ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Steganographic Approach for Securing Biometric Templates

Shweta Setiya
Research Scholar(M.Tech)
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

Chander Kant
Assistant Professor
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

Abstract: Biometric systems are used for recognising a user on the basis of his biometric traits. During authentication some of the frequently asked questions are "Is he who he claims to be?", "Is he a valid user for gaining access to the system?". Biometric system answers all these questions by authenticating the users. Every second information is shared and transferred between people and it is important to make sure that what is sent by sender is what received by the receiver thus raising the demand of security. Steganography is one of the techniques used for securing the data. The secret message is hidden inside a cover media like audio, video or image with the help of a secret key. Biometric templates can also be secured with this technique. Instead of storing original templates in the database stego-image is stored. LSB is one of the common techniques that replace the LSB of every pixel of the cover image with the secret message to form stego-image.

Keywords: Biometric, Biometric Attacks, Biometric template, Security, Steganography.

I. INTRODUCTION

With increasing rate of attacks, everyone today needs a reliable and secure system. Biometric systems fulfil the needs to a great extent as biometric traits are better than passwords or pins which have chances of being stolen and forgotten. Biometric system consists of mainly four modules i.e. Sensor module, Feature extraction module, Matching module and Decision module. Before using biometric system enrolment phase is necessary during which the templates of the users are stored in the database. During authentication user's claim is matched with the templates in the database and a matching score is generated by the matching module. Then this score is compared with the pre-determined threshold. If the value is greater than or equal to the threshold value, then the user is declared as genuine otherwise the system rejects the user. If the biometric templates are stolen, they cannot be used, as it can be done with passwords or tokens [1].

Steganography is one of the techniques used for securing the biometric templates. In this technique, secret message that is biometric template here is hidden in the cover image and stego-image is formed that will get stored in the database of the system. A secret-key is used for identifying the pixels to store the secret message. Common steganographic technique is the LSB in which the secret message is embedded in the LSB of the cover image. Distortion created is so small that human eye is unable to discover the presence of the secret message. Many message hiding techniques have been developed by the researchers using audio files, text files, images, or other Medias [2].

II. PROBLEM STATEMENT

Attacks on the system

Biometric systems are vulnerable to many attacks including replay, correlation, hill-climbing and brute-force attacks [3] as shown in Fig. 1.

A. Fake Biometric

Biometric system consists of various modules. Sensor module is used to capture the biometric traits of the user in form of image, audio, video or some other form [5]. Attacker can provide fake biometric here like artificial finger and can gain access to the system.

B. Replay Old Data

Attacker can act as man-in-the-middle on the communication channel between sensor and feature extractor module and illegally captures the data or the trait. This captured data is then presented at the sensor module to fool it.

C. Override Feature Extractor

The second module is the feature extractor that is used to extracts the features out of the biometric traits like minutiae in case of fingerprint. During enrolment these extracted features called templates are stored in the database of the system. Attacker can replace this module with his own program like Trojan horse that will generate features sets of his own instead those generated by the original data captured by the sensor.

D. Synthesized Feature Vector

Features extracted by the feature extractor module are sent to the matching module through a communication channel where an attacker can sit and capture the feature set values. These captured feature set values can be sent to the matching module later.

E. Override Matcher

Third module is the matcher module that generates the matching scores on the basis of which the user is declared as genuine or not. Attacker can override this module with Trojan horse program that will produce high or low scores according to the wish of the attacker.

F. Modify Templates

Templates of the users are stored in the database that is most crucial part of the system being attacked most of the times. Attacker can modify the stored templates, remove the templates or can replace them with other templates.

G. Intercept the Channel

The communication channel between the stored templates and the matcher module is hacked here by the attacker. He can now steal or modify the templates.

H. Override Final Decision

Attacker can change the final decision of the biometric system by sitting at the channel between the matcher module and the user application. This final decision can declare a fraud user as genuine user when intercepted by the attacker.

