a guarantee that no substitution or tampering has taken place. Without this guarantee passport-G can be forged enabling unauthorized, fraud, criminal persons, and terrorists to enter or travel from the country. Depending on the principle of document authenticity "*an authentic document is the document that can be verified to prove that its data come from the correct and legitimate issuing authority*" [2], this research aims to present a method that can be used to detect passport-G forgery by proving that the passport data as well as its container (the passport-G itself) are authentic.

This proposed method embeds (detects) an invisible watermark into the digitized

photograph of the passport's bearer. The used watermark is considered as a reference number formed by encoding the data of issuing authority that are required for passport authentication, and they are available on the printed bio-data page of the passport. The passport is said to be authentic, if the extracted watermark matches properly the issuing data. Else, an unauthorized passport production is detected. In such E-Governance and E-Commerce applications, the type of digital watermark that is used for authentication purpose is referred to as "**vapor mark**". The rest of this research is organized as follows: section II describes the digital watermarking technology, section III presents the proposed methodology.

Experimental results are involved in section IV; section V involves the conclusions and future suggestions.

II. Digital Watermarking Technology

A digital watermark is a piece of information that can be hidden directly into the media content, in such a way that it is imperceptible to a human observer, but easily detected by the computer [3]. Digital watermarks are widely used for in E-Commerce and E-Governance applications that include distribution of multimedia[1] content, services, security, document authentication, ownership identification and so on [3].

But, it must be noted that one of the basic requirements for digital watermarking applications are: (1) maintaining the quality of the original data not being distorted when a watermark is embedded into it. (2) The perceptual transparency: which means, the embedded watermark is undetectable perceptually. (3) The robustness: which ensures the embedded watermark will not be destroyed by third parties [3, 4].

For authentication, performance issues such as: robustness to attacks, capacity (how many bits can be hidden in the multimedia), and how transparent is the watermark under normal viewing conditions, are very important [4].

[1] i.e. video, image, audio and text.

The "digital *watermarking process*" uses a specific type of digital multimedia data (like images) as cover-data. It embeds and extract/detects a *"watermark"* in or out of the cover-data such that the usability of the multimedia data is not affected. For this purpose a *"cryptographic key"* is applied to encode and embed the watermark into the cover-data, resulting in "*watermarked data*" or "*stego data*". The *watermark* can be extracted from the *stego data* if the correct key is used. The embedding and extraction processes are illustrated in Fig. (1) [4].

This research assumes that the watermark process is applied for embedding the watermark in one-way function, and robust, i.e. it is for an unauthorized third party not possible to overwrite or delete this watermark without the *cryptographic key* information. The *cryptographic key* is unique and only known for the Passport-G legitimate production or issuing authority.

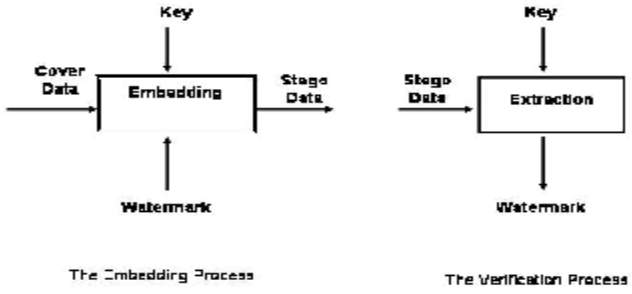

Fig.(1): The Embedding and Authentication Processes of Digital watermark..

III. The Proposed Methodology

The proposed watermarking methodology aims to enhance the security of the Passport-G by proving its authenticity and detecting the forgery. This method is based on two phases:

A. Embedding Phase.
B. Authentication Phase.

A. **Embedding Phase**: in this phase, firstly, the watermark and its location are derived from the authentication data of the legitimate issuer (that are printed on the bio-data page of the passport) such as:

- The issuing date.
- The expiry date.
- The passport number.

Secondly, the watermark is encoded using the cryptographic key information and then embedded in the digitized photo of the passport's bearer in the derived location. Note that the bearer's photo which is printed on passport-G, must have a white background. Therefore, the location of the embedded watermark is computed by using some parameters (such as: width and height) of the bearer's image. Fig.(2) illustrates this phase.

Algorithm (1): Encoding Information

1- Read as string of integers the following data respectively: date of issue, date of expiration, the passport number.
2- Read the width and height of the bearer's photo.
3- Compute IssDat using the following equation:

$$IssDat = \sum_{i=1}^{N} digit_i \times i \quad \text{.....(1)}$$

Where digit is each digit in the string of issue date, N is the length of the string, and I is the cryptographic key.

