DOI: https://doi.org/10.33103/uot.ijccce.19.1.4

# Design and development of E-passport scheme using multi encryption biometric information

Dr. Israa Shaker Tawfic
*Provinces Affairs ,Ministry of Science and Tecghnology, Baghdad, Iraq.*
*isshakeralani@yahoo.com*

***Abstract***— *within the next year, travelers from difference world may be holding a new form of a passport.The electronic passport has been widespread in recent times, all around the world, since the e-passports can save biometric identifiers.To forbidden the illegal entry of passengers into a particular state and stop the use of fake documents, an e-passport is used for more precise identification of a person.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. This paper suggests also an encryption security analysis of the e-passport representing by using Arnold transform on fingerprint and add a privet key to encrypted data that are aimed to provide more security to the biometric information to protecting the e-passport.Our paper focuses on the security features which are suggested to make the e-Passport safer and protect it from unauthorized access.*

***Index Terms***—*E-Passport; Fingerprint; Biometric; Arnold transform; Discrete Wavelet Transform (DWT).*

## I. INTRODUCTION

One of the fundamental parts of international security is the trusted and secure travel documents, which is given an opportunity to international institutions to distinguish the movement of criminal or undesired persons.To prove the person's identity travel document is depended, this process is adopted by both governmental and non-governmental institutions.Therefore a secure travel document is, a significant means against identity stolen [1].

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

In 2006, 27 member states of European Union have been work in with to issue a new generation of passport called e-passport that includes some kind of digital image. Since 2009 they decide to issue next generation of e-passport that includes some biometric technologies (i.e. add two fingerprints). The idea behind the issuance of e-passport is to closely tie between the passport and its holder, in addition, to make sure of verification of authenticity of the passport.

So that an e-passport collected the passport booklet with its printed data (physically data) and physical security (for anti-fraud) measures, the electronic chip, the security mechanisms and data that are composed within the chip.We will pay attention to chip and the information it contains, also we will focus on its security mechanisms. An e-Passport has sometime known as a biometric passport which holds inside it the same information that already printed on passport's pages such as: person name, date of birth, and other biographic information [3,4].

The aim of the e-Passport is to improve security by fight fraud. In some cases, it helps speed up border crossings, but there is no guarantee that this will be the case[4]. The symbol of e-Passport is illustrated in Fig.(1).

Received 3 Sep 2018; Accepted 4 Dec 2018
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

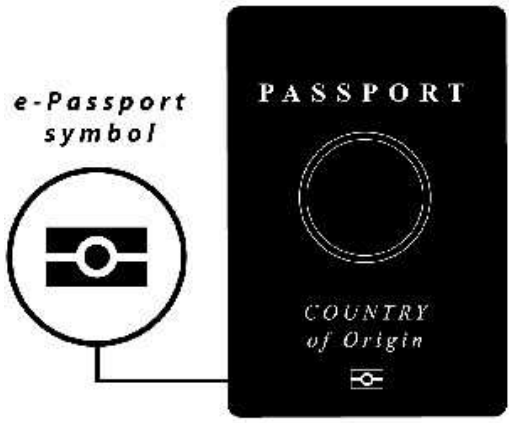



FIG.1 E-PASSPORT SYMBOL

The most commone used biometrics in this field are fingerprint recognetion, iris recognetion and facial recognetion. These were embraced after evaluation of a few various types of biometrics including retinal scan.

The comparison of biometric features is performed outside the passport chip by electronic border control systems (e-borders) [5]. Biometrics in e-passports consenting to the ICAO (The International Civil Aviation Organization) standard comprises of a mandatory facial image and fingerprints. While the previous is utilized by a significant number of countries and thus information on them is broadly accessible, the latter is utilized only occasionally. Therefore, this segment just covers the vulnerabilities of facial pictures and fingerprints [5].

In its simplest form an electronic passport contains only a gathering of read-only files, further developed can incorporate sophisticated cryptographic mechanisms protecting security of the document and / or privacy of the passport holder. The passport's critical information is both printed on the data page of the passport and stored in the chip.

In this paper we proposed a new and simple method for an encryption (Arnold transform) was used to add security for confidentiality of passport holders. Privet Key is add to recognize which was previously stored electronically in the passport chip making it precious and difficult to forge when all security mechanisms are fully and correctly implemented. Each country has a specific choice to biometric security features selected which results in it a major difference in the level of security and privacy protection.

at the checkpoint , the image can be gotten by reading the chip of the e-passport, in addition the biometric data which is encrypted in chip is extracted from the image and decrypted depending on the original key which was stored earlier.

