Design and Implementation of Hiding Secure Information Based Transposition Cipher Technique for National Identification Card

Sabah A. Gitaffa* (Lecturer)

Abstract

The Security of information on web has turn into a former thing. In spite of the fact that any message is scrambled utilizing a stronger cryptography method, it can't evade the suspicion of interloper. This paper proposes a methodology in such way that, identity information (ID) is encoded utilizing transposition cipher algorithm and afterward this ciphertext is hiding in person image utilizing LSB method. Also in this paper, a ciphertext and biometric key generation algorithm are combined using an effective algorithm to protect the ID information. The purpose of proposed algorithm is to prevent unauthorized persons from viewing or modifying the data and has resistance to Brute-force attack. The obvious attributes of the individual picture prior and then afterward disguise remained just about the same. This algorithm can provide better security to ID card information. The algorithm has been executed utilizing Matlab.

Keywords: ID card, Biometric, Information hiding, Transposition method, Identification Code.

* Department of Electrical Engineering, University of Technology

1. Introduction

Biometrics is an intense method based on the anatomical and behavioral qualities of the individuals. Biometrics is characterized as the measure of human body qualities, for example, unique finger impression, Finger Knuckle Print (FKP), eye, retina, voice example, and iris and Hand estimation. Most anatomical attributes utilized for security application are unique mark, Iris, face and palm print. Aside from anatomical attributes, behavioral characters like voice, mark, and walk minutes are likewise used to perceive the client. Subsequently, confirmation drives a vital part in the secured method for correspondence. Right now, passwords and smartcards are utilized as the verification instruments for confirming the approved client. Biometrics-cryptography techniques are an effective way to provide better secure privacy and prevent ID information theft. Conventional cryptography uses encryption keys, usually 128-bits or more. The problem with these conventional cryptography techniques is that a person cannot memorize such a long random key and it can be guessed, found or stolen by an attacker with a brute force search. On the other hand, Biometric Encryption is a type of technology which has enormous potential to enhance privacy and security. Biometric Encryption is a combination of biometric and cryptography. Hence, it can be used as a solution to this problem as it is difficult for an intruder to know the biometric key [1,2].

2. Integration of Biometrics into Identification Card

Personality cards (IDs) are being used, in some structure, in various nations around the globe. The kind of cards, its capacity, and its honesty change hugely. Around a hundred nations have official, mandatory, national IDs that are utilized for a mixed bag of purposes, for example, Germany, France, Portugal and Spain. Participation in national identification card scheme may be mandatory or voluntary. Traditional, such programs have been used primarily to control access checkpoint, such as border control at ports of entry into a country. These cards usually contain identifying information such as name, date of birth, gender, and a government –issued identification number. In some countries additional information such as height, eye, and hair color, or current address can be included as well [3]. A biometric framework is a suitable approach to confirm clients to utilize ID card and it is works by getting biometric information from a man, extricating a list of capabilities from the gained information, and contrasting this information and data put away in the database [4]. Fingerprint recognition is one of the oldest methods of biometric identification. Biometric-key can be used to provide enhanced security level. It uses key which is generated from more than one biometric. This provides reliable biometric keys for encryption algorithms and can be used for better security. Biometric key authentication process suffers from attacks like presenting fake biometrics, tampering with the biometric feature presentation, attacking the channel between stored template and the matching unit, corrupting the matching unit. To avoid these attacks, authentication biometric key is used. In this paper, an algorithm is proposed to hiding encrypted person information based transposition cipher technique into person image for ID card applications.

