Vol 2 | Issue 1 | Pages 42-46

Archives of Information Science and Technology

Original Research

An Implementation of Electronic Passport Scheme Using Encrypted Security Along with Multiple Biometrics

*Israa Shaker Tawfic**

Ministry of Science and Tecghnology, Baghdad, Iraq

Abstract

Within the next year, travellers from dozens of nations may be carrying a new form of a passport. Electronic passports have known a wide and fast deployment all around the world since the International Civil Aviation Organization the world has adopted standards whereby passports can store biometric identifiers. The purpose of biometric passports is to prevent the illegal entry of traveller into a specific country and limit the use of counterfeit documents by more accurate identification of an individual.

The paper used the image of the e-Passport holder as a cover image to hide the fingerprint inside it within the operation of e-Passport design. The paper also provides a cryptographic security analysis of the e-passport using Arnold transform on fingerprint and add a privet key to encrypted data that are intended to provide improved security in protecting biometric information of the E-passport holder.

Our paper gives attention to the security features which are used to make the e-Passport safe and protect it from unauthorised access

Keywords

E-Passport, Fingerprint, Biometric, Arnold transform, Discrete wavelet transform (DWT)

Introduction

Secure and trusted travel documents are an essential part of international security, as they allow states and international institutions to identify the movement of undesired or dangerous persons. At a national level, both governmental and non-governmental institutions depend on travel documents in order to establish a person's identity as well (e.g. when opening a bank account). A secure travel document is, thus, a significant means against identity fraud [1].

Major initiatives by the government's aim to fuse Radio Frequency Identification (RFID) and biometric technologies in a new generation of identity cards [2].

Since August 2006 the 27 Member States of the European Union have been required to issue e-Passports that contain a digital facial image, and since June 2009 they have been obliged to issue second generation e-Passports that also include two fingerprints. The purpose of mandating the issuance of e-Passports has been to strengthen the link between the passport and the carrier of the passport, as well as to make it easier to verify the authenticity of the passport. Other European biometric initiatives include the Visa information System currently being rolled out, which is used for 3rd country nationals applying for a visa to the Schengen area [1].

An e-passport is, thus, composed of the passport booklet with its physically printed data and physical security (usually anti-forgery) measures, the electronic chip and the security mechanisms and data that are contained within the chip. For the purposes of this documented study, however, we will focus on the chip and the security mechanisms and information it contains.

An e-Passport is also known as a biometric passport contains an electronic chip. The chip holds the same information that is printed on the passport's data page: the holder's name, date of birth, and other biographic information. An e-Passport also contains a biometric identifier [3,4].

The goal of the e-Passport is to improve security by combating fraud. It may, in some cases, help speed up border crossings, but there is no guarantee that this will be the case [4]. The symbol of e-Passport is illustrated in Figure 1.

***Corresponding author:** Dr. Israa Shaker Tawfic, Ministry of Science and Tecghnology, Baghdad, Iraq

Accepted: March 16, 2019

Published online: March 18, 2019

Citation: Tawfic IS (2019) An Implementation of Electronic Passport Scheme Using Encrypted Security Along with Multiple Biometrics. Arch Inf Sci Tech 2(1):42-46

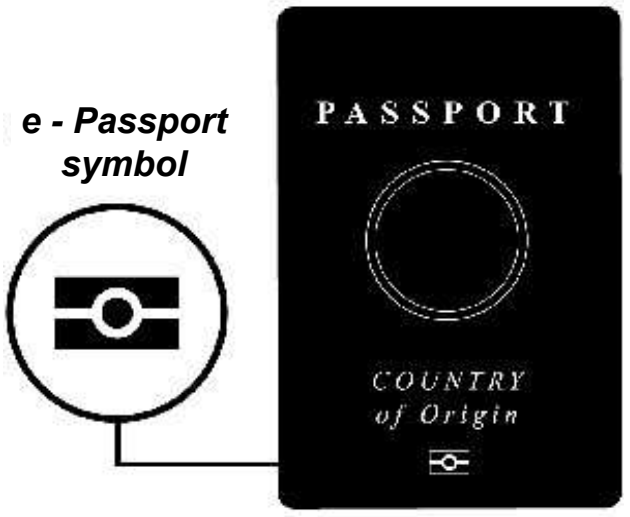

Figure 1: e-Passport symbol.