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)[6,7].

Our new suggested method although it shares with the previous papers in the use of biometric data, but it uses more than one biometric identification and hides one of them in another after encrypting it, which gives a confirmation and confidentiality of the passport holder.

The proposed method helps in:

1- Enabled border officers to automate picket list checks in near-real time during the inspection
2- Permitted airline staff to produce shows of travelers with brief time
3- Generates a unified “secret key” that enables the conduct of selective inspections by retrieving information about the biometric identity of the passengers from the registration database

Received 3 Sep 2018; Accepted 4 Dec 2018

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

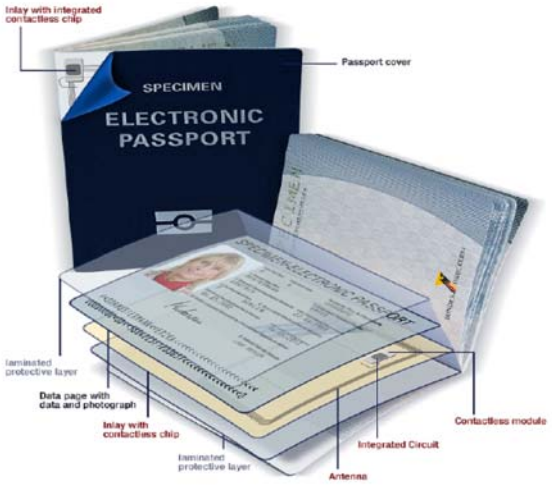



FIG.2. THE LAYERS OF AN ELECTRONIC PASSPORT.

## II. PHYSICAL ASPECTS OF e-PASSPORT

E-passports used a small Radio Frequency Identification (RFID) chip to stores some biometric information. The stored information is used to authenticate the identity of a passenger via a wireless network to the reader [8].

Fig.2 illustrates a passport sample, the logo of an electronic passport can be seen on the bottom of the passport cover. So that, a special paper is used to make out the cover. This paper should be secure and hard to counterfeit. The paper includes cotton and cellulose with no optical brighteners used. In addition, a watermark used on all the pages of the passport [9].

Furthermore, some chemical reagents used to prevent manipulation by acids or petrol derivatives. In case of using these substances, the chemical reagents will react and appear a passport in a useless state. Also, some fibers and small holographic stripes are embedded too. These material are visible only under UV light.

The printed inks used have a limited distribution and not obtainable commercially. The inks ingredients are secret because they contain some chemical reagents to make the passport safety for the same reason as the pages have to react differently if they are placed under UV light [10].

## III. ARNOLD TRANSFORM

Arnold transform is only suitable for encrypting $N\times N$ images. It is defined as [11]

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \quad (1)$$

Where (x,y),$(x', y')$ are the pixel coordinates of the original image and the encrypted image, respectively. Right part of (1), we denoted it by $\boldsymbol{A}$, and the original image pixels and the encrypted image is represented by I(x,y),$\mathrm{I}(x', y')^{(n)}$ which obtained by performing $n$ times of Arnold transform. So, encrypted image which using $n$ times Arnold transforms can be written as [11,12]

