Secure biometrics using difference expansion reversible data hiding technique

[1] Shivani Gupta and [2]Farah Shah Khan

[1,] Research Scholar, Kanpur institute of Technology, Kanpur, Uttar Pradesh, INDIA
[2] Department of Computer Science and Engineering, Kanpur institute of Technology, Kanpur, Uttar Pradesh, INDIA

E-mail: [1] nancygupta41@gmail.com

ABSTRACT

Biometrics is the branch of science which is developing and gaining popularity day by day. As with time, more and more easy and reliable technologies are permitting the use of biometrics in common life, it is becoming a vital part of our life. Except some counties, a majority of nations on the planet has got biometric passport, by not every person comprehends what data it contains, for what reason it is utilized for. Here and there individuals can't discover data about such sort of passport. This paper presents an idea of secure biometrics, using reversible data hiding technique. This paper discusses the proposed method of fingerprint embedding using difference expansion methods. Various important design parameters are derived, however these set of parameters are different for different images. In the simulation Lenna image is considered, and various size of fingerprint embedding and percentage of cover image is used is discussed. It has been found that the considered method is very effective in secure online biometric system.

Keywords: *Biometrics, fingerprint, reversible data hiding*

1. INTRODUCTION

Biometric techniques have advanced over the past years to a reliable means of authentication, which are increasingly deployed in various application domains [1-8]. The widespread use of biometrics raises crucial privacy concerns, in particular if the biometric matching process is performed at a central or untrusted server, and calls for the implementation of Privacy-Enhancing Technologies. To protect biometric identifier from intrusive actions various security methods are proposed, most of these methods are based on the steganography, watermarking and cryptography. Reversible data hiding using room before and after encryption is also proposed where hidden data can be recovered without any loss.

In this paper, we propose a secure biometric system for online application. Here raw or processed fingerprint image is embedded in a cover image. In this process, on the chosen cover image using difference expansion method fingerprint data or fingerprint image is inserted and thereafter image is encrypted using cipher keys. Now the encrypted image is transmitted to the internet and on the other side, the information is first decrypted and using DE bit recovery mechanism error free information is received by the receiver [6-9]. For this data transfer, any secure network like GPS/GPRS or fiber optic networks etc. can be used. It is noticeable that size of chosen cover image should be sufficiently high which can embed both data and location map bits. The below mention Difference Expansion method can be applied to any of the above network.

For the encryption and secure data hiding Tian's Difference Expansion (DE) scheme [10] is considered. The DE scheme allows error free recovery of data with significantly high PSNR and embedding rates.

2. DIFFERENCE EXPANSION SCHEME (DE)

In difference expansion scheme, first image is divided into pair of pixels, and then one bit information is embedded into allowed pairs. The information will only be embedded into those pairs of pixels which are expandable and do not cause over and underflow. If the pixels values cross the range (0,255) then we call it over and underflow. Therefore, a location map, which is an indicator of whether, a pair of pixels is embeddable or not, is constructed in the embedding process. Finally, the location map is compressed, concatenated with the payload, and then embedded into the image. The DE scheme described below:

For a pixel pair (x_0 ; x_1), characterize their integer mean and difference as

$$l = \lfloor (x_0 + x_1) / 2 \rfloor \text{ and } h = x_1 - x_0 . \qquad (1)$$

With the end goal to embed one bit $m \in \{0,1\}$, the pixel difference h is expanded to $\tilde{h} = 2h + m$, and the marked pixel pair (y_0 ; y_1) is found out as $y_0 = l - \lfloor \tilde{h} / 2 \rfloor$ and $y_1 = l + \lfloor \tilde{h} + 1 / 2 \rfloor$. Using above relations, we have

$$\begin{cases} y_0 = 2x_0 - \lceil (x_0 + x_1) / 2 \rceil \\ y_1 = 2x_1 - \lceil (x_0 + x_1) / 2 \rceil + m \end{cases} \qquad (2)$$

Now, in this state, the decoder is able to find out the embedded bit m as the LSB of $y_1 - y_0$, and can make recovery of the real pixel pair (x_0 ; x_1) as $x_0 = l' - \lfloor h'/2 \rfloor$ and $x_1 = l' + \lfloor h'/2 \rfloor$ where $l' = \lfloor (y_0 + y_1) / 2 \rfloor$ and $h' = \lfloor (y_0 - y_1) / 2 \rfloor$.

