Journal of Computer Science 1 (1): 103-106, 2005
ISSN 1549-3636

A New Approach for Authentication Technique

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

Abstract: One of the serious problems is how to authenticate the passport document for its holder. The major factor of this authenticity is the corresponding of the Passport's photo with its holder. Most of the Passport document contains a holder's signature in addition, of course, to the full name. We propose 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. The modern method of issuing a passport now is by using a computer in fixing the passport's photo (imaging). In using this method we could hide the invisible watermark which contains the digest name and passport number inside the passport's photo. During the hidden process there are many techniques could be applied to disguise any color difference appears during the hidden process. 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 number.

Key words: Passport's Photo, Holder's Name, Watermark, Authentication

INTRODUCTION

Steganography provides for the embedding of information in a block of host data in conditions where perceptible modification of the host data is intolerable. Steganographic techniques are highly dependent on the character of the host data.

A technique for embedding information in image makes subtle changes in hue, while a method for embedding information in audio data could exploit the limitations of the human ear by encoding the encapsulated information in audible frequency ranges. Current implementations of textual Steganography exploit tolerances in type setting by making minute changes in line placement and kerning in order to encapsulate hidden information, making them vulnerable to simple retype setting attacks.

Manipulating digital media in an effort to disable or remove the embedded messages is a simpler task than detecting the messages. Any image can be manipulated with the intent of destroying some hidden information whether an embedded message exists or not. Detecting the existence of a hidden message will save time in the activity to disable or remove messages by guiding the analyst to process only the media that contain hidden information [1]. Because the most successful hiding method is the uncommon one, but it is unthinkable one and needs a knowledge and experience to be discovered.

Every few years, computer security has to re-invert itself. New technologies and new applications bring new threats, and force us to invent new protection mechanisms. Cryptography has become important when business started to build networked computer system; Virus epidemics started once large numbers of Personal Computer (PC) users were swapping programs; and when the Internet took off, the firewall industry was one of the first to benefit [2].

One of the newest hot spots in security application is information hiding. It is driven by two of the biggest policy issues of the information age-copyright protection (watermark) and state surveillance (Steganography). In the proposed system we have implemented the scheme of watermark as a method of authentication.

The Problem: Watermarking has been suggested to play an important role in securing the business, as it allows placing an imperceptible mark in the multimedia data to identify the legitimate owner and to prosecute the pirate [3].

There are a number of requirements for watermarking techniques [4]:

Robustness: The embedded information is said to be robust if its presence can be reliably detected after the image has been modified, but not destroyed beyond recognition.

Invisibility: This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carries that contain the hidden information and those that do not.

Undetectability: The concept of undetectability is inherently tied to the statistical model of the image source. If an attacker has a more detailed model of the source, he may be able to detect the presence of a hidden image, but this does not imply the ability to read the hidden message.

Security: The embedding algorithm is said to be secure, if the embedded information can not remove beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except the secret key).

Nowadays, computer involved in all life details. One of these issues is producing the passport document by using the computer application. To fill full this objective there are several requirements such as using a computerize photo for the passport holder with special colors (grey and white). Also most of the passport offices are connected through a network to exchange their information about the correctness of passport information and the authentication of the passport holder. It is possible to transfer the passport image between different offices to get information confirmation.

Here, the main problem is how to confirm and authenticate the passport's photo with the information about the holder. There is no other way to tell if the photo been replaced with a new one (for the current holder) because there is no physical connection between the photo and the passport details.

The Proposed Method: The aim of the proposed method is to develop a firm connection between the passport's photo and the passport's details. In this case it is possible to use this method for confirmation of passport's information.

The summery of this method is by converting the holder's name (1st, 2nd, 3rd and family name) in addition to the passport number into one form called an invisible watermark. This watermark will be disguised and distributed inside the passport's photo. This process will be done during the issue of the passport for the first time. Note that all the watermark requirements will be considered. The details of the proposed method is shown in Fig. 1.

The proposed method consists of several algorithms. Each algorithm is responsible for one type of process. All the required validations processes will be taken in consideration by the proposed method. The following algorithms are used in the proposed method:

Algorithm One (Parameters 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.