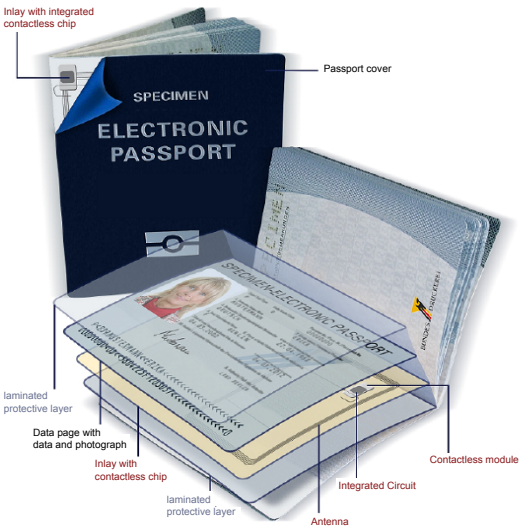

Figure 2: The layers of an electronic passport.

Figure 3: Images used for suggest method: a) The 4 test images used in suggest method; b) Logo used as a watermark; and c) Shape of watermark after three level of Arnold transform.

The main goal of upgrading passports to an electronic version is making it hard for criminals or anybody to counterfeit or illegally duplicate them. A practical way of doing so is through the use of Cryptographic for information install in the e-passport chip.

In this paper we proposed a new and simple method to hide the same biometric of the e-Passport holder (finger print), encrypted it then choosing one of the information that store in the chip (holder image) and hide it.

At the checkpoint, the image is acquired by reading the e-Passport chip and the encrypted compound biometric data is extracted from the acquired image and decrypted using the original key that was earlier stored in a secure external storage.

The biometric data is then authenticated with the biometric data of the passport's owner through invisible encryption. This biometric data can be considered as an invisible watermark image.

We try to use some transformation before embedded the biometric fingerprint. The transformation adopted here may be discrete cosine transform (DCT) or discrete wavelet transforms (DWT) [5,6].

Physical Aspects of e-Passport

E-passports are widely deployed in most of the developed countries that stores the biometric information on a tiny Radio Frequency Identification (RFID) chip. The stored information is used to authenticate the identity of an individual via a wireless interface to the reader [7].

Figure 2 shows a sample passport. On its bottom of the cover, we can see the standard logo for an electronic passport. The passport is made out of a special paper which should be secure and hard to imitate. This paper contains cotton and cellulose and there are no optical brighteners used. Furthermore, there is a watermark on all the pages in the passport [8]. There are also some chemical reagents in it to prevent manipulation by acids, petrol derivatives or whitening elements. If someone uses these substances to manipulate a passport, the chemical reagents will react and thereby return the passport in a useless state. Some small holographic stripes and some fibers which are only visible under UV light are embedded too.

The inks used to print passports have a restricted distribution and they are not available commercially. The ingredients of these inks are secret because they contribute a lot to the safety of the passport. They can also contain some chemical reagents for the same reason as the pages have and they react differently if they are placed under UV light [9].

Proposed Schemes

The suggested process to hide the watermark image (which is here is the fingerprint) is illustrated in Figure 3. First