As the pixel values are in the range $0 \le y_0 , y_1 \le 255$. Then we have

$0 \le l + \left\lfloor \frac{h+1}{2} \right\rfloor \le 255$ and $0 \le l - \left\lfloor \frac{h}{2} \right\rfloor \le 255$. Or in other words $|h| \le 2(255 - l)$ and $|h| \le 2l + 1$

The above condition can be combined together and can be re-written as

$$\begin{cases} |h| \le 2l+1 & if \;\; 128 \le l \le 255 \\ |h| \le 2(255-l) & if \;\; 0 \le l \le 127 \end{cases} \tag{3}$$

The expandable difference after embedding bit *b* in *h* after DE is defined as

$$h' = 2 \times h + b \tag{4}$$

The overflow and underflow can be avoided if expandable difference h' satisfies

$$|h'| = 2 \times h + b \le \min(2(255-l),(2l+1)) \tag{5}$$

For both *b*=0 or1.

The new expandable difference can be written as

$$h' = 2 \times \left\lfloor \frac{h'}{2} \right\rfloor + LSB(h') \tag{6}$$

With $LSB(h')$ =0 or 1.

In case of modified LSB,

$$g = 2 \times \left\lfloor \frac{h'}{2} \right\rfloor + b' \tag{7}$$

With b' =0 or 1.

$$|g| = 2 \times h + b' \le \min(2(255-l),(2l+1)) \tag{8}$$

Example

Next we describe DE method using an example as shown in Figure 1.

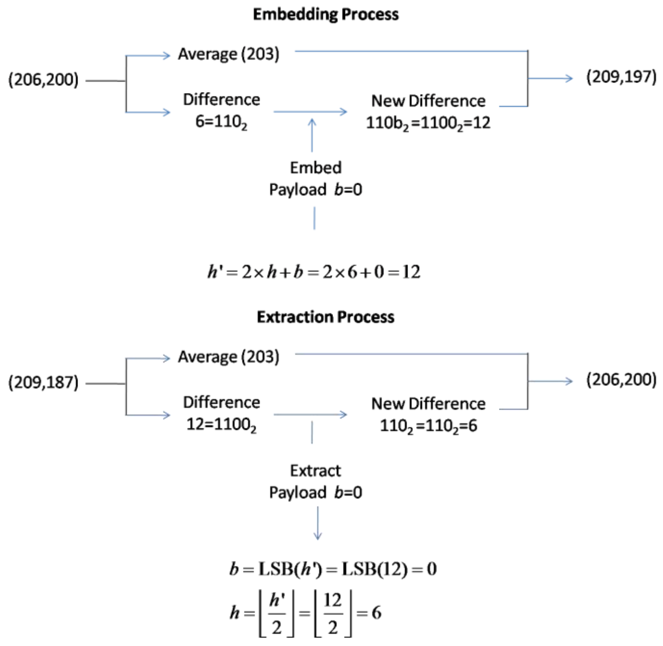

Figure 1: (a) Embedding process (b) Extraction process

Thus, LSB could be modified without resulting in the underflow and overflow. To restore the original cover and extract data decoder needs to know the difference values where information is embedded, to facilitate this, location map which contain information regarding expandable difference is also included at the time of encryption [10].

Before embedding, per-processing of fingerprint is done as discussed in previous paper. However for embedding any stage image can be used. As early image we transfer more time will be required at the receiver. However, the most efficient scheme at the receiver is shown Figure 2. Here, from the captured fingerprint image minutia points are selected and from these minutiae map is created and finally this information is converted into data stream.

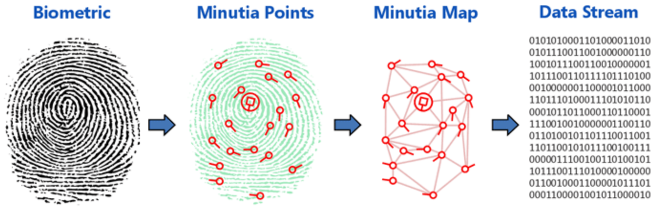

Figure 2: (a) Embedding process (b) Extraction process

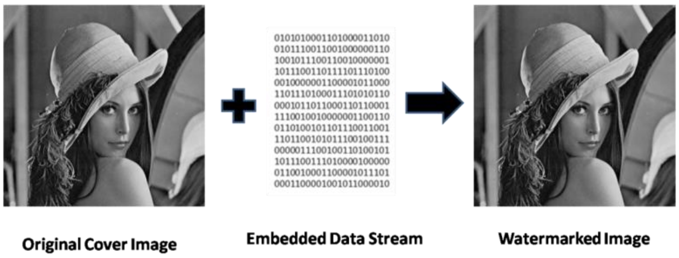

Figure 3: (a) Original Cover Image (b) Embedded Data Stream (c) Watermark Image

In Figure 3, (a) Original Cover Image (b) Embedded Data Stream (c) Watermark Image is shown. It is clear that our human vision system fail to identify difference between original and watermarked image.