4- Compute ExpDat using the following equation:

$$ExpDat = \sum_{i=1}^{N} digit_i \times i \quad \text{.....(2)}$$

Where, digit is each digit in the string of expiration date, N is the length of the string, and I is the cryptographic key.

5- Compute the value of the character (G) that is involved in the passport number as follows [2]:

$$Val = ASCII(G) - 64 \quad \text{..... (3)}$$

6- Compute the code of passport number as follows:

$$PassNo = \sum_{k=1}^{M} digit_k \quad \text{..... (4)}$$

Where, digit is each digit in the sequence of passport number, and M is the length of that sequence.

7- Derive the embedded reference number as follows:

$$Refernce\text{-}Number = PassNo + Val \quad \text{..... (5)}$$

8- Read the parameters of the bearer's image: width and height.
9- Derive the watermark location using the following equations:

$$Row = width - IssDat \quad \text{..... (6)}$$

$$Column = height - ExpDat \quad \text{..... (7)}$$

10- The resultant values are: Reference - Number, Row and Column.

Algorithm (2): Embedding the Watermark in the bearer's photo

1. Read the value of the pixel on location (Row, Column).
2. Get the RGB color values for that pixel.
3. Exchange the red color value with the Refernce-Number[3].
4. Restore the pixel at the same location.

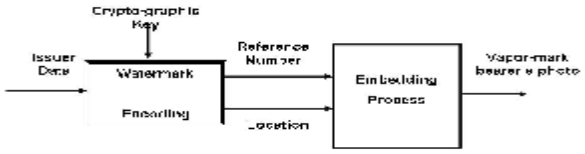

Fig.(2): The illustration of Embedding Phase.

B. Authentication Phase: the key ideas of this phase are: (i) formation of the Id-Watermark and Id-Location using the same issuing information, (ii) extraction of the embedded Reference-Number from the digitized bearer's photo, (iii) detecting whether the extracted Reference-Number and the Id-Watermark are identical in order to decide that the present passport-G is authentic or forfeit. Fig.(3) illustrates this phase.

Algorithm (5): (Authentication Phase)

1. Repeat algorithm (2) to produce the ID-Watermark and its ID-Location.
2. Read the value of the pixel on Row and Column.

[2] In this research, the passport character value (G) is constant for all passports. If this character will be changed to any other character in the future, this equation can be used to compute its value

[3] The green or blue color values can be used instead of red color value.

3. Get the RGB color values for that read pixel.
4. Compare the present red color value (the embedded Refernce-Number) with the (ID-Watermark). If they are identical, then the passport is authentic. Else, the passport is forged.

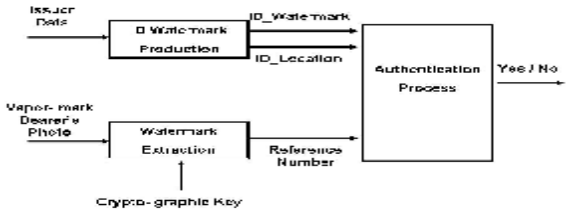

Fig. (3): The illustration of Authentication Phase.

IV. Experimental Results

The proposed methodology and its algorithms are applied into one example as described below.

Example: A passport-G with the issuer authentication data (date of issue: 2008-01-03, date of expiration: 2016-01-02, and passport number: G1702824).

Application: For this example, the reference number and its location are encoded and embedded using equations (1...7) during the embedding phase. The resultant reference number is (31) and its location is (row: 106, column: 169).

Then, the RGB color values of the pixel on the location (row, column) are retrieved from the original bearer's photo, and the red color value is replaced with the calculated reference number (either green or blue color values can be used, too). Here, this embedded reference number is considered as the watermark. Fig. (4) shows the application of this phase. During the authentication phase, the ID-Watermark and its ID-Location are derived and encoded from the issuer authentication data in the same way by using the width and height of the extracted bearer's photo and the equations (1…7). Then, the red color value (The original reference number) of pixel at location (row, column) on the bearer's photo is retrieved and compared with the calculated ID-Watermark. If they are identical (as shown in this example) the passport-G is said to be authentic. Otherwise, it is not. Fig. (5) illustrates the application of authentication phase