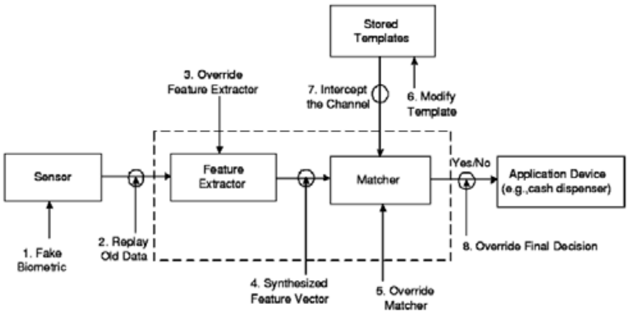

Figure 1. Vulnerabilities in a Biometric System [4]

These eight points shows the vulnerabilities of the biometric system. Attacks can be avoided by using template protection schemes like watermarking, cryptography and steganography. A large amount of data is being stored on computers and is transmitted over network thus the need of steganography has entered the digital age. The word steganography is combination of two words-“steganos” meaning “covered, concealed or protected” and “graphie” meaning “writing”. Steganography is the art of concealing a message, file, image or video with another message, file, image or video such that no one else knows the existence of the message other than the authorized users. It hides the message from the third party.

Computers treat image as an array of numbers and the location and value of that number is called pixel [6]. 8-bit or greyscale images and 24-bit or digital colour images are typically used for steganography. Both have their advantages and disadvantages [7]. Advantage of 8-bit image is its flexibility when used for steganography. Large amount of data can be hidden in 24-bit images as opposed to 8-bit images. Due to only 256 possible colours available in 8-bit images, it becomes a potential problem during encoding. Problem with 24-bit images is their larger size that makes them more suspect when sent over internet.

The components involved in the steganography technique are:-

- Carrier image, the image in which we have to embed our secret message.
- The message, which is the secret message to be hidden inside the carrier image.
- The key, which determines the pixel values to be used for embedding and extracting process.

III. TECHNIQUES OF STEGANOGRAPHY

A. Spatial Domain Technique

These techniques directly change some bits in image pixel values during embedding of secret message. The secret bits are written directly to the cover image pixel bytes [8]. Among various spatial domain techniques, Least Significant Bit (LSB) is one of the widely used techniques. It is the simplest technique that embeds the secret message in the LSB of pixel values without introducing much distortion. Stego-image and carrier-image both looks identical to human eyes. Classification of spatial domain techniques- [9]

- Least significant bit (LSB)
- Pixel value differencing (PVD)
- Edges based data embedding method (EBE)
- Random pixel embedding method (RPE)
- Mapping pixel to hidden data method
- Labelling or connectivity method
- Pixel intensity based method
- Texture based method
- Histogram shifting methods

1) *Least Significant Bit Encoding:* it is the most popular and simple technique. It encodes the message in LSB of every byte of image. Thus, value of each pixel is slightly changed but not enough to be noticed by the human eyes. It is easy to hide information inside high resolution and high quality image i.e. 24 bit BMP (bitmap) image. 8-bit BMP’s or another format images like GIF may also be used. 24-bit image is derived from three basic colours i.e. red, green and blue. Each of these primary colours is represented by 8 bits making pixel 3 bytes long. One can store 3 bits in each pixel by changing LSB of each red, green and blue component but in 8-bit images only 1-bit per pixel can be used for hiding secret message.

Suppose that we have 3 adjacent pixels (9 bytes) with RGB encoding [10]

10010101 01010100 11001001
10010110 01101111 11001011
10000111 00011100 11001011

We will embed the number 500, whose binary representation is 111110100 over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 0101010**1** 11001001
1001011**1** 01101111 1100101**0**
10000111 00011100 1100101**0**

Here the number 500 was embedded into the image, only 4 bits are changed in the stego image. Thus, only half of the bits in an image get modified during hiding a secret message. These changes cannot be identify by the human eye, thus the message is successfully hidden in image.