Requirements:

1. The size of cover image should be more than the size of imbedded image, so can be embedded without any error.

2. Data should be able to recover without any error.

However, in full image embedding a large size cover image is desirable, to avoid this data stream of minutia map can only be embedded and at the time of verification/authentication only this information is desirable

General Rule for Cover Sizing

In both cover as well as in embedding images, intensity value varies from 0 to 255. Thus a total of 256=2^8 values and to represent them 8 bits will be required. Let the size of embedding image is *m*×*n*, therefore number of bits to represents the embedding image is 8×*m*×*n*. As in the cover image each LSB is attached with single bit therefore least size of cover image is 8×*m*×*n*.

Thresholding also plays an important role in data embedding. If any two pixels difference is greater than threshold i.e., $p_{i,j} - p_{m.n} > T$, than embedding will be performed. If difference is more, than more embedding is possible, but PSNR will be lower. In above, $p_{i,j} \in [0,255]$, $p_{m,n} \in [0,255]$ and T is threshold.

If thresholding is used than the minimum cover image size is given by

$$S_c = 8 \times m \times n \left(\frac{255}{255 - T} \right) \quad (9)$$

Moreover some extra bits are also need for location map. Let size of location map is a×b, than total size of cover image is

$$S_c = 8 \times m \times n \left(\frac{255}{255 - T} \right) + a \times b \quad (10)$$

Roughly it can deduce that the size of cover image should be at-least 10 times of embedded image. However, while inserting location minutia map information size of embedded data reduces significantly, and thus size of cover image also reduces.

Selection of DE parameters

In Figure 4, PSNR (dB) vs. threshold is shown, here as the threshold increases, PSNR (dB) decreases. This can be explained as under, more embedding will lead to the difference in original and watermarked image, and thus pixel difference will increase. This difference in both the images, increases MSE and in turn PSNR decreases.

3. RESULTS

In Figure 5, bpp vs. threshold is shown, here as the threshold increases, bpp increases. This happens because more space leads to more embedding. At the threshold of 30 the bpp is 0.58, while for threshold of 70 the bpp is 0.81.

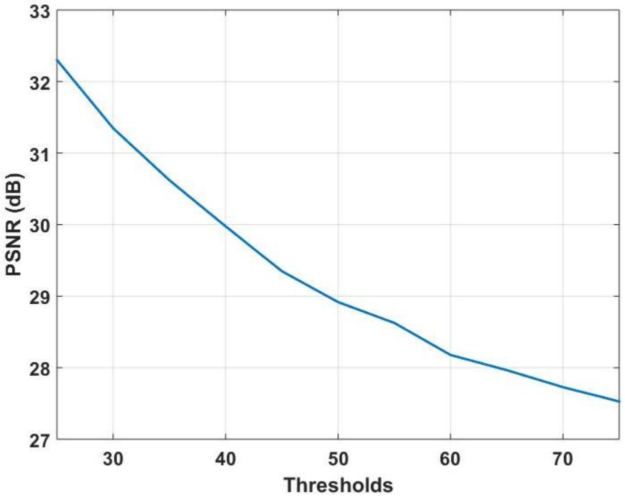

Figure 4: PSNR (dB) vs. Thresholds

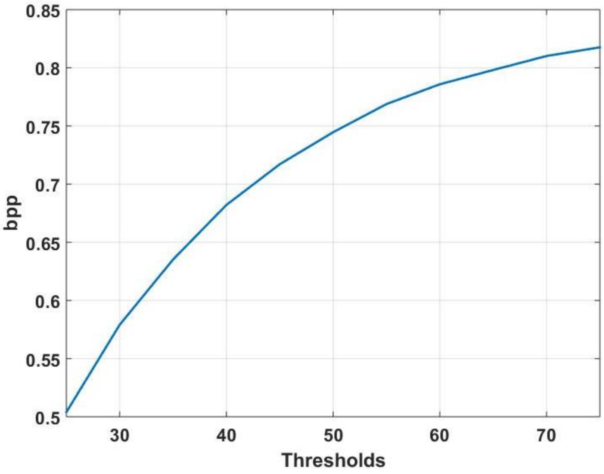

Figure 5: bpp vs. Thresholds

In Figure 6, bpp vs. PSNR (dB) is shown, here as the bpp increases, PSNR decreases. It is expected as more embedding leads to the more error, and thus PSNR increases.

