Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Novel Approach to Secure Biometric Template with Steganography

Sukhdev Singh
Research Scholar, Department of Comp Sci & Applications
Kurukshetra University, Kurukshetra, Haryana, India

Chander Kant
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra, Haryana, India

Abstract: Security is a major concern in today's modern era because the frauds are increasing day by day. Biometric systems are used for security applications to access the control in many fields. Biometric systems, like all systems have vulnerabilities. Many attacks are possible on biometric templates also, to secure it from these attacks a novel approach is presented to make biometric template more secure by using steganography technique. Steganography is an art and science of embedding or hiding data in an image. In this paper, we have used the steganography technique for embedding the biometric template bits into a cover image. Cover image is divided into blocks of equal size and then converted biometric template into bit form and it is embedded into the central pixel of the block using cyclic combination method (CCM) steganography. It provides the more security to the biometric template with minimum deficiency in cover image that cannot be perceived by human eye.

Keywords: Biometric, Steganography, Pseudo Random Number Generator, Cover Image, Stego-image.

I. INTRODUCTION

Biometric deals with our physical as well as behavioral characteristics for recognition and authentication. Security is an application which associates with biometric as identification to access the control. Iris, fingerprint, finger knuckle print, hand geometry, palm print, face, voice, and gait are mostly used for authenticate the identity of a person [1]. Today Biometric identification system has several advantages over the password, pin and tokens methods. Because biometric concept use the physical or behavioral trait of human being, so physical presence is mandatory to access the control. On the basis of biometric function, this system can be classified into two categories: i) identification system which is known as one to many relationships that can identify a person's identification and ii) verification system known as one to one relationship that can be used to verify the identity of someone. Biometrics system has three phase of its operations first phase processing is capture the image of biometric trait (e.g. finger knuckle print, iris) for identity with the help of scanner or video camera. Second phase of processing is to extract the feature from image of trait which is unique with individual human being. Next phase is enrollment; the feature extraction phase operates on the biometric signal and extracts a relevant set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. Template security is very essential in biometrics system; once the biometrics template has been compromised it cannot be revoked or reissued for authentication. Attacks, unauthorized access of the biometric template in biometric systems have greater issues. Ratha et al [2] proposed the various attacks on the biometric systems. Fig 1. show various attacks that are possible on biometric systems. Ratha classified the biometric system attack as follows:

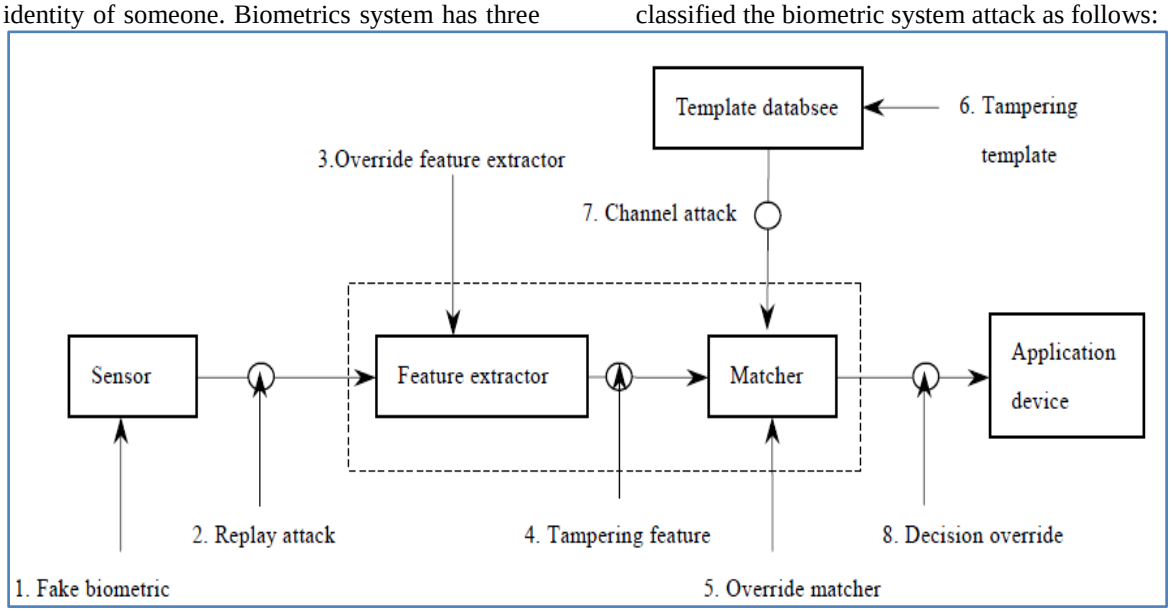

Figure 1: Attacks on Biometric System

1. **Attack at Sensor:** In this type of attack the attackers physically destroy the recognition scanner and can represent the artificial template at the sensor.
2. **Replay Attack:** In this the attackers attacks on communication channel between the scanner and the feature extractor. It includes the resubmission of digitally stores biometric data. After scanning the biometric trait it will send to the feature extractor module for processing at that time attacker replace the biometric traits.
3. **Override Feature Extractor:** In this type of attack feature extractor could produce the feature values chosen by the attackers not the data that is obtain from the sensor.
4. **Tampering Feature:** In this type of attack commutation channels between the feature extractor and the matcher is intercepted. A synthetic feature set is used to replace the data that is obtained from the sensor.
5. **Override Matcher:** In this attack matcher is replace with the Trojan horse by attackers and matcher will always produce the high matching score and allow application to pass the biometric authentication mechanism.
6. **Tampering Template:** In this type of attack attackers compromises the security of database where the entire template is stored. The attackers can add new template, delete the template or modify the existing template.
7. **Channel Attack:** The communication channel between the database and matcher is intercepted by the attackers to alter the data.
8. **Decision Override:** In this type of attack attackers capture the channel between the matcher and the application to replay previously submitted data.

To solve these problems steganography technique used to hide the biometric template in cover image and it makes the stego-image as shown in fig. 2. Stego-image is stored in database instead of template. Using steganography technique with biometric system can enhance user convenience and increase security; it is also protected the biometric template from various types of attacks [3].

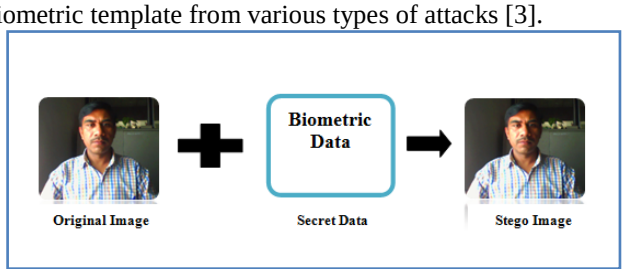

Figure 2: Simple Steganography System

Steganography is a Greek origin word meaning "Concealed Writing". It can be considered as a way to hide secret information in cover image pixels such that it cannot be detected by human visual system and nobody know about its existence without the intended sender and receiver. Three main components are carrier object, secret data and steganographic algorithm for working of steganography technique. Sometimes a secret key and cryptographic algorithm is also required in order to increase the security levels and introduce multiple barriers in the way of an attacker. Most useful applications of steganography technique are secure transmission of secret data between government of different countries, security of online voting, data security of military and intelligent agencies, in circulation of secret documents among defense organizations and online banking security. On the other hand, steganography is also very immoral; it is used by terrorists and criminals for their secure communication and sending viruses to compromise machines. [4].

This paper is organized as follows: section II presents the related works for template protection of biometric systems using different steganography schemes, section III presents the proposed approach, section IV shows the results and discussion, and finally concluding observations are given in section V.

II. RELATED WORKS

A few research works that have been done for improve the privacy and security of biometrics template using steganography technique. Related works with steganography technique have been studied which is listed below.

Uludag et al. [5] in this paper they have presented two applications of a watermarking method. The first application is related to increasing the security of biometric data exchange, which is based on steganography. In the second application they authenticate a user based on his face image, along with the fingerprint information hidden in the face image. They proposed a method to utilize several properties of the human visual system to keep the visibility of the changes made to the host image low. They also analyzed data decoding performance in the case of several attacks on host images.