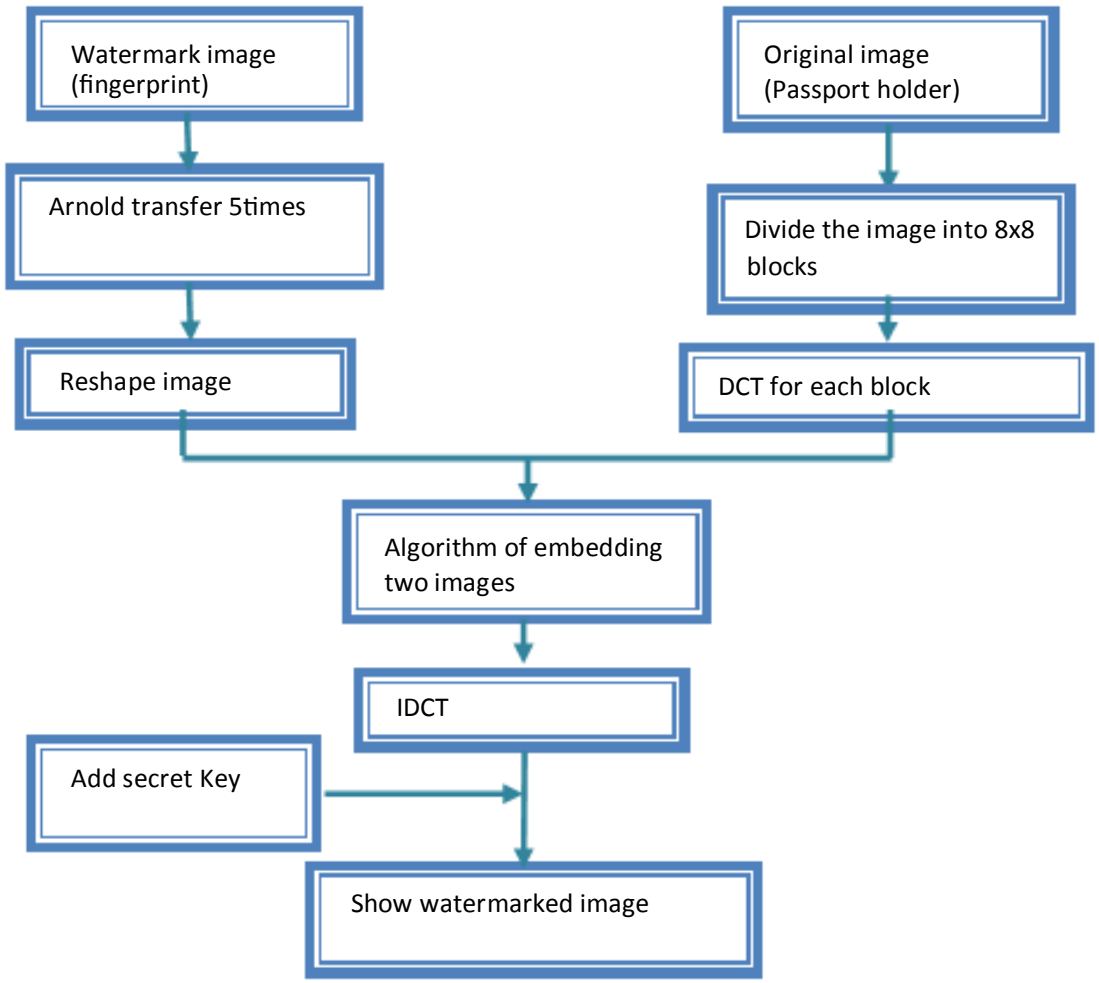

Figure 4: Main processes for embedding watermark using DCT.

step began by using multiple level Arnold transform into the watermark image and add privet key, then we choose the cover image (which is here is the passport holder). We used either DCT or DWT for the cover image, in addition, to considering the transformation operation is a simple encrypted method, and also we can consider it as an extra operation for information compression. After that, we embedded the watermarked information into the transformed image to get the watermarked image. Figure 4 illustrate the operation of adding watermark to cover image.

The algorithm can be described below:

i. Arnold algorithm

Step 1 save dimension of image (NxN)

Step 2 read each pixel of image (x, y)

Step 3 alters our x value by a taking the x value, adding y to it mod N

Step 4 y value changes by taking this x value adding to $2y \mod N$

Step 5 store (x', y')

ii. Algorithm for Embedded two images using DCT

Step 1 read cover image (I) (e-Passport holder image)

Step 2 read watermark image (fingerprint)

Step 3 divide the image into (8 × 8) blocks

Step 4 find DCT for each block of cover image (I)

Step 5 do Arnold transform 5 times for watermark image

Step 6 Compare the position I(3,3) with I(2,4)

If I (3,3) >= I(2,4) → I(5,2) = W(N)* watermark factor

Else

I (4,3) = W(N)* watermark factor

Step 7 use IDCT transformation for the block that has been embedded with watermarking information

Step 8 Repeat step 6 and 7 until all of the water marking information have been added to all blocks.