$$\mathrm{I}(x', y')^{(k)} = A\mathrm{I}(x, y)^{(k-1)} (mod N) \quad (2)$$

*Where* $k = 1,2,..n$, *and* $I(x', y')^{(0)} = I(x, y)$

Fig.3 illustrate a different level of Arnold transform

Received 3 Sep 2018; Accepted 4 Dec 2018

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

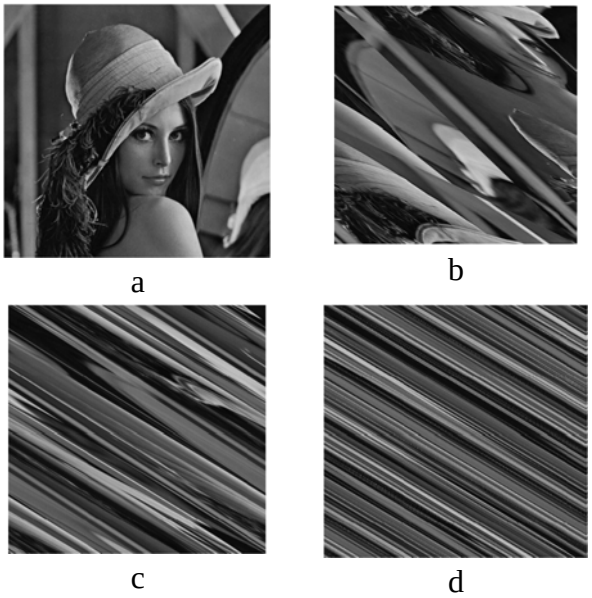



FIG.3. ILLUSTRATIONS OF THE ARNOLD TRANSFORM OF THE INPUT IMAGE LENA: (A)ORIGINAL, (B)ONE LEVEL, (C) TWO LEVEL AND (D) THREE LEVEL

## IV. PROPOSED SCHEMES

The suggested process to hide the watermark image (which is here is the fingerprint) is illustrated in Fig.4. First step for watermark image began by using multiple levels of Arnold transform. Because of a transformation used, the shape of watermark image is changing so we need to reshape it to its owned shape. For cover image (which is here is the passport holder) we used either DCT or DWT, in addition, we can consider it an extra operation for information compression.

After that, we embedded the watermarked information into the transformed image to get the watermarked image. In this step, we can add a privet key in order to verify the authenticity of the process. Fig.4 illustrates the operation of adding watermark to cover image.

The algorithm can be described below:

*i.* *Arnold algorithm (using eq.1)*

Step 1 save dimension of image $(NxN)$

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

Step 3 find $x'$ value by adding y mod N to x value

Step 4 new $y'$ value is calculate by adding $(2y\ mod\ N)$ to $x$ value.

Step 5 store $(x', y')$

*ii.* *Algorithm for Embedded two images using DCT*

Step 1 read cover image$(I)$ (holder image)

Step 2 read watermark image (fingerprint $(x, y)$)

Step 3 divides the image *I* into (8x8) blocks

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

Step 5 do Arnold transform 5 times for watermark image (use algorithm *i*)

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

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

Else

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

Step 7 Use IDCT transformation on the block which is embedded with watermarking information

Step 8 Repeat step 6 and 7 till all the information of the watermarked image have been added to all blocks.

Step 9 Add secret key

Received 3 Sep 2018; Accepted 4 Dec 2018

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

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

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j) - X'(i,j))^2 \quad (3)$$

The Second factor is peak signal-to-noise ratio (PSNR) which is used to evaluate the imperceptibility of the watermarked image, this can be calculated as [12]:

$$PSNR = 10.\log_{10}\left(\frac{MAX_i{}^2}{MSE}\right) \quad (dB) \quad (4)$$

Where $MAX_i$ is the maximum value of the pixel of the image.