3. Hiding of ID Information

Information hiding is a common, simple technique to embedding information in to a file. The most used method of information hiding is a least significant bit (LSB). The LSB is the lowest significant bit in the byte estimation of the picture pixel [5]. There are two types of LSB based on image format (8-bit, 24-bit) [6,7]. In this paper, we will focus on a 24-bit color image. In 24-bit color image there are a 3-bits from each pixel of image can be stored to hide an image by using LSB algorithm. The information hiding based on LSB is as following steps:

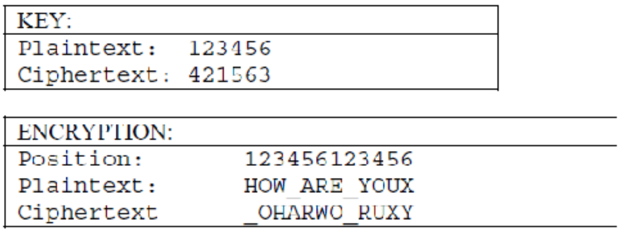
- Read the 24-bit face-image in RGB format (Red (8-bit), Green (8-bit) and blue (8-bit)),
- Preform dec2bin conversion (Decimal to Binary) for face-image,
- Read the 8-bit of person information (plaintext).

- Let the first RGB pixel of face-image is [11011111 11000110 10000111],
- Let the first byte of plaintext is [00110101],
- Perform the replacing 2 bit of LSB of each of RGB component and then hiding first 2 most significant bits (MSB) of first pixel of fingerprint image to RED component,
- Repeat the previous step for the second 2 MSB of first pixel of fingerprint image to GREEN component and lastly another next 2 MSB of first pixel of fingerprint image to BLUE component.
- The final result of first pixel of output image is: [11011100 11000111 100000101].

4. Transposition Cipher Method

In this paper, the personal information of ID card is encrypted by using transposition method before hiding. A transposition works by dividing a message into settled size blocks, and after that permuting the characters inside each block as indicated by an altered change, P. The way to the transposition cipher is just the change P. In this way, the transposition cipher has the property that the encoded message i.e. the ciphertext contains every one of the characters that were in the plaintext message. At the end of this process, the unigram insights for the message are unaltered by the encryption process. The size of the permutation is called the period. For an example transposition technique, a period is (6), and a key (P) is {4, 2, 1, 5, 6, 3}. The plaintext is divided into 6 characters, and from right side the third character in the block will be moved to position 6, the second character moves to position 5, the fifth character is moved to position 4, the first character will move to position 3, the second remains in position 2 and the fourth character to position 1. The encryption process is shown in table 1 [8].

Table 1: Trans-position example.



KEY:	
Plaintext:	123456
Ciphertext:	421563

ENCRYPTION:	
Position:	123456123456
Plaintext:	HOW_ARE_YOUX
Ciphertext	_OHARWO_RUXY

5. Proposed Methodology

In this section we describe the proposed algorithm with a brief introduction. The proposed biometric algorithm is shown in figure 1. The algorithm is as the follow:

- Read the person image,

  ```
  img = imread( strcat(PathName,FileName) );
  ```

- Read the plaintext (personal information),

  ```
  % Read Message (Plaintext) File

      [FileName,PathName] = uigetfile('*.txt','Select TEXT MESSAGE.');
      testmsg = fopen( strcat(PathName,FileName) );
      [msg] = fscanf(testmsg,'%c');
  ```

- The PN sequence generator produces 512 random keys depend on identification key.

  ```
        G=512;  % Code length
       %Generation of first m-sequence

      Bit1 =[0 0 0 0 0 0 0 1];          % Initial state of Shift register

      PN1=[];                   % First m-sequence

      for j=1:G

      PN1=[PN1 bit1(8)];
  ```

- The keys (K1 and K2) are applied to the xor gate.

```
KEY = bitxor (K1,K2);
```

- The output of xor gate is shifted for n-bits (in this work 6-bit).
- The biometric encipher password is now available to encrypt the personal information.