B. Transform Domain Technique

Here the message is embedded in the frequency domain of the carrier image. Embedding data in the frequency domain of an image is much stronger than embedding principles that operate in the time domain. These methods of image enhancement consist of computing a 2-D discrete unitary transform of image, for instance 2-D DFT [11]. The orthogonal transform of the image consists of two components- magnitude or the frequency part and phase. The phase component restores the image back to the spatial domain. The usual transform domain enables operation on the frequency content of the image, and therefore high frequency content such as edges and other subtle information can easily be enhanced.[3] Transform domain techniques are broadly classified into:

- Discrete Fourier transformation (DFT).
- Discrete cosine transformation (DCT).
- Discrete Wavelet transformation (DWT).

1) Discrete Wavelet Transform: Discrete wavelet transform is a method used for decomposing an image as shown in Fig. 2. The transform is based on small waves, called wavelets, of varying frequency and limited duration. [11] It splits an image into different frequency bands i.e., low, medium and high thus offering multi-resolution representation of image. The low frequency part is also called approximation because it contains almost all information about the image while the high frequency part has information about edge component only. [12]

2) Discrete Cosine Transform: - The basic purpose of it is to take a signal and transform its representation from one form to another. For example, an image is a 2-D signal perceived by human eyes. The DCT converts the signal into numeric data (frequency). It helps separate the image into parts of differing importance. The DCT is same as Discrete Fourier Transform (DFT): it transforms an image from the spatial domain to the frequency domain. The basic purpose of DCT is to identify the “piece of information” that is not perceivable by the human eye or can be thrown away or discarded without affecting the quality of image.

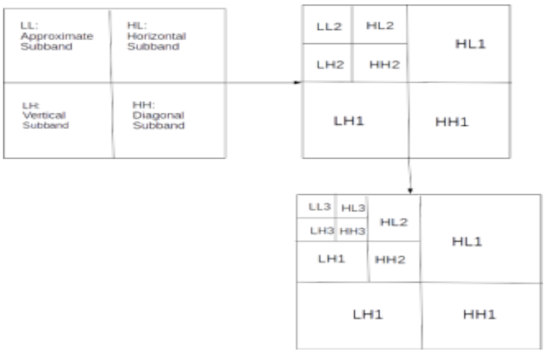

Figure 2. 3-level Discrete Wavelet Transform

IV. TYPES OF STEGANOGRAPHY PROTOCOLS

Three types of steganography protocols are there: [7]

- Pure steganography
- Secret key steganography
- Public key steganography

In pure steganography, no exchange of secret key is required. Sender and receiver assume that no third party will be aware of secret message. Thus, it is least secure type of protocol.

Secret key steganography requires the exchange of secret key between two communicating parties prior to communication. Secret message is embedded into the cover message with the help of secret key. This protocol is more susceptible to interception. But if the secret message is intercepted, it will be of no use to the third party as only the communicating parties knows how to extract the secret message with the help of secret key.

Public key steganography is similar to public key cryptography that uses pair of public and private key for secure communication between two parties. Encoding of message is done with public key and private key is used for extracting the secret message.

V. RELATED WORK

Sudhanshi Sharma et.al. [7] have explained transform domain techniques of steganography i.e. DWT and DCT. Separate algorithms for both the techniques are given. Comparison of both the techniques has been done on the basis of PSNR and MSE. It has been shown that PSNR of DCT is higher than DWT techniques which show that the quality of image in DCT is best. While DWT method is more robust as it extracts the secret message from the cover image without destroying it.

Rubal Jain et.al. [9] proposed a new LSB algorithm of steganography that is enhancement of existing LSB method. Instead of using a separate secret key for choosing the pixel positions for embedding secret message, XORing of MSB of each RGB channel has been done. On the basis of the XOR operation the LSB's for embedding the secret message are decided. This enhanced LSB algorithm has prevented the system from the malicious attacks caused by the intruders.

