Journal of Engineering and Development

www.jead.org
Vol. 20, No.1, January 2016
ISSN 1813-7822

IMPLEMENTATION OF HIDING SECURED FINGERPRINT IN FACE IMAGE FOR BIOMETRIC APPLICATIONS

Lecturer Sabah A. Gitaffa*

Lecturer Department of Electrical Engineering, University of Technology, Baghdad, Iraq.

(Received:07/06/2015 ; Accepted:08/12/2015)

Abstract: Biometrics are the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual. The most common biometric form is fingerprints. In this paper, a fingerprint and password are combined using an effective algorithm to protect fingerprint. This algorithm can provide better security to ID card information. The proposed system provides strong backbone for its security and enhances the security of data. The final result of power signal to noise ratio (PSNR) is 44 dB. The programming language MATLAB is used for implementing the proposed algorithm.

Keywords: *Fingerprint, Biometric, Information hiding, Encipher, Decipher, Identification Code.*

تنفيذ اخفاء بصمات الأصابع مؤمنه في صورة الوجه للتطبيقات البيومترية

الخلاصة: المقاييس الشخصية او البيومترية هي الخصائص البيولوجية القابلة للقياس (التشريحية والفسيولوجية) أو الخصائص السلوكية المتستخدمة لتحديد هوية الفرد. أن اكثرالمقاييس الشخصية شيوعاهي بصمات الأصابع. في هذه البحث،تم الجمع بين بصمة الاصبع ومفتاح تشفيرباستخدام خوارزمية فعالة لحماية بصمات الأصابع. يمكن لهذه الخوارزمية توفير أمن أفضل لمعلومات بطاقة الهوية. ويوفرالنظام المقترح الاساس القوي لأمنها ويعزز أمن البيانات. تم الحصول على اعلى نسبة اشاره الى الضوضاء بمقدار (44 dB). تم تنفيذ الخوارزمية المقترحة باستخدام لغة البرمجة MATLAB.

1. Introduction

Biometrics is an emerging technique which provides an effective solution regarding security issues of wireless communication. Biometric identifies or verifies individuals accurately in real time based upon their unique physical characteristics such as faces, hands, irises, and fingerprints or behavioral characteristics such as typing rhythm, gait and voice.

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

*sabahahg@yahoo.com

attacker with a brute force search. On the other hand, biometric encryption is a type of 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. Fingerprints

Biometrics based authentication systems have inherent advantages over other personal identification techniques. Biometrics uses data, such as faces, fingerprints, irises, voice prints, palm prints, retinal patterns and signatures, to identify persons using image processing techniques [2]. The biometrics information is unique to the individual and remains during one's life. It is very important to have reliable personal identification because growing significance of Information Technology (IT). Among all the biometric methods being used in present day, fingerprint recognition is the oldest method, which has been successfully used in multiple applications. Every person is known to have a unique fingerprint and it does not change during his lifetime and so the fingerprint matching is considered one of the most reliable techniques of people identification. A fingerprint consists of valleys and ridges, as shown in Figure 1.