- Encrypt the plaintext,

```
 f_file = fopen(add, 'r');
 plain_txt = fscanf(f_file, '%c');
 trans=zeros(N,N);
 NN=N*N;
 cipher_txt=[];
 D=length(plain_txt);
 pad=mod(D,NN);
plain_txt=[plain_txt zeros(1,pad)];
for r=1:length(plain_txt)/NN
for s=1:NN
trans(s)=plain_txt(s+NN*(r-1)+3);
end
trans=trans';
for q=1:NN
 cipher_txt=[cipher_txt trans(q)];
end
end
cipher_data=char(cipher_txt);
```

- Hide the ciphertext in the face image,
- The result is a face-image with encrypted personal information.

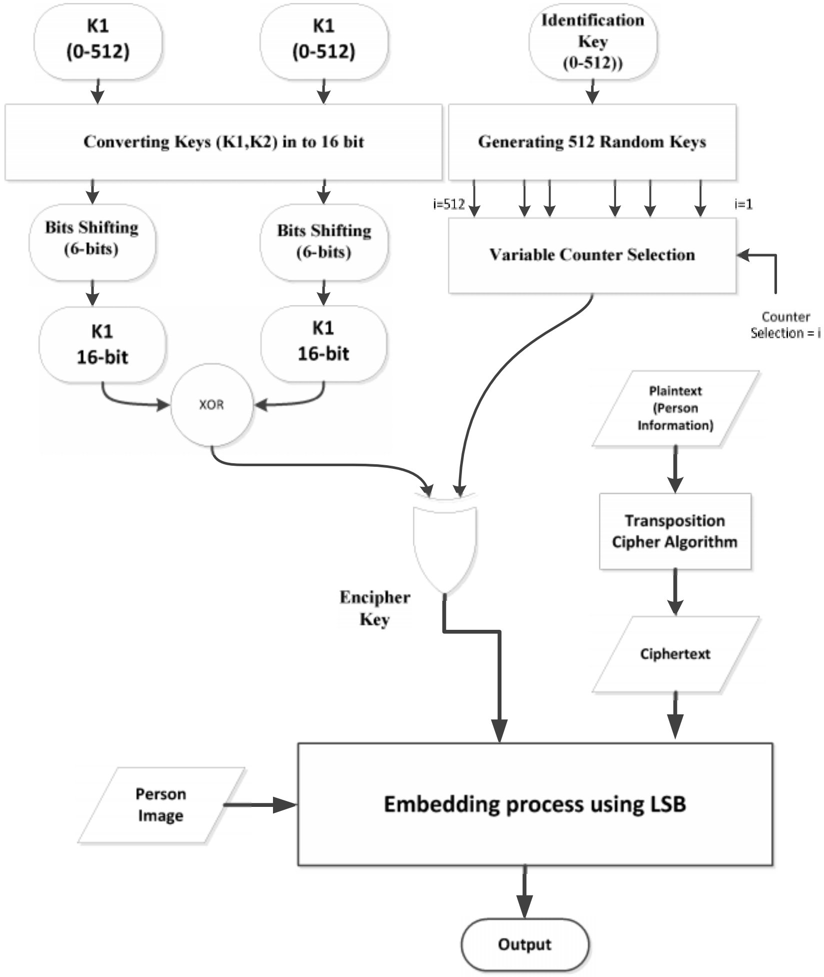


Figure 1: Biometric Encipher Algorithm.

6. Simulation Results & Discussion

We have used 256 × 256 size image is taken from [9] for cover image (person). The proposed algorithm has been implemented in the working platform of MATLAB (version 8.1). To test the performance of the proposed system, the Peak Signal to Noise Ratio (PSNR) parameter is used to evaluate the quality of image. The PSNR ratio is defined as a quality measurement between the original image and stego image. The higher of PSNR parameter improves the quality of the stego image. For wireless applications, PSNR values are between 30 db and 50 db. The PSNR is calculated by the following equations [10,11]:

$$\mathrm{PSNR} = 10 \log_{10} \{255^2 / \mathrm{MSE}\} \quad \text{.................................(1)}$$