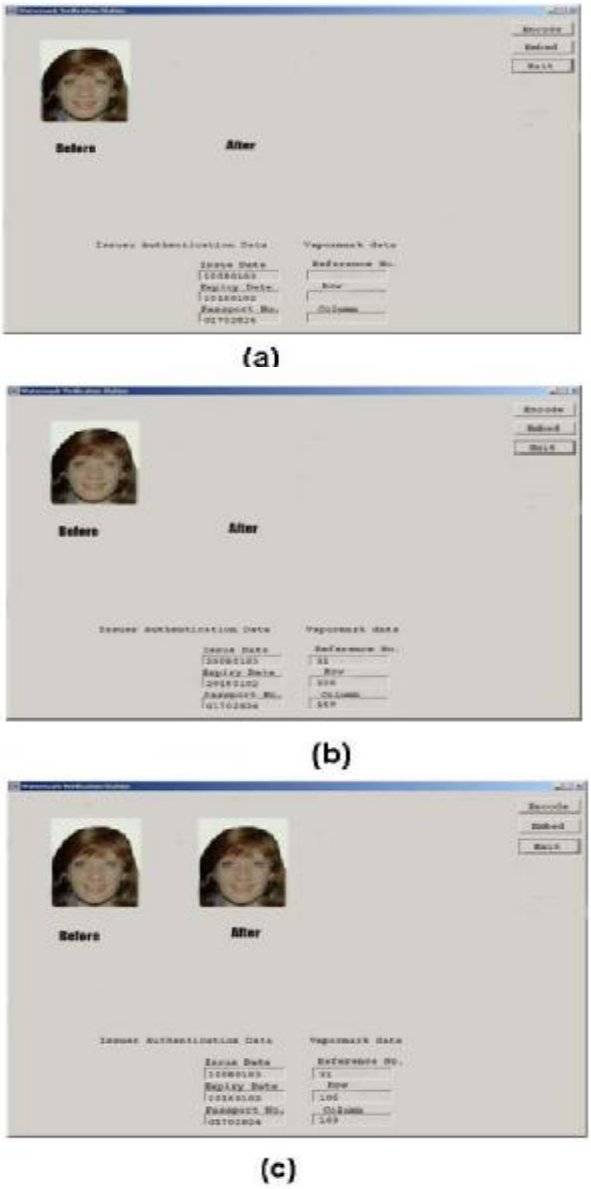

Fig. (4): The application of Embedding Phase, (a) and (b) application of algorithms 1 , (c) application of algorithm 2.

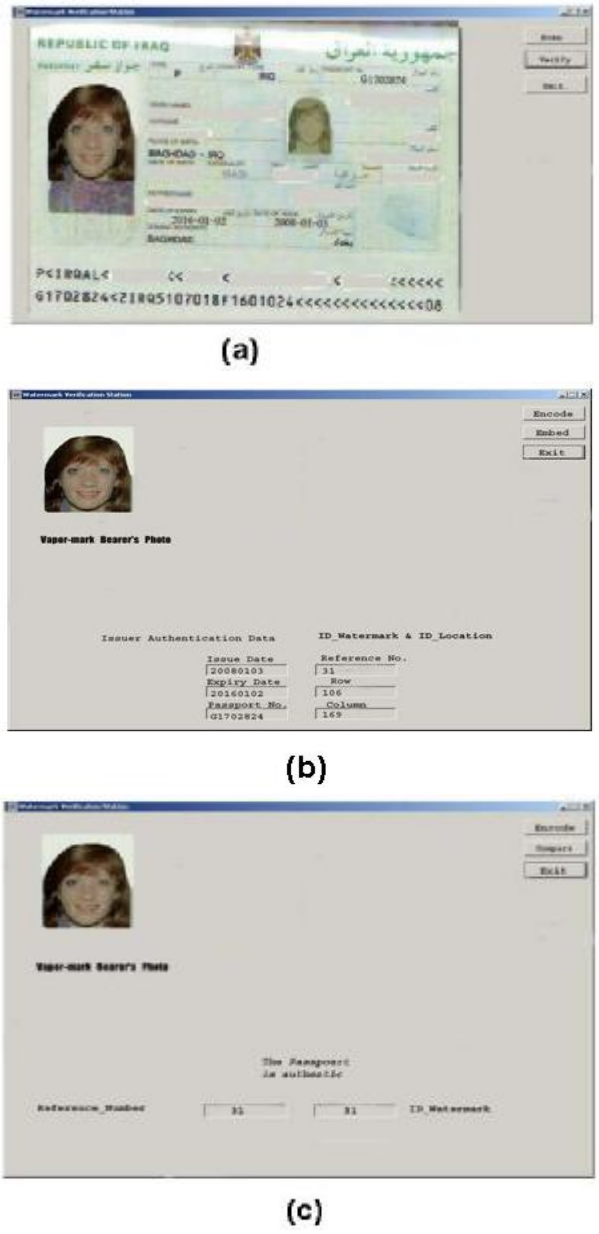

Fig.(5): The application of Authentication Phase:

(a) imaging the bio-data page of passport,

(b) computing ID-Watermark and its Location,

(c) comparison of the retrieved Reference Number and ID-Watermark.