Chander Kant et al. [6] in this paper they presented a new idea to make system more secure by use of steganography. They have proposed algorithm for insertion and retrieval message bit in original template. Secret key, which is in the form of pixel intensities, has merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode. Their proposed work gives 49% chances, that message bit will be inserted at pseudorandom location at first chance. 50% chance, that when message bit is inserted, no change in pixel value is required.

A. Gutub et al. [7] presents pixel indicator technique (PIT) in which one channel is used for indication while other two channels are used for embedding secret data in a predefined cycle manner which enhances the robustness of proposed method. The experimental results demonstrate the larger payload and enhanced imperceptibility of the proposed method. This method also eliminates the stego key exchange overhead. The major limitation of this technique is the fixed number of bits embedded in each gray level of the host image which may cause noticeable distortion if we increase the number of embedded bits. Furthermore, the payload of this method is absolutely dependent on the carrier image and indicator bits which may be reduced.

Arkadiusz et al. [8] in this paper they presented a novel approach to logical access control to secured repository or container by integration of methods related to cryptography, steganography and biometrics.

Bhattacharyya, Souvik, et al. [9] in this technique an image steganography process has been occurs by using a series for embedding space selection and a polynomial has been used for embedding the secret message, so that secret message bit is not embedded directly and makes difficult for steganalysis. Also for pixel selection mechanism, the

biometric features has been used which comes from both the cover and secret embedding information. From the security aspects the attack technique is very low between the cover image and stego image which have already surrender a very high security value of the hidden data.

Sheetal Chaudhary et al. [10] in this paper they proposed an approach to protect the iris template using steganography. They have used Random number based embedding in LSB steganography to enhance security. To provide more security, bits are embedded into LSB's of blue pixel only. The IrisCode bits are embedded across three least significant bits randomly. The resulting template is more secure as original biometric data is not stored in the database rather it is stored after embedding in cover image. They evaluated and found to be better in terms of Peak Signal to Noise Ratio (PSNR) value, histogram plot and Receiver Operating Characteristic (ROC) curve plot.

III. PROPOSED WORK

The proposed system formulates about securing the biometric template by well known method steganography. In the proposed method, biometrics template has uniformly distributed throughout the cover image. For this purpose, first the cover image is divided into blocks of equal size. Size of each block depends upon the size of cover image and on length of biometric data. After that, the central pixel of selected block is calculated. The block is selected using Pseudo Random Number Generator (PRNG) which is seeded with a secret key. Now, the bit information of biometric data is inserted at the central pixel based upon cyclic combination of last three bits which is 6^{th}, 7th and 8^{th}. Cyclic combinations of last three bits are used separately for insertion of 0 & 1. The combinations 000, 010, 100, 110 are used for insertion of 0 and 001, 011, 101, 111 are used for insertion of 1. If corresponding combination does not exist for insertion of a particular bit then we make corresponding combination using addition and subtraction 1 to that particular pixel value. Insertion and retrieval of this method of biometric data in cover image is as follow [11]:

a. Insertion Algorithm for biometric data

Step 1: Find the blocking factor (BF) using the cover image size in pixels i.e. I(p) and the template length L(t) in bits:

$$BF=\text{Abs}\left[\frac{I(P)}{L(t)}\right] \quad (1)$$

Step 2: The image is divided in at least L(t) blocks of size BF. They are disjoint and continuous, each one of them is used to store only one bit of message.

Step 3: The block for insertion of template bit is chosen by using Pseudo-Random Number Generator which uses a secret key that is shared between sender & receiver.

Step 4: With the block i indicated by PRNG, we calculate its central pixel C(i):

$$C(i)=\text{Abs}\left[\frac{B(F)*(2i-1)+1}{2}\right] \quad (2)$$

Step 5: If want to insert 0 then go to step 6 else go to step 7.