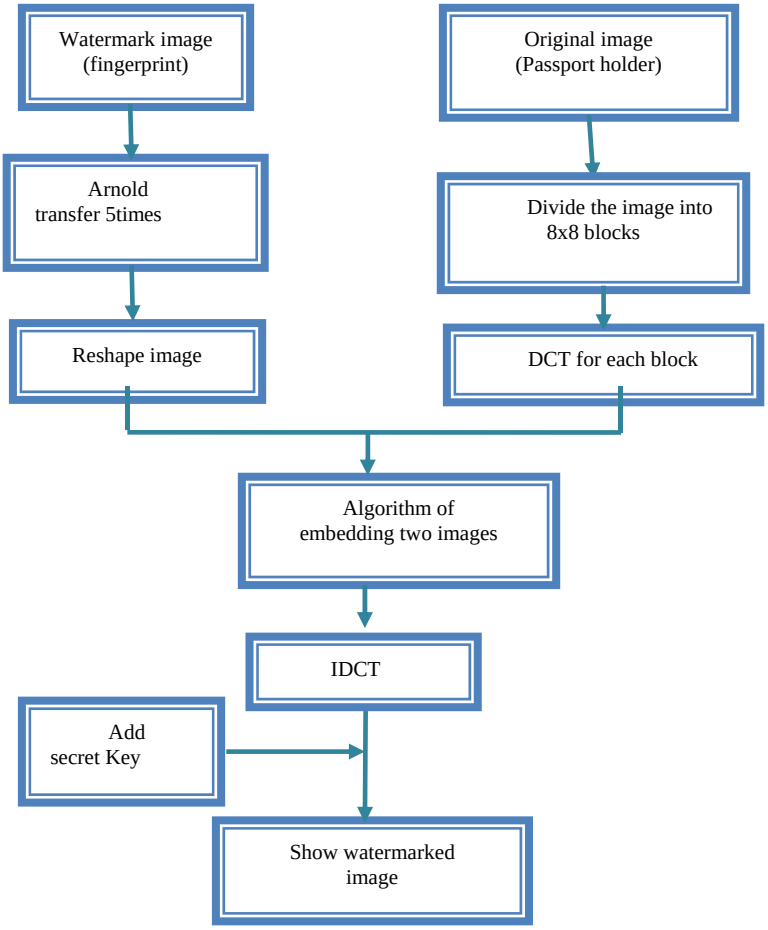



FIG. 4. MAIN PROCESSES FOR EMBEDDING WATERMARK USING DCT

Third factor used here is Normalized Correlation Coefficient (NCC), which is used to measure the performance extraction results of the blind or non-blind watermark for the extracted watermark W' and the original watermark W, NCC can be defined as[13]:

Received 3 Sep 2018; Accepted 4 Dec 2018

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

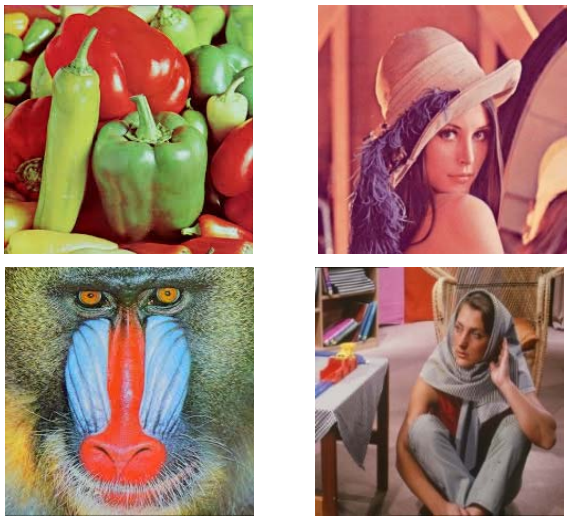
$$NC(W,W') = \frac{\sum_{i=1}^{n} W(i).W'(i)}{\sqrt{\sum_{i=1}^{n} W(i)^2}.\sqrt{\sum_{i=1}^{n} W'(i)^2}} \quad (5)$$

Where (n×n) are represent the dimensions of the watermark. The magnitude range of NC alter between [-1 and 1], exact matching between original watermark and extracted one will give a unity value.

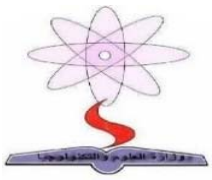
In the beginning, we used some slandered test images to evaluate the performance of our new suggest method to get comparable results.

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 types and choose the better method. For doing this we used four standard color images as a cover image with dimension 512x512, and one color logo as an invisible watermark with dimension 100x100, these image is shown in Fig.5

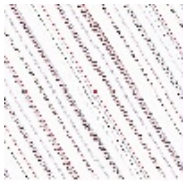
Also, we try to change the number of Arnold level to study its effect on the reconstructed image. Table.2 illustrates the results of changing Arnold level, we used DWT on Lena color image.



-a- standerd 512x512 image



-b-
logo watermark image



-c-
after 3 level of Arnold transform

FIG.5. 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 interface of our application program for the suggested method is illustrated in Fig.6. 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 to read the image of the passport holder then the second biometric which is the fingerprint is

Received 3 Sep 2018; Accepted 4 Dec 2018

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

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 stored into the information list for the e-Passport chip. At the checkpoint, the operation of decryption is started and the fingerprint is extracted and checks it with the original one to distinguish the fake one.