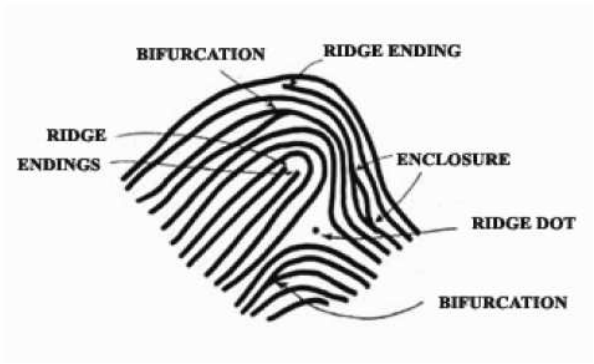


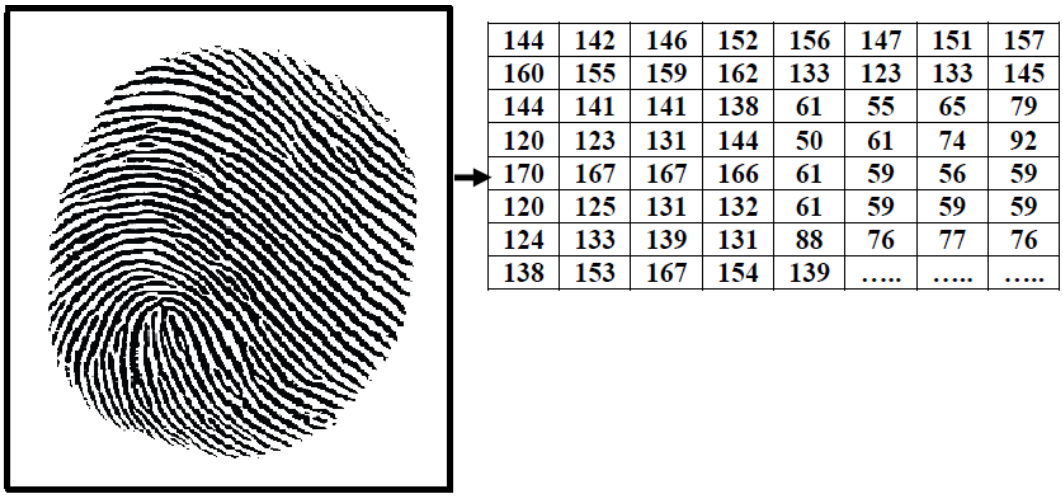
Figure 1 Minutiae image [2].

A biometric system is a suitable way to authenticate users to use ID card and it is operates by getting biometric data from a person, extracting a feature set from the acquired data, and comparing this data with information stored in the database [3]. 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. This biometric key is generated from biometric keys algorithm. Each biometric feature will generate its own key [1]. These keys are combined with certain fingerprint to give biometric key. In this paper, an algorithm is proposed with which the biometric keys can be processed to generate cryptographic key for suitable encryption procedures.

3. Information Hiding

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 value of the image pixel [4].There are two types of LSB based on image format (8-bit, 24-bit) [5,6]. 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 24-bit fingerprint-image in gray format, as shown in figure 2.
- Preform dec2bin conversion (Decimal to Binary) for fingerprint-image,
- Let the first RGB pixel of face-image is [11011111 11000110 10000111],
- Let the first gray pixel of fingerprint image 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].



144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	79
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	…..	…..	…..

Figure 2. Finger print reading procedure.

4. Proposed Methodology

This section presents the proposed algorithm with a brief introduction. The general biometric process is shown in figure 3. The proposed biometric password algorithm is shown in Figure 4. The algorithm is as the follow:The algorithm is shown below:

%% Select "person Image" and "finger image".

```
[FileName,PathName] = uigetfile({'*.jpg';'*.png';'*.gif';'*.bmp'},'Select "Canvas Image" to Hide finger image.');
img = imread( strcat(PathName,FileName) );
```

- Read the finger image,

```
% Read image (image) File
[FileName,PathName]=uigetfile({'*.jpg';'*.png';'*.gif';'*.bmp'},'Select IMAGE MESSAGE.');
msg = imread( strcat(PathName,FileName) );
```

- 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.

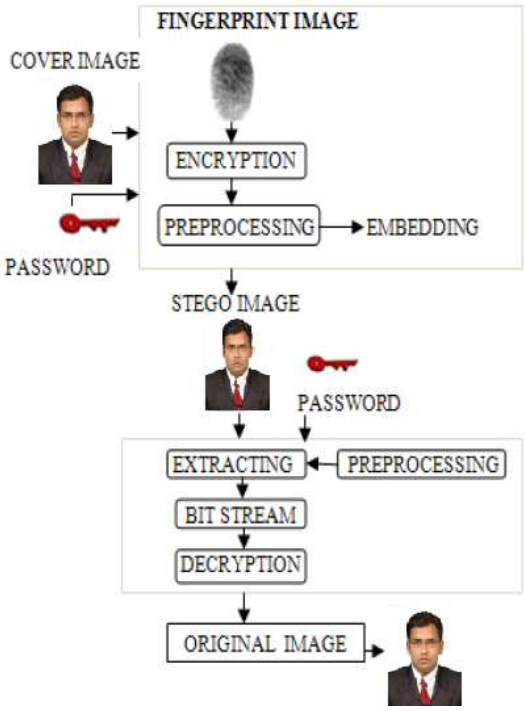


Figure 3. General Process of Biometric Encryption [2].