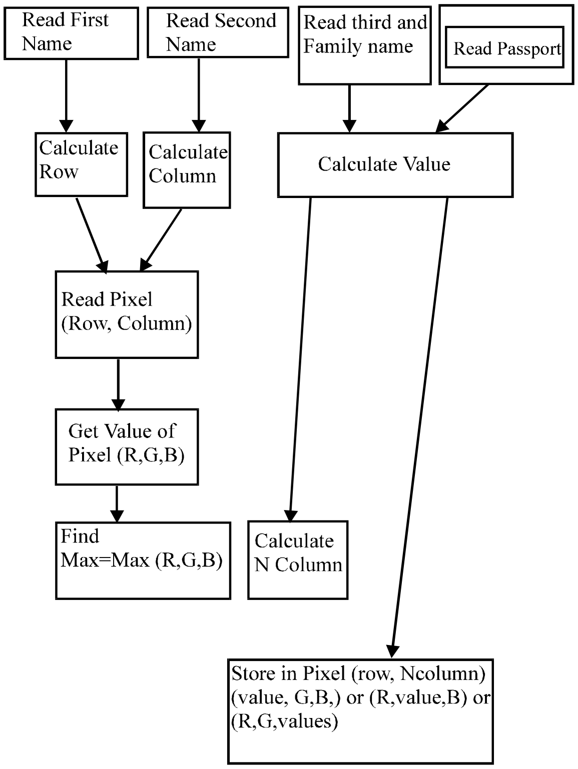


Fig. 1: Method for Confirmation of Passport's Information

Algorithm Two (Convert)

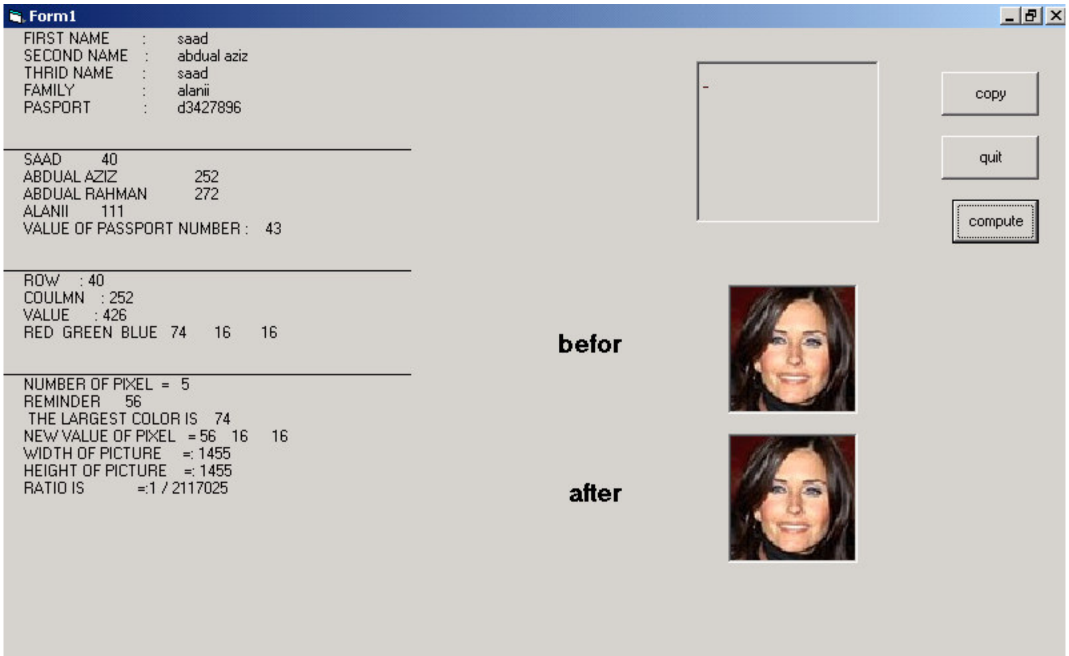
1. Consider the key value. E.g. key = "1,2,3,4"
2. Get the summation of the first name by adding the code of each character multiplied by the key's character on a sequence manner. E.g. code[1]* key[1] + code[2[*key[2] + code[3]*key[3]+……
3. Consider the result as " row ".
4. Repeat step (2) for the second name.
5. Consider the result as " column ".
6. Repeat step (2) for the third name and family name.
7. Add the third name, family name and the passport number and the result will be "value".