TABLE 1: RESULTS FOR DWT METHOD

| Test Image 512x512 | 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 |

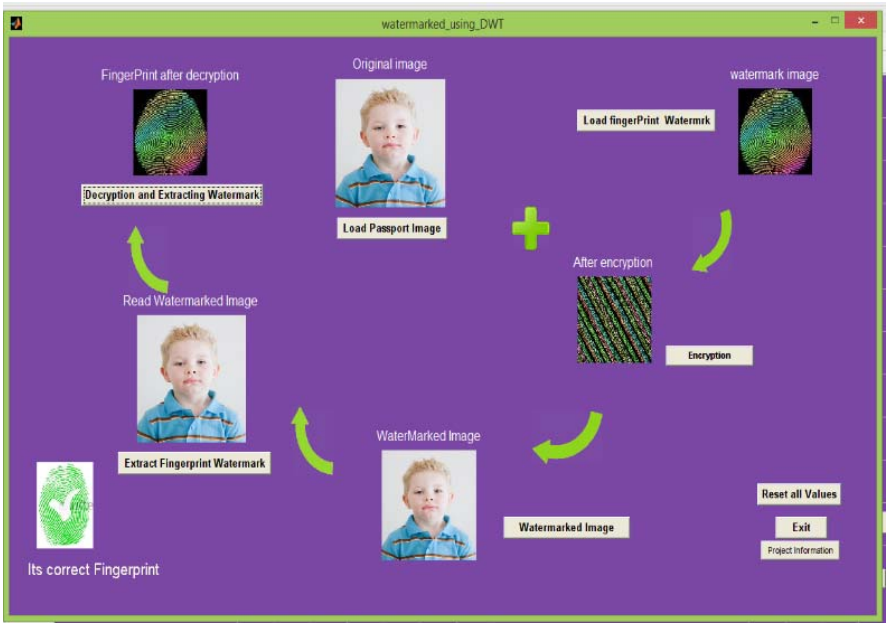



FIG.6 INTERFACE FOR SUGGESTED APPLICATION USED FOR HIDING FINGERPRINT INTO ANOTHER BIOMETRIC

## VI. CONCLUSIONS

The specific objectives of this paper are to identify the best pursuit related to the processes of issuance e-passport and to suggest a set of recommendation to repair security gaps in the issuance process.

The paper represents an attempt to add multi biometric to the e-passport scheme using face and fingerprint of the e-passport holder to improved identification for more security and fraud prevention.

Received 3 Sep 2018; Accepted 4 Dec 2018

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

The used of biometrics in passports required high accuracy rates, secure data storage, secure exchange of data and trustworthy 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 passports machine-readable will improve their robustness against id theft if additional security measures are performed.

## REFERENCES


[1] Rondo ONZ " Operational and Technical security of Electronic Passports", Frontex Agency , Warsaw, July 2011.

[2] Ari Juels_, David Molnar†, and David Wagner "Security and Privacy Issues in E-passports", UC-Berkeley,,2011

[3] Official website of the Department of Homeland Security "e-Passports" , https://www.dhs.gov/e-passports, USA, 2016

[4] Government of Canada Site "How ePassports work", http://www.cic.gc.ca/english/passport/help/epassport.asp

[5] V.K. NARENDIRA KUMAR & B. SRINIVASAN, "Design and development of E-passprts using biometric access control system",International Journal Of Advanced Smart Sensor Network Systems ( IJASSN ), Vol 2, No.3, July 2012

[6] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce " A Multiresolution Watermark for Digital Images" Image Processing, conference IEEE Xplore , 2010

[7] Syed Ali Khayam "The Discrete Cosine Transform(DCT):Theory and Application" chapter3, Michigan State University 2003

[8] Hesam Kolahan, Tejendra Thapaliya "Biometric Passport: Security And Privacy Aspects Of Machine Readable Travel Documents", Swiss Joint Master of Science in Computer Science, December 2011

[9] Prashant Shende , Pranoti mude, and Sanket Lichade "Design and Implementation of Secure Electronic Passport system", International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Issue 11, November 2015

[10] Johannes Eifert , Lorenz Schwob "Security and Privacy of the biometric Passport", Universität Freiburg,Department of Informatics December, 2012

[11] Zhenjun Tang and Xianquan Zhang "Secure Image Encryption without Size limitation Using Arnold Transform and Random Strategies", JOURNAL OF MULTIMEDIA, VOL. 6, NO. 2, APRIL 2011

[12] Divya saxena "Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform" International Journal of Electronics and Computer Science Engineering 2014

[13] YahyaAL-Nabhani Hamid AL-Jalab "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network",Journal of King Saud University - Computer and Information Sciences Volume 27, Issue 4, October 2015, Pages 393-401


Received 3 Sep 2018; Accepted 4 Dec 2018

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352