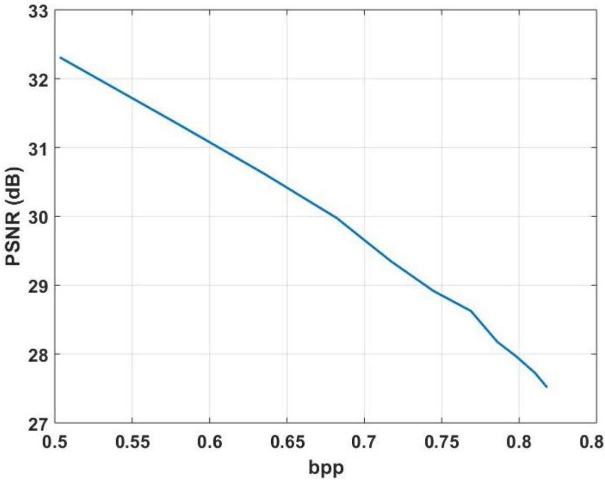

Figure 6: bpp vs. PSNR (dB)

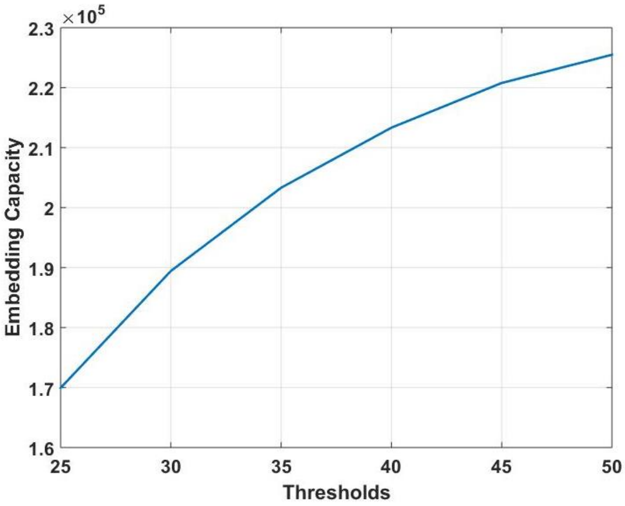

Figure 7: Thresholds vs. Embedding Capacity

In Figure 7, Thresholds vs. Embedding Capacity is shown, here as threshold increases, embedding capacity also increases.

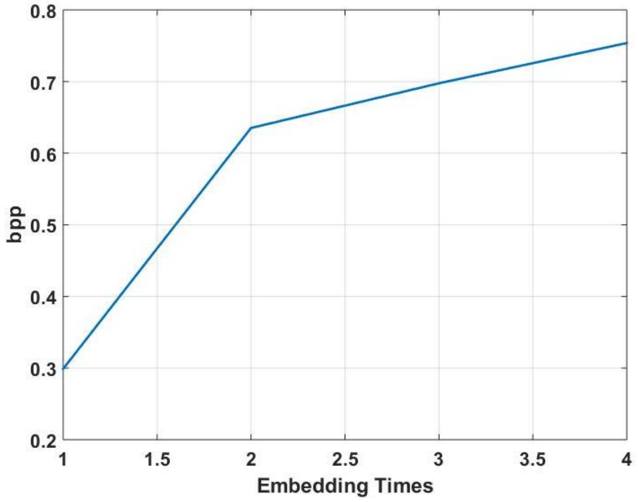

Figure 8: Embedding Times vs. bpp

In Figure 8, number of times embedding vs. bpp is shown, here as the number of times of embedding increases, bpp also increases. In Figure 9, number of times embedding vs. PSNR is shown, here as the number of times of embedding increases, PSNR decreases.