Step 9 add secret key

Experimental Result

In this section, we present numerical experiments that explain the effectiveness of using suggest a method of hiding biometric information into original extra biometric data by

Table 1: Results for DWT method.

Test image 512 × 512	PSNR	MSE	Correlation coefficient
Lena	48.1628	0.9643	1
Baboon	36.0360	1.8248	1
Pepper	38.6914	1.6422	1
Barbara	48.1061	1.0057	1

Table 2: Effect of number of Arnold transfer on Lena image.

No. of Arnold transfer	PSNR	MSE	Correlation coefficient
1	47.9183	1.0501	1
3	48.2889	0.9643	1
5	48.2671	0.9691	1
10	48.2757	0.9672	1

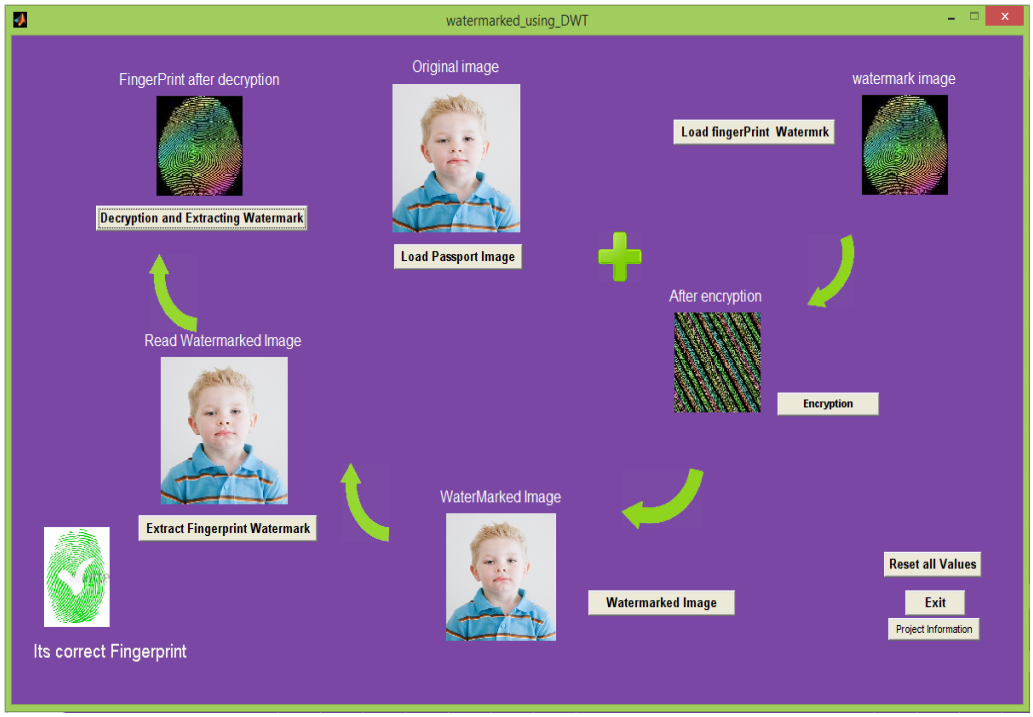

Figure 5: Interface for suggested application used for hiding fingerprint into another biometric.

using a different type of transformation. Different evaluation is used for measuring the performance of our new method. Such as The mean square error (MSE) which was used to measure performance of the reconstructed image and it's defined as

$$MSE = \frac{1}{M\ N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X\ (i,j)\ -\ X'\ (i,j))^2$$

also commonly employed measure to evaluate the imperceptibility of the watermarked image is the peak signal-to-noise ratio (PSNR) which can be calculated as.

$$PSNR = 10.\log_{10}\left(\frac{MAX_i^2}{MSE}\right)(dB)$$

Where is the maximum possible pixel value of the image.