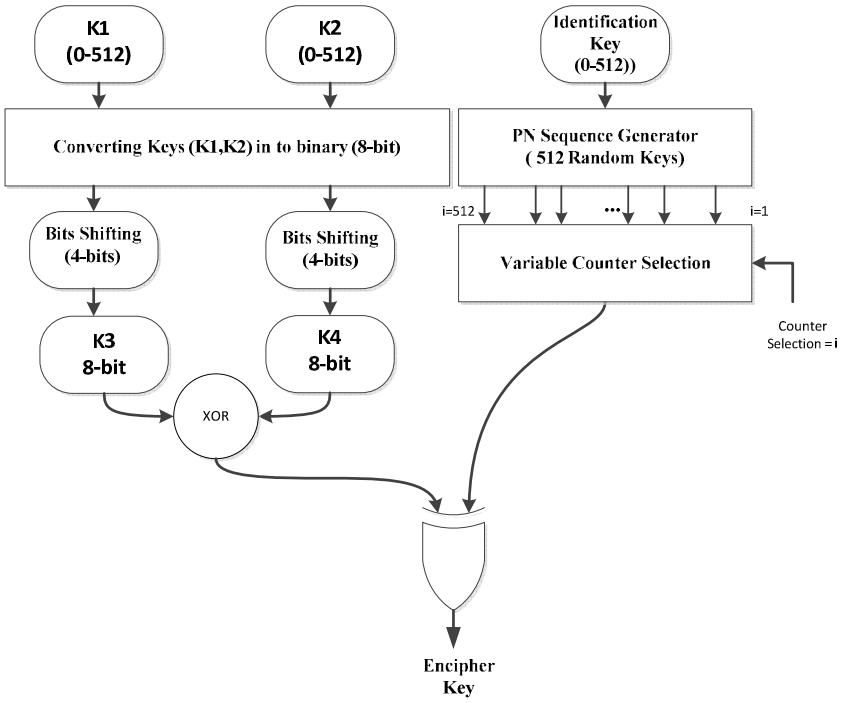


Figure 4 Biometric encipher-key (password) algorithm.

5. Simulation Results and Discussion

The proposed algorithm has been implemented in the working platform of MATLAB (version 8.1).In this paper, a 256 × 256 size image is used for cover image (person) and 128 × 128 size image is used for fingerprint image. 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 [7,8]:

$$PSNR = 10Log_{10}\left(255^2 / MSE\right) \quad (1)$$

where MSE: Mean-Square error and is given by Eqn.2 [9].

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

The PSNR value is 44 dB for original and stego images. A comparison between original image, biometric image and LSB embedded image is shown in Figure 5. After seeing Figure 5 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 1 by using Matlab.

Table 1. The final result of measurements.

Mean Square Error	*Peak Signal to Noise Ratio*	*MNormalized Cross-Correlation*	*Average Difference*	*Maximum Difference*
2.7110	44 dB	0.9994	0.0387	16

(a) (b) (c)

Figure 5 (a) Person I/P image, (b) Fingerprint,(c) LSB O/P image.

6. Conclusion and Future Work

In this paper, biometrics key which are generated from fingerprint and password are combined using an effective algorithm. 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, our algorithm can be applied on different types of sources (audio, video and Text).

7. References

1. P. Muthu Kannan andAnupriya Asthana.(2012).“Secured Encryption Algorithm for Two Factor Biometric Keys”, International Journal of Latest Research in Science and Technology, Vol.1, No.2, PP.102-105.
2. S.Brindha and Ia.Vennila. (2011).“Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart card based Authentication system”,International Journal of Computer Applications, Vol. 26, No.10.
3. N. Zehra and M. Sharma.(2010).“Bio-authentication based secure transmission system using steganography”, International Journal of Computer Science and Information Security (IJCSIS), Vol.8, No.1.
4. B.S Champakamala, K. Padmini and D. K Radhika. (2014).“Least Significant Bit algorithm for image steganography”, International Journal of Advance Computer Technology, Vol.3, No.4.

5. M. K. Meena, S. Kumar and N. Gupta.(2011). “Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity”, International Journal of Soft Computing and Engineering (IJSCE), Vol.1, No.2.
6. G. Viji and J. Balamurugan. (2011).“LSB Steganography in Color and Grayscale Images without using the Transformation”,Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue.
7. Sh. A. Laskar and K.Hemachandran. (2012).“High Capacity data hiding using LSBSteganography and Encryption”, International Journal of Database Management Systems (IJDMS), Vol.4, No.6.
8. H. Yang, X. Sun and G. Sun. (2009).“A High-Capacity Image Data Hiding Scheme UsingAdaptive LSB Substitution”,Radio Engineering Journal, Vol.18, No.4.
9. Sh. A.Tambe1, N. P. Joshi and P.S. Topannavar. (2014).“Steganography & Biometric Security Based Online Voting System”, International Journal of Engineering Research and General Science, Vol.2, No.3.