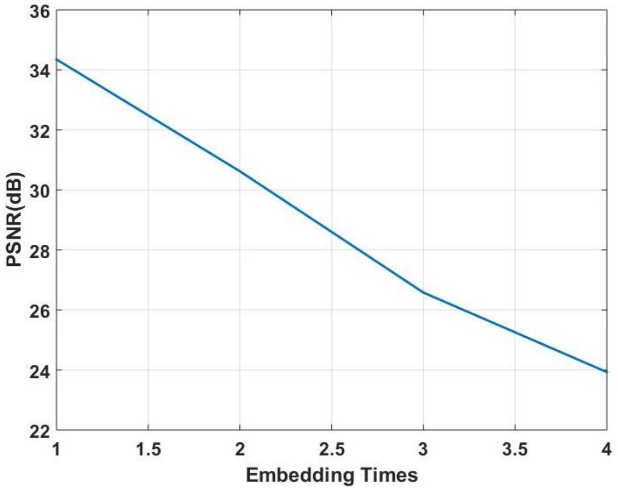

Figure 9: Embedding Times vs. PSNR

(a)

(b)

Figure 10: (a) Original Lenna Image (b) Watermarked image

The above results are obtained on Lenna image as shown in Figure 10 (a) and watermarked image is shown in Figure 10(b). The optimized parametric values are detailed in Figure 1.1.

Table 1: Optimized Parameter values

Parameters	Value
Threshold	40
PSNR	30 dB
Embedding Times	2
bpp	0.68
Capacity	2.12×10^5

We have re-sized fingerprint image and size of re-sized image is 128×128, and consider bit depth of 8.

The total size of image is 128×128×8 $=1.31\times10^5$.

Table 2: Percentage of cover image used for various size of fingerprint image

Size of Fingerprint Image	Percentage of cover image used
64×64×8	15.46%
128×128×8	61.79%
256×256×8	Cover image size is small

For larger size image other cover images or same image of larger size can be selected. However, very large size image should be avoided to avoid unnecessary delay in the transmission and network. As a thumb rule select cover image whose size is at least 10 times of embedded image.

4. CONCLUSIONS:

In this paper secure biometric data transfer mechanism is proposed which enable the security of biometric identifier over the internet. The difference expansion scheme is a reversible data hiding technique which allows error free recovery. On the basis of obtained results we conclude the followings:

1. In DE method threshold plays an important role
2. The minimum required PSNR for good quality image is of 30 dB; therefore the threshold should be fixed to 40.
3. At the threshold of 40, maximum number of allowed embedding times is two.
4. Maximum achievable bpp is 0.68.
5. The maximum capacity is of 2.12×10^5 bits.
6. The above mentioned results are for Lenna image; these results will vary with image and its size.
7. Larger size images provide better embedding capacity, but processing time will be more.
8. Therefore in real time applications, selection of cover image size is important such that the complete information can be embedded with lesser extra space.

.

REFRENCES

[1] Aleksandra Babich, “Biometric Authentication. Types of biometric identifiers,” Bachelor Thesis, Hagga Helia University, 2012.

[2] S.S. Chikkerur, “On Line Fingerprint verification”, Master’s Thesis, University at Buffalo, The State University of New York, 2005.

[3] Yu Chengpu, Xie Mei, Qi Jin, “An effective and robust fingerprint enhancement method,” IEEE International Symposium on computational Intelligence and Design, Vol.7, pp.110-113, 2008.

[4] L. Hong, “Automatic Personal Identification Using Fingerprints,” PhD Thesis, Michigan State University, 1998.

[5] Phillips, P. J.; Martin, A.; Wilson, C. L.; Przybocki, M. “An introduction to evaluating biometric systems”, Computer Vol.33, No. 2, pp.56–63, 2000.

[6] R. Thai, “Fingerprint Image Enhancement and Minutiae Extraction,” PhD Thesis Submitted to School of Computer Science and Software Engineering, 2003, University of Western Australia.

[7] J. Fridrich, M. Goljan, and R. Du. Invertible authentication. In *Proc. SPIE EI*, volume 4314 of *SPIE*, pages 197–208, 2001.

[8] T. Kalker and F. M. J. Willems, “Capacity bounds and construction for reversible data-hiding,” in *Proc. Int. Conf. DSP*, Santorini, Greece, 2002.

[9] X. Li, B. Li, B. Yang, and T. Zeng. General framework to histogram shifting based reversible data hiding. *IEEE Trans. Image processes*, 22(6):2181–2191, Jun. 2013.

[10] J. Tian. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.*, 13(8):890–896, Aug. 2003.