Step 6: (a) If the combination of last three bits of C(i) have value 000, 010, 100 or 110, then insert 0 at C(i) and go to END. (In this case no change in pixel value is required)

(b) If the combination of last three bits of C(i) have value 001, 011, 101 or 111, then make these combinations equal to 000, 010, 100 or 110 by adding or subtracting 1 to pixel value C(i), insert 0 at C(i) and go to END. (In this case +1 or -1 change in pixel value is required)

Step 7: (a) If the combination of last three bits of C(i) have value 001, 011, 101 or 111, then insert 1 at C(i) and go to END. (In this case no change in pixel value is required)

(b) If the combination of last three bits of C(i) have value 000, 010, 100 or 110, then make these combinations equal to 001, 011, 101 or 111 using addition or subtraction 1 to the pixel value C(i). Insert 1 at C(i) and go to END. (In this case +1 or -1 change in pixel value is required)

Step 8: END.

b. Retrieval Algorithm for biometric data

Step 1: Find the blocking factor (BF) using the cover image size in pixels i.e. I(p) and the template length L(t) in bits as given by equation (1).

Step 2: The image is also divided in at least L(t) blocks of size BF at the retrieval end.

Step 3: The block where template bit is present is chosen by using Pseudo-Random Number Generator by using a secret key.

Step 4: With the block i indicated by PRNG, we calculate its central pixel C(i) as given by equation (2).

Step 5: Check C(i), the combinations of last three bits. If it is 000, 010, 100 or 110 then template bit is 0 else 1 will be template bit.

Step 6: END.

c. Proposed Approach Architecture

Figure 3 shows the block diagram of the proposed approach to protect the template by using steganography. The proposed approach is using one biometric traits finger knuckle print. It has some phases which include: image preprocessing, feature extraction, conversion of template in to binary form, insertion method of steganography. In the proposed enrollment approach, biometric sensor captures the biometric traits from the person and converts them into feature set. Initially user select the cover image and divide the image into block of equal size shown in the figure 3. Each block has a central pixel value and a block number. Obtain a sequence of block numbers using a random number generator make the stego image with according the insertion method of steganography. In proposed verification approach, retrieval method of steganography have extract the template bits information from the stego image and after conversion the template bits in to decimal form matcher module match the template as it is genuine or not.