Shilpa Gupta et.al.[6] proposed a new method for steganography by analysing the existing least significant bit algorithm. In this novel approach only the blue component of the pixels has been chosen for embedding the secret data which results in minimum distortion of the carrier image. Comparative results of standard and the new LSB method are also provided.

Bret Dunbar has provided a detailed look at the steganography technique. Brief history of steganography as well as steganographic protocols: pure steganography, secret key steganography and public steganography are also explained. Encoding of secret messages in audio, text and images have been explained.

Chander Kant et.al.[4] explained various possible attacks on the biometric system. Description about modules of the biometric system has also been given. To enhance the template security steganography technique has been used. Secret message is embedded in the LSB of the cover image by avoiding the boundary values as change in pixel values there will be +2 or -2 .

Joseph Mwema et.al.[2] have discussed various possible biometric system attacks and threats. They have classified the biometric template protection schemes into two types i.e. feature transformation and biometric encryption. These techniques are further classified into many types each of which is used to secure the biometric templates. They have concluded that no particular biometric template protection scheme is satisfactory in all aspects.

VI. PROPOSED WORK

The proposed system increases the security of the biometric system by embedding the biometric templates in the cover image and storing the stego-image in the database instead of storing then template. The proposed model is shown in fig.3 which illustrates the enrolment as well as the authentication process using steganography. Enhancement of standard LSB algorithm is used for hiding the templates. With this approach the privacy, integrity and confidentiality of the biometric data has been achieved.

Working

1. During enrolment, the sensor is used to acquire the biometric trait of the user. Trait could be fingerprint, face, retina, iris etc.

2. Pre-processing of the image captured by the sensor is required including enhancement, normalisation, binarisation. denoising etc.

3. The feature extractor module will extract the necessary features from the traits like minutiae in case of fingerprint.

4. The template has to be converted into its binary equivalent for embedding process.

5. Cover image is chosen of size larger than that of the size of the template.

6. Cover image is of RGB format i.e. it contains 24-bits per pixel. Convert the cover image also in the binary format.

7. After making the formats of the cover image and the template compatible, embedding is done with the help of the steps given in the embedding process of the proposed LSB algorithm. Stego-image is generated at the end of embedding process. All these steps are performed at the sender side.

8. The stego-image generated in the above step is sent at the receiver side where the template is extracted from the stego-image with the help of steps described in the extraction process of the proposed LSB algorithm.

Proposed LSB algorithm

Existing standard LSB algorithm embeds the secret message in the LSB of the pixels determined with the help of the secret key but the proposed algorithm makes use of the MSB bit to determine the pixel positions for embedding the secret message. Thus no separate secret key is required. This LSB algorithm works in the spatial domain. It increases the performance by hiding biometric template in any one or two of the colours rather than choosing all the three colours to hide the data [13]. By choosing one or two of the colours the distortion in the stego image will be less. Fig. 3 describes the approach used for embedding.