V. Conclusions and Future Suggestions

The objective of this research is to enhance one of the passport-G' security aspects (authenticity of its issuer) by suggesting a simple method that verifying the passport's issuer authenticity using embedded vapor-mark on the bearer's photo. The vapor-mark is the digital watermarking technology that is used for authentication in E-Governance and E-Commerce applications such as the passport document production.

This proposed method preserves the requirements of watermarking such as invisibility and robustness, through:-

- Embedding the watermark on a small area (only one pixel) so that it is robust against image compression.
- Embedding the watermark at a random location over the entire bearer's digitized photo that makes the detection of the embedded watermark is time consuming.
- Using a unique cryptographic key that is only known for the legitimate passport issuing authority, makes this passport form more secure against modification of unlawful people those exploit the vulnerabilities of the passport.
- Encryption of the stored passport authentication data that the watermark and its location are derived from.
- The small capacity of the embedded watermark comparing to the size of bearer's image makes the watermark invisible.

Recently, this method can be used for one country (Iraq). In the future, it can be applied for passport's issuer authentication globally by suggesting two cryptographic keys one of them used for each country to embed the watermark and the other key used to extract the watermark by different countries.

References

[1] S.Schime, S. Kiltz, C. Vielhauer, "Security Analysis for Biometric Data in ID Documents", SPIE-IS&IT Electronic Imaging, vol. 5681, 2005.

[2] A. Juels, D. Molnar and D. Wagner, "Security and Privacy Issues in E-Passports", UC-Berkeley, Oct. 2005, e-mail1:ajuels@rsasecurity.com, e-mail2:dmolnar@eecs.berkeley.edu, e-mail3:daw@eecs.berkeley.edu.

[3] S.S. Sherekar, V. M. Thakare, S. Jain, "Role of Digital Watermark in E-Governance and E-Commerce", IJCSNS International Journal

of Computer Science and Network Security, vol. 8, no.1, Jan. 2008.
[4] I. J. Cox, M. L. Miller and J. A. Bloom, "Watermarking Applications and their Properties", Int. Conf. on Information Technology, Las Vegas, 2000.
[5] A. Herrigel, S. Voloshynovskiy, and Z. Hrytskiv, "An Optical/Digital Identification/Verification System Based on Digital Watermarking Technology", workshop on Information Hiding, Derd3en, Germany, Sept.29-Oct.1, 1999.

الخلاصـــة

يُقدم هذا البحث طريقة بسيطة لاثبات صحة اصدار الشكل الجديد لجواز السفر العراقي و المسمى (الجواز G) و تعتمد هذه الطريقة على تكنولوجيا العلامة الرقمية المسماة (vapor-mark). تتضمن هذه الطريقة مرحلتين: مرحلة بناء العلامة الرقمية و مرحلة التحقق منها.

في مرحلة البناء: يتم بناء عـــدد معين يسمى (عدد الاصدار) داخل صورة حامل الجواز، حيث يتم استخلاص هذا العدد من البيانات الثبوتيـــة الخاصة بالجهة الرسمية المخولة لاصدار الجواز.و تشمل هذه البيانات: تاريخ الاصدار، تاريخ النفاذ و رقم الجواز.

امـــا في مرحلة التحقق او الاثبات: فيتم اجراء مسح رقمي لجواز السفرG و استخلاص عـــدد الاصدار من صورة حاملـــه لتتم مقارنتها مـــع العدد الذي تم تكوينه من بيانات الاصدار المطبوعة في ورقة البيانات الثبوتية داخل الجواز G.

في حالة حصول تطابق بين العددين، فيمكن القول ان الجواز G أصلي او معتمـــد او صادر من الجهة المخولة، امـــــا في حالة كونهما مختلفين فهذا يعني ان الجواز غير صادر من جهة الاصدار الاصلية المخولة.