Algorithm Three (Hide)

1. Read the value of the pixel on location (row, column) from the original Image.
2. Find the largest value of RGB color for that pixel and assign it to "large ".
3. Divide "value " on " large " to get number of pixels.
4. Calculate the modulo of " value " over " large " and assign it to " color ".
5. Calculate Ncolumn so that equals to " column " + " No. of pixel " + 1.
6. Get the pixel value in location (row, Ncolumn).
7. Replace the largest value of RGB for that pixel with "color".
8. Restore the pixel at the same location.

Table 1: Letters with their Equivalent Numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26



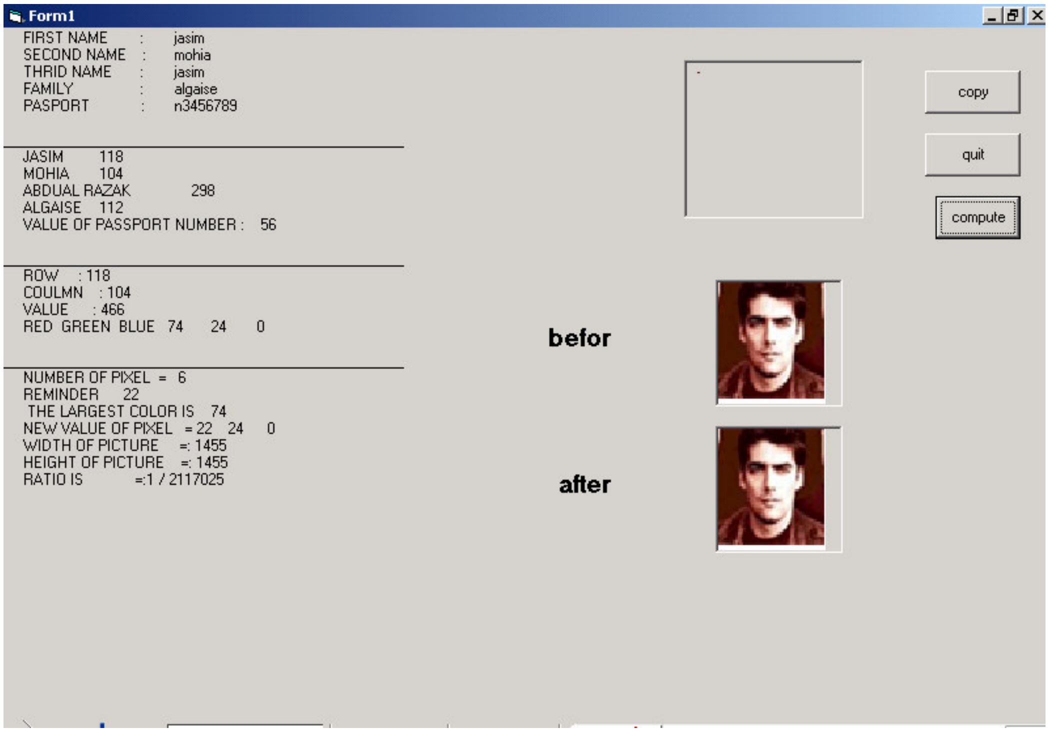
```
FIRST NAME      :     saad
SECOND NAME   :     abdual aziz
THRID NAME      :     saad
FAMILY             :     alanii
PASPORT          :     d3427896

SAAD       40
ABDUAL AZIZ              252
ABDUAL RAHMAN         272
ALANII      111
VALUE OF PASSPORT NUMBER :   43

ROW    : 40
COULMN   : 252
VALUE     : 426
RED  GREEN  BLUE   74      16       16

NUMBER OF PIXEL  =   5
REMINDER      56
 THE LARGEST COLOR IS    74
NEW VALUE OF PIXEL   = 56   16      16
WIDTH OF PICTURE     =: 1455
HEIGHT OF PICTURE    =: 1455
RATIO IS            =:1 / 2117025
```