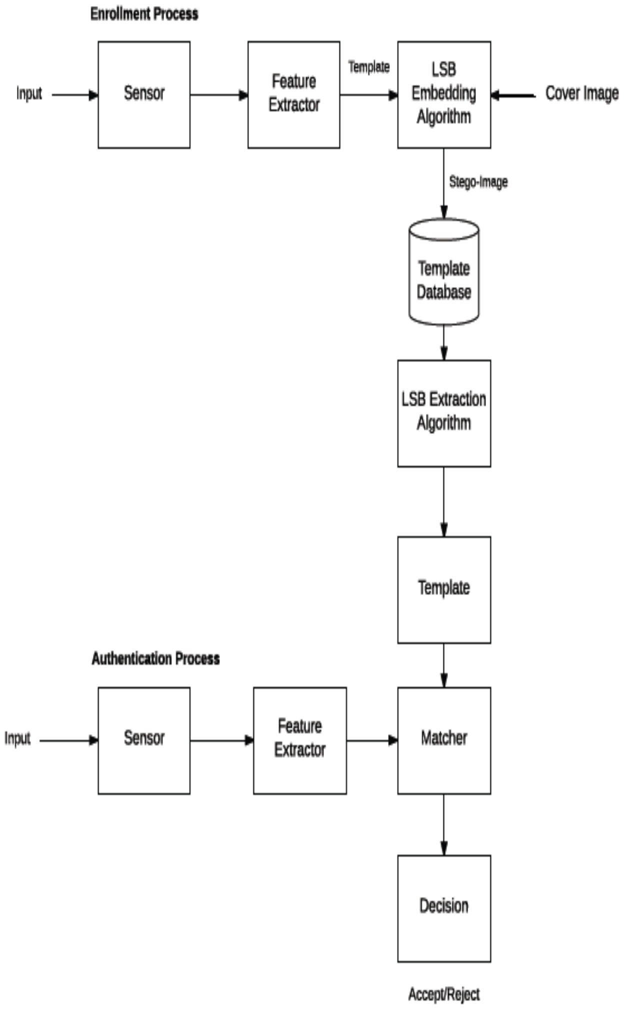

Figure 3. Architecture of Proposed Work

Embedding technique

Fig. 4 shows the data embedding approach. Following are the steps involved in the embedding technique.

1. Take the cover image and convert it into binary format, denoting number of pixels p0,p1......pn.

2. Take the biometric template to be embedded in the cover image and convert it into binary format.

3. Divide the template in blocks of 4 bits denoting by b1,b2.......bm.(if bits of template are not multiple of 4 then apply padding in last block)

4. For embedding, initialize PIX=1 and BLOCK=1.

Here, PIX stands for pixel number and BLOCK stands for block number

```
5. For PIX = 1 to n
   {
     for BLOCK = 1 to m
       {
         if (value of MSB of R and B == 00)
         then embed all 4 bits in the LSB of green channel
         if (value of MSB of R and B == 01)
         then embed all 4 bits in the LSB of blue channel
         if (value of MSB of R and B == 10)
         then embed all 4 bits in the LSB of red channel
         if (value of MSB of R and B == 11)
         then embed 2 bits in the LSB of red channel and 2 bits in LSB of blue channel.
       }
   }
```

6. Resultant image is known as stego image.

Extraction technique

1. Read the stego-image.

2. Check the value of MSB of Red and Blue channel starting from 1st pixel i.e. PIX=1. Value could be 00,01,10,11. Depending on this value, MSB of corresponding channel will be the pixel value of 1st Block (BLOCK=1).

3. Repeat step 2 for PIX=1 to n

4. Now the template is retrieved in binary form. Convert it into decimal form so that authentication process can proceed.

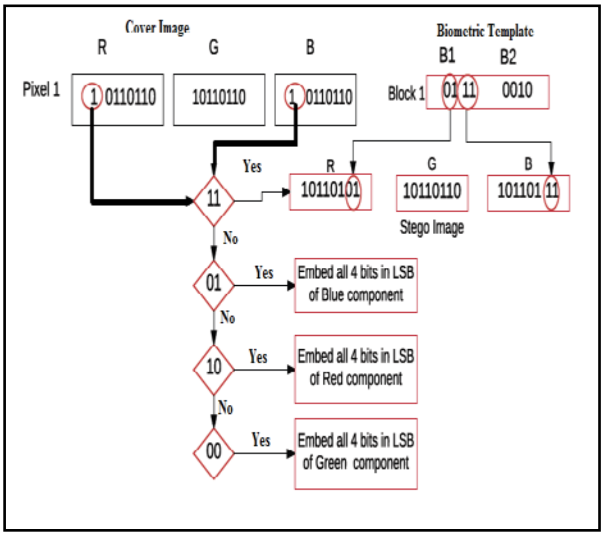

Figure 4. Data Embedding Approach

VII. Results

Let us consider a pixel of the cover image with the RGB (Red- Green-Blue code) colour B6B6B6 whose binary is 10110110-10110110- 10110110 to hide the secret message 1100. MSB of red and blue channel will be checked. Here in this example, the value of MSB of red and blue are 11. Thus 2 bits of secret message will be embedded in the LSB of Red channel and 2 bits in LSB of Blue channel. The stego-image that will be generated after embedding process is 101101**11**-10110110-101101**00**).