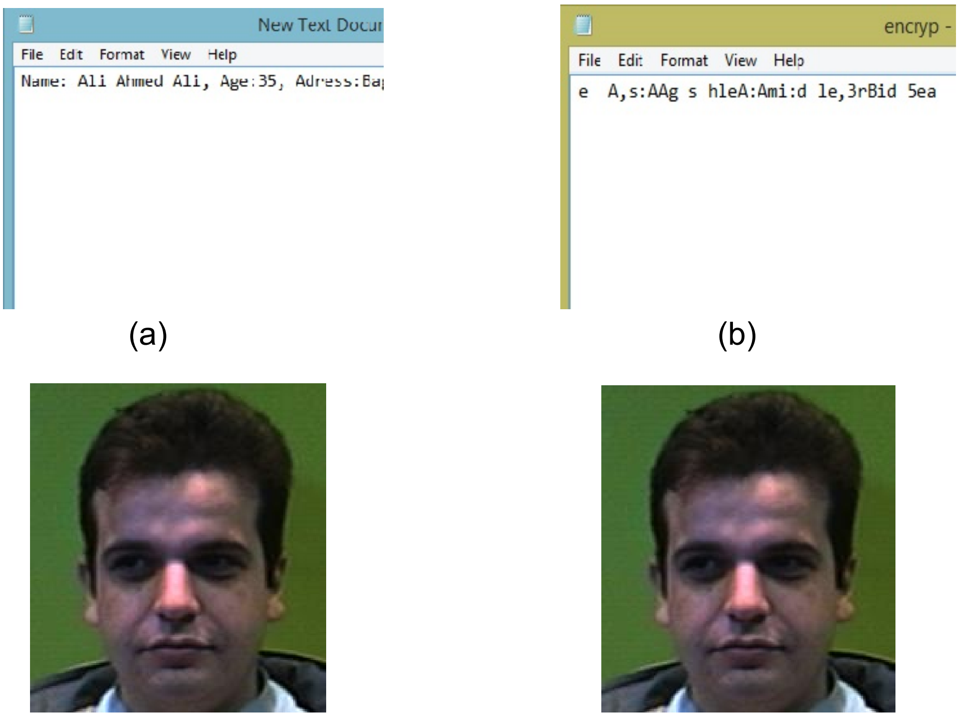
where MSE: Mean-Square error and is given by Eqn.2 [12].

$$MSE = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{ij} - B_{ij}|)^2}{x * y} \quad \text{...............................(2)}$$

The input file is information for person in plaintext, as shown in figure 2a. The output of transposition cipher is shown in figure 2b. This ciphertext is then encrypted by using biometric cipher algorithm. A comparison between original image, LSB embedded image is shown in Figure 2(c,d). After seeing the figure it is clearly seen that quality of LSB image diminish when data is hided. And after seeing the image it can be encoded message is seen with visible eye. While in biometric image data is completely unseen and cannot be perceived by eye and quality of image remain unchanged. The final result of measurements is shown in table 2. The PSNR is 77.4613 dB greater than 73.4008 dB in Ref. [13]. The mean square error is 0.0012 lower than 0.00297 in the Ref. [13].

Table 2

Mean Square Error	Normalized Cross-Correlation	Peak Signal to Noise Ratio
0.0012	1.0000	= 77.4613



```
Name: Ali Ahmed Ali, Age:35, Adress:Ba
```

```
e  A,s:AAg s hleA:Ami:d le,3rBid 5ea
```

(a) (b)

(c) (d)

Figure 2: (a) Plaintext, (b) Ciphertext, (c) Person I/P image (d) LSB O/P image.

7. Conclusion and Future Work

The proposed framework has two layered security levels. The first one is through encryption of the content utilizing transposition cipher method and second one is through embedding the encoded content into LSBs with variable biometric cipher key. This algorithm can provide better security to ID card information. Digital steganography is a fascinating work area which falls under security systems. The main emphasis in mine results will be on visual image quality being preserved and also the PSNR value which is a measure of quality of embedding. From the presented results, the proposed system provides strong a backbone for its security and enhances the security of data. For future work, we can apply our algorithm on different types of sources (audio and video).