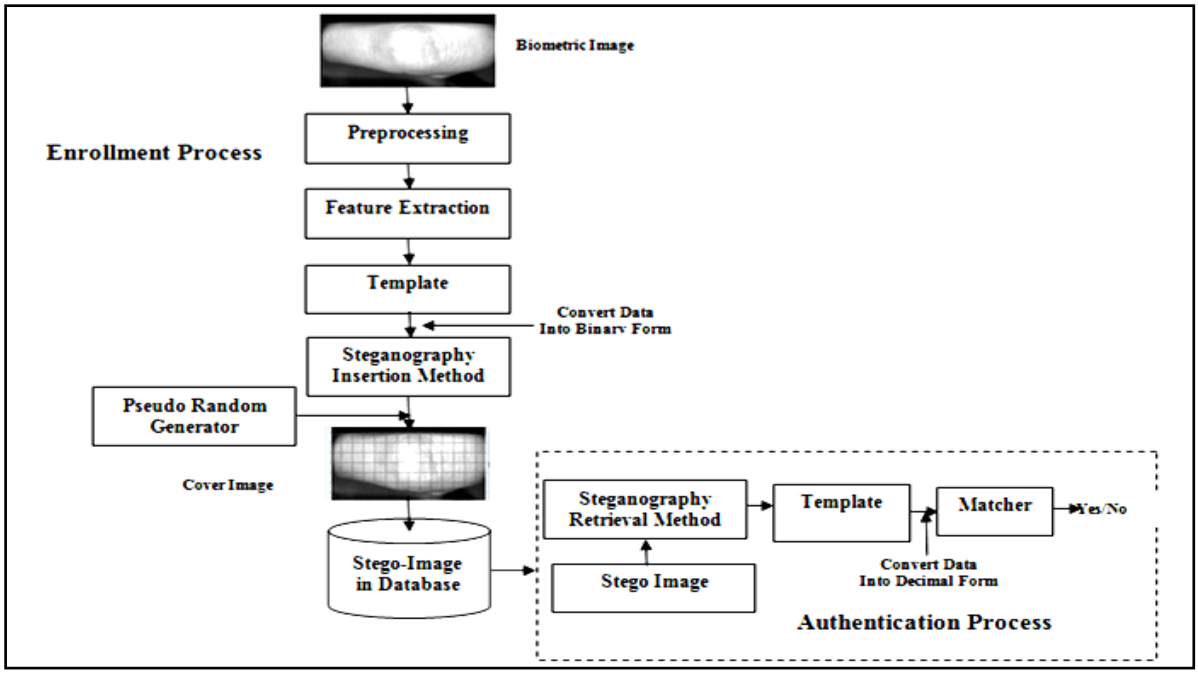

Figure 3: The architecture of proposed approach of biometric template protection using steganography.

IV. RESULTS

In our proposed approach template data in bits form is directly hidden in the cover image based upon cyclic combination of last three bits. Thus security of template is achieved to a great extend compared to existing system. In simple Gray Level Image, each pixel is represented by 8 bit. So, there are 256 possible values of a pixel. These 256 values can change during insertion of template. By using this steganography method we will obtain the following result:

i) 100% chances of template bit insertion at a pixel value by calculating:

(Pixel values for insertion/Possible Values of a Pixel)*100

ii) 50 % chances of no change in pixel value after insertion of template by calculating:

(Pixel values without any change after insertion of template bit/Total pixel values where we can insert the template)*100

V. CONCLUSION AND FUTURE WORK

The main objective of this paper is to introduce a novel approach to secure biometric template using steganography that ensures more secure template in the database. There is need of cover image with division of same blocks. This method uses the cyclic combination of last three bits for insertion and retrieval of template bit at the central pixel of the selected block. The block for insertion and retrieval of template bit are selected by using pseudo random number generator that is seeded with a secret key. This method distributes the template bits uniformly in the cover image. This method provides minimal change at a pixel value i.e. of +1 or -1 and does not provide any evidence to the intruder to identify the template image because stego image will be appearing in the database. This approach of template protection provides strong degree of temper resistance. If an intruder tries to tamper with the stego image he can't obtain the original template. In future work it can be used for improving the robustness of multimodal biometrics and will preserve the security of multimodal biometric systems.

VI. REFERENCES

[1] Anil K. Jain and Ajay Kumar. 2010. Biometrics of next generation: An overview. Second Generation Biometrics 12, 1 (2010), 2–3

[2] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing security and privacy in biometrics-based authentication systems." IBM systems Journal 40.3 (2001): 614-634.

[3] A. K. Jain, Arun Ross and U. Uludag "Biometrics Template security: Challenges and solutions" in Proc. of European Signal Processing Conference September 2005.

[4] P. Pathak, A. K. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security," in Automation, Control, Energy and Systems (ACES), 2014 First International Conference, 2014, pp. 1-4.

[5] Jain, Anil K., and Umut Uludag. "Hiding fingerprint minutiae in images." Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies. 2002

[6] Kant, Chander, Ranjender Nath, and Sheetal Chaudhary. "Biometrics security using steganography." International Journal of Security 2.1 (2008): 1-5.

[7] A. A.-A. Gutub, "Pixel indicator technique for RGB image steganography," Journal of Emerging Technologies in Web Intelligence, vol. 2, pp. 56-64, 2010.

[8] Kapczyński, Adrian, and Arkadiusz Banasik. "Biometric logical access control enhanced by use of steganography over secured transmission channel." Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011 IEEE 6th International Conference on. Vol. 2. IEEE, 2011.

[9] Bhattacharyya, Souvik, et al. "Biometric Steganography Using Variable Length Embedding." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 8.4 (2014): 668-679.

[10] Chaudhary, Sheetal, and Rajender Nath. "A new template protection approach for iris recognition." Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) 4th International Conference on. IEEE, 2015.

[11] Yadav, Rajkumar, and Ravi Saini. "Cyclic combination method for digital image steganography with uniform distribution of message." Advanced Computing 2.6 (2011): 29.