The proposed technique will introduce less distortion as either LSB of one channel or any two channels will be changed thus enhancing the efficiency of the method.

TABLE I. RESULT OF THE PROPOSED METHOD

	Hexadecimal	*Decimal*	*Red*	*Green*	*Blue*
Original Pixel	B6B6B6	10110110 10110110 10110110	192	192	192

Modified Pixel	B7B6B4	10110111 10110110 10110100	193	192	190

VIII. CONCLUSION AND FUTURE SCOPE

To enhance the security of the biometric system, a new steganographic approach is proposed that uses the MSB bits of the RGB component to embed the template in the cover image. MSB will act as the secret key thus avoiding the need of remembering separate secret key. MSB of only two components is used as secret key. The proposed technique is better as it generates less distortion in the stego-image which is negligent for human eyes. Future works should aim to achieve better performance by hiding secret message in such a way that steg-analysis should be unable to detect it as well as it should be undetectable by human eyes also.

IX. REFERENCES

[1] . V.P. Pawar Ms. C.B. Tatepamulwar, "Comparison of Biometric Trends Based on Different Criteria," *Asian Journal of Management Sciences*, vol. 2, no. 3, pp. 159-165, 2014.

[2] Murugan and Deepu V. Krishnan R. Rejani, "Pixel Pattern Based Steganography on Images," *ICTACT Journal On Image And Video Processing*, vol. 5, no. 3, pp. 991-997, February 2015.

[3] chael Kimwele, Stephen Kimani Joseph Mwema, "A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates," *International Journal of Computer Trends and*

chnology, no. 2231-2803.

[4] M. Boll, N. Ratha J.H. Connell, "An Analysis of Minutiae Matching Strength," *Audio and Video Based Biometric Person Authentication* , pp. 223-228, June 2001.

[5] jender Nath, Sheetal Chaudhary Chander Kant, "Biometrics Security using Steganography," *International Journal of Security*, vol. 2, no. 1, pp. 1-5, Feb 2008.

[6] ssilawati Sulaiman Mohammed Abdul Majeed, "An Improved LSB Image Steganography Technique Using Bit Inverse in 24 Bit Colour Image," *Journal of Theoretical and Applied Information Technology*, vol. 80, no. 2, pp. 342

3, October 2015.

[7] et Dunbar, "A detailed look at Steganographic Techniques and their use in an Open-Systems," SANS Institute InfoSec

ading Room, 2002.

[8] dmini.K, Radhika.D. K Champakamala.B.S, "Least Significant Bit algorithm for image steganography," *International Journal of Advanced Computer Technology (IJACT)*, vol. 3, no. 4, pp. 34-38.

[9] ehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques," *International Journal of Advanced Science and Technology*, vol. 54, pp. 113-124, May 2013.

[10] eta Gujral, Neha Aggarwal Shilpa Gupta, "Enhanced Least Significant Bit algorithm For Image Steganography," *International Journal of Computational Engineering & Management*, vol. 15, no. 4, July 2012.

[11] nesh Kumar Sudhanshi Sharma, "Review of Transform Domain Techniques for Image Steganography," *International Journal of Science and Research (IJSR)*, vol. 4, no. 5, pp. 194-197, May 2015.

[12] ander Kant Shweta Setiya, "Watermarking: A Technique For Securing Biometric Template," in *National Conference on Recent Innovations in Electronics, Electrical and Computer Science and Engineering* , Baddi, 2016.

[13] ander Kant Rubal Jain, "A Novel Approach for Securing Fingerprint Template using Steganography," *International Journal of Innovations & Advancement in Computer Science*, vol. 4, no. 6, pp. 17-24, June 2015.