Fig. 2: Practicing of the Proposed Algorithm



```
FIRST NAME      :     jasim
SECOND NAME   :     mohia
THRID NAME      :     jasim
FAMILY             :     algaise
PASPORT          :     n3456789

JASIM       118
MOHIA       104
ABDUAL RAZAK             298
ALGAISE    112
VALUE OF PASSPORT NUMBER :   56

ROW    : 118
COULMN   : 104
VALUE     : 466
RED  GREEN  BLUE   74      24       0

NUMBER OF PIXEL  =   6
REMINDER      22
 THE LARGEST COLOR IS    74
NEW VALUE OF PIXEL   = 22    24      0
WIDTH OF PICTURE     =: 1455
HEIGHT OF PICTURE    =: 1455
RATIO IS            =:1 / 2117025
```

Fig. 3: Another Example before and after Hiding Process

Implementation: We apply the three proposed algorithms into two examples. Figure 2 shows the practicing of the proposed algorithms.

Algorithm one will accept the necessary information and that will be the full name of the passport's holder and the passport's number. After the required information has been entered, there will be a validation process to make sure that all the inserted information is correct.

Each letter in the names string is assigned a number chosen from a table. This table contains the letters with their equivalent numbers as shown in Table 1. The following equation can be used to assign the value: value = ASCII (character)-64.

At the end of this algorithm each name (first, second, third and family) has a sequence of number according to its length.

Algorithm two starts by assigning a key with four digits (e.g. 1,2,3,4) referring to the used four names (1st,2nd,3rd and family name). Then calculating the value for each name and the passport number according to algorithm two. E.g. code[1]*key[1] + code[2]*key[2]+…… for the 1st name. The following equation could be used:

$$\sum_{\substack{i=1\\ j=1}}^{\substack{j=m\\ i=n}} i * code_i * key_j$$

key(j) = 1 $\forall j$

where, n= name length and m= key length.

The same thing will be done for the rest of the names and the passport number. We will get:

First name = 40 = row number.

Second name = 272 = column number.

Third name + family name + passport number.

272 + 93 + 37 = 402 = value.

Now we arrived to the last stage (algorithm three) which is responsible for the hiding process. According to this algorithm we read the value of the pixel on location (row, column) from the original Image. Then we find the largest value of RGB color for the pixel and we call it "large". After we divide the "value" by "large" we get the number of pixels. We use modulo of "value" over "large" to get "color". Then we calculate the new column for the pixel to be hidden. Figure 2 shows also the passport's photo before and after hiding process. Figure 3 shows another example for the hiding process.

DISCUSSION

This research has suggested a new method for authentication. An invisible watermark has been suggested to authenticate the passport's holder. All the requirements for the watermark technique have been taken into account.

The suggested invisible watermark has satisfied the Invisibility, undetectibility, and Security requirements. Because the proposed technique has used a small area for hiding (one pixel), so it satisfied the robustness against image compression. The security requirement is achieved by the random distribution of the watermark over the entire image, which makes the watermark detection is time consuming.

To preserve the undetectibility requirement, the invisible watermark has a small capacity comparing to the image size (1/2117025) which is unnoticeable even if we use the statistical comparison for the images (before and after hiding). One additional factor has been used to make the watermark undetectable and that by changing the pixel color to be compatible with RGB color for the original image.

The proposed method is secure and effective, but it works for one National State and could be used between more than two States and that by transmitting copy of the passport between them for authentication.

It is possible to make the suggested method works globally and that by using a public key for each Country to hide the watermark and a private key to open it by different countries.

REFERENCES

1. Neil, F. Johson, Zoran Duric and Sushil Jajodia, 2001. Information Hiding: Steganography and watermarking attacks and countermeasures. Kluwer Academic puplishers.
2. Al-Hamami, Alaa and Soukaina Hassan, 2003. A proposed Firewall Security against different types of attacks. Al-Rafidain Magazine for Science, No. 14, Baghdad, Iraq.
3. Richard, Clark, 2001. An introduction to JPEG 2000 and Watermarking. © Elysium Ltd.
4. Stefan, K. and F.A.P. Petitcolas (Eds.), 2000. Information Hiding techniques for steganography and digital watermarking. ISBN 1-58053-035-4 © Artech House, Inc.