8. References

[1]. Ashraf El-Sisi, “Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter”, The International Arab Journal of Information Technology, Vol. 8, No. 4, October (2011).

[2]. P. Muthu Kannan and Anupriya Asthana “Secured Encryption Algorithm for Two Factor Biometric Keys”, International Journal of Latest Research in Science and Technology, Vol.1, No.2, PP.102-105, July-August (2012).

[3]. William Sloan Coats, “The Practitioner's Guide to Biometrics”, American Bar Association (ABA) publishing, 2007.

[4]. Najme Zehra, Mansi Sharma, etc, “Bio-authentication based secure transmission

system using steganography”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 8, No. 1, April (2010).

[5]. Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, etc, “Least Significant Bit algorithm for image steganography”, International Journal of Advance Computer Technology, Vol.3, No. 4, August (2014).

[6]. Manoj Kumar Meena and Shiv Kumar, “Neetesh Gupta, Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity”, International Journal of Soft Computing and Engineering (IJSCE), Vol.1, No.2, May (2011).

[7]. G. Viji and J. Balamurugan, “ LSB Steganography in Color and Grayscale Images without using the Transformation ”, Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue, December (2011).

[8]. R. Toemeh and S. Arumugam, “Breaking Transposition Cipher with Genetic Algorithm”, Electronics And Electrical Engineering journal, Vol.79, No.7, (2007).

[9]. http://www.face-rec.org/databases/.

[10]. Shamim Ahmed Laskar and Kattamanchi Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems (IJDMS), Vol.4, No.6, December (2012).

[11]. Hengfu YANG, Xingming SUN and Guang SUN, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, Radio Engineering Journal, Vol. 18, No. 4, December (2009).

[12]. Shweta A.Tambe1, Nikita P. Joshi and P.S. Topannavar, “Steganography & Biometric Security Based Online Voting System”, International Journal of Engineering Research and General Science, Volume 2, No.3, April-May (2014).

[13]. R.S. Gutte1, Y.D. Chincholkar and P.U. Lahane, “Steganography for Two and Three LSBs Using Extended Substitution Algorithm”, ICTACT Journal on Communication Technology, Volume 4, No.1, March (2013).

تصميم وتنفيذ إخفاء معلومات الآمنة بالاعتماد على تقنية شفرة إبدال الموضع لبطاقة الهوية الوطنية

م.صباح عبد الحسن كطافة*

المستخلص

اصبح أمن المعلومات على شبكة الإنترنت من الاشياء المهمة. وعلى الرغم من حقيقة أن أي رسالة تشفر باستخدام طريقة تشفير قويه، فإنه لا يمكن التهرب من شبهة الدخيل. تقترح هذه الورقة منهجية في مثل هذه الطريقة التي، يتم ترميز معلومات الهوية (ID) باستخدام خوارزمية شفرة أبدال الموضع ومن ثم يتم اخفاء المعلومات المشفره في صورة باستخدام طريقة LSB. أيضا في هذه الورقة ،تم الجمع بين النص المشفر و خوارزمية توليد مفاتيح باستخدام خوارزمية فعالة لحماية المعلومات الشخصية. والغرض من الخوارزمية المقترحة هو منع الأشخاص غير المخولين من عرض أو تعديل البيانات ولديها مقاومة لكسر الشفرة. ان السمات الواضحة للصورة الفردية قبل و بعد تنفيذ النظام المقترح ظلت بدون تغيير. توفر هذه الخوارزمية أمن أفضل لمعلومات بطاقة الهوية. تم تنفيذ الخوارزمية باستخدام برنامج الماتلاب.

*الجامعة التكنولوجية – قسم الهندسة الكهربائية