Third factor used here is Normalized Correlation Coefficient (NCC), which is used to measure the performance of the blind or non-blind watermark extraction result for the extracted watermark W' and the original watermark W, NCC can be defined as:

$$NC\ (W,\ W') = \frac{\sum_{i=1}^{n}W\ (i).\ W'\ (i)}{\sqrt{\sum_{i=1}^{n}W\ (i)^2}.\sqrt{\sum_{i=1}^{n}W'\ (i)^2}}$$

Where (n × n) are the watermark dimensions. The magnitude range of NC varies between [-1 and 1], the unity value is given exact matching between the extracted watermark image and the original watermark image.

At the beginning, we used some slandered test images to evaluate the performance of our new suggest method to get comparable results.

In our experiments we used two approaches for designing engine of the embedded watermark into the image, the first one used DCT and the other one is the DWT, to make a compression between these two transformation type and choose the better method. For doing this we used four standard color images as a cover image with dimension 512 × 512 (Table 1), and one color logo as an invisible watermark with dimension 100 × 100, these image is shown in Figure 3 [10,11].

Also, we try to change the number of Arnold level to study its effect on the reconstructed image. Table 2 illustrate the results of changing Arnold level, we used DWT on Lena color image

The interface of our application program for the suggested method is illustrated in Figure 5. We used Matlab 7.6.0 to design and program all the step explain above. As it appears

from the figure the first step is read the image of the passport holder then the second biometric which is the fingerprint is used. To get rid of fraud and manipulation we used a number of Arnold transform on fingerprint image before we embed it on the original image, and a private key is added. After that, the watermarked image is store into the information list for the e-Passport chip. At the check point, the operation of decryption is started and the fingerprint is extracted and checks it with original one to distinguish the fake one.

Conclusions

The specific objectives of this paper is to identify best practices related to the issuance processes and to suggest a set of recommendation to redress security gaps in the issuance process.

The paper represents an attempt to acknowledge and account for the presence of e-passport scheme using face and fingerprint of the e-Passport holder to improved identification for more security and fraud prevention. The application of biometric in passports requires high accuracy rates; secure data storage, secure transfer of data and reliable generation of biometric data.

The ordinary passport data is not required to be encrypted, identity thief and terrorists can easily obtain the biometric information. A possible solution is to store a unique biometric date after encrypted and add a privet key to it. The key is then used to decrypt e-Passport data.

The inclusion of biometric identification information into machine readable passports will improve their robustness against identity theft if additional security measures are implemented in order to compensate for the limitations of the biometric technologies.

References

1. Rondo ONZ (2011) Operational and technical security of electronic passports. Frontex Agency, Warsaw.
2. Ari Juels, David Molnar, David Wagner (2011) Security and privacy issues in e-passports. UC-Berkeley.
3. (2016) e-Passports. The Department of Homeland Security, USA.
4. Government of Canada Site. How ePassports work.
5. Xiang-Gen Xia, Charles G Boncelet, Gonzalo R Arce (2010) A multiresolution watermark for digital images. Image Processing, Conference IEEE Xplore.
6. Syed Ali Khayam (2003) The discrete cosine transform (DCT): Theory and application. Michigan State University.
7. Hesam Kolahan, Tejendra Thapaliya (2011) Biometric passport: Security and privacy aspects of machine readable travel documents. Swiss Joint Master of Science in Computer Science.
8. Prashant Shende, Pranoti mude, Sanket Lichade (2015) Design and implementation of secure electronic passport system. International Journal of Innovative Research in Computer and Communication Engineering 3: 10885-10892.
9. Johannes Eifert, Lorenz Schwob (2012) Security and privacy of the biometric passport. Department of Informatics, Universität Freiburg.
10. Zhenjun Tang, Xianquan Zhang (2011) Secure image encryption without size limitation using arnold transform and random strategies. Journal of Multimedia.
11. Divya saxena (2011) Digital watermarking algorithm based on singular value decomposition and arnold transform. International Journal of Electronics and Computer Science Engineering 1: 22-27.