Performance Enhancement of Identification System using Vein Biometric with Modified Run Length Encoding, Stegnography and Cryptography

Madhumita Kathuria
Assistant Professor (CSE), C.I.T.M,
INDIA

ABSTRACT

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. These days, biometric technologies are typically used to analyze human characteristics for security purposes. In this paper we describe a method for integrating together cryptography and steganography through image processing. In particular, we present a system able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography. In this paper we will present some schemes for strengthening personal authentication over insecure channels with biometric concepts or how to securely transfer or use vein biometric characteristics. Our concept can be applied on any biometric authentication scheme and is universal for all systems

General Terms

Image, Pattern Recognition, Image processing, Security, Hiding Identification.

Keywords

Biometric, Template, Compression, Steganography,

Cryptography, Preprocessing.

1. INTRODUCTION

Now a day's many application areas need secure schemes for authentication. Biometric recognition scheme refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Our Proposed System overcomes the deficiencies usually found in commercially available biometric systems: Imposter Attack- someone has improperly obtained the biometric template and is staging a replay attack. An impostor may gain access to the system protected by biometrics and peruse sensitive data. An impostor may secretly obtain the raw biometric data of a user to access the system. For example, latent fingerprints. The proposed systems uses Pattern Recognition, Image Processing in the ways of extracting and manipulating the vein patterns, Cryptography and Stegnography Technique to provide security to Vein pattern template and Data Compressing Technique in order to save memory space to store compressed vein pattern images. With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. Binary images are very commonly used in our daily life. Changing the pixel values in these images for hiding the data, may produce a noticeable change in the cover media. The primary problem is the capacity of the embedding technique and preserving the visible artifacts of the cover image even after embedding the secured data.

2. RELATED WORK

In recent year several secure biometric systems have emerged and several verification technologies utilizing vein biometric features had been developed [1-8].Han Shuihua and Yang Shuangyuan [1] proposed scheme is especially useful for encryption of large amounts of data, such as digital images. Here first, a pair of keys is given by using matrix transformation; second, the image is encrypted using private key in its transformation domain; Finally the receiver uses the public key to decrypt the encrypted messages Lala Krikor,Sami Baba,Thawar Arif,Zyad Shaaban [2] present a new method for image encryption by selecting specific higher frequencies of DCT coefficients that taken as the characteristic values, and encrypting them, and the resulted encrypted blocks are shuffled according to a pseudorandom bit sequence. Selective encryption is a recent approach to reduce the computational requirements for huge volumes of images. Mehdi Kharrazi, Husrev T. Sencar have [3] used a large data set of JPEG images obtained by randomly crawling a set of publicly available websites. The image data set is categorized with respect to size, quality, and texture to determine their potential impact on steganalysis performance. To establish a comparative evaluation of techniques, undetectability results are obtained at various embedding rates. Chander Kant, Ranjender Nath & Sheetal Chaudhary [4] applied a new idea is presented to make system more secure by use of steganography. Here the secret key (which is in the form of pixel intensities) will be merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode. Mohit Soni, Sandesh Gupta, M.S. Rao, Phalguni Gupta [5] applied Euclidean Distance based matching technique for making the decision for feature extraction. Maleika, Naushad and Raja [6] applied Principle Component Analysis (PCA), with Cholesky decomposition and Lanczos algorithm to extract the vein features which decreases the number of computation and the processing time. Amioy Kumar M. Hanmandlu Vamsi K. Madasu Brian C. Lovell [7] used Box and branch point based approaches for multiple feature extractions. Region of interest (ROI) was extracted from the vein patterns were convolved with Gabor filter. Debnath Bhattacharyya, Poulami Das, Tai-hoon Kim, Samir Kumar Bandyopadhyay [8] proposed Pattern Marker Algorithm (VPMA), Vascular Pattern Extractor Algorithm (VPEA), and Vascular Pattern Thinning Algorithm (VPTA). Dr. M.Umamaheswari, Prof. S. Sivasubramanian, S. Pandiarajan [9] had compressed the secret message and encrypts it by the receiver's public key along with the stego key and embeds both messages in a carrier using an embedding algorithm. They saved the stego - image into BMP or PNG format because they are lossless. Kshitiz Agarwal, Karm Veer Arya [10] had proposed lossy compression technique which can be effectively used for correlated pixels in both continuous and discontinuous series because compression is achieved by reducing redundancy through removal of similar pixels. They had removed dependency of effective compression over their continuity. Ms. Mansi Kambli, Ms. Shalini Bhatia [11] had applied important features of wavelet transform and different methods for compression of fingerprint images. They have done a comparative study using discrete cosine transform based Joint Photographic Experts Group (JPEG), wavelet based basic Set Partitioning in Hierarchical trees (SPIHT) and Modified SPIHT. Their proposed comparison shows that Modified SPIHT offers better compression than basic SPIHT and JPEG. Eman Abdelfattah, Asif Mohiuddin [12] had evaluated the performance of Huffman and Run Length Encoding compression algorithms with multimedia data. They had used different types of multimedia formats such as images and text and performed Extensive experimentation with different file sizes to compare both algorithms evaluating the compression ratio and compression time.

3. PROPOSED WORK

Proposed Personal authentication system given in Figure 1. Promises to overcome all disadvantage or limitation of the above stated Personal Identification Systems We have proposed various Algorithms and methods to develop our Designed System.

3.1 Vein Image Extraction

In this stage the vein pattern is extracted by the help of sensor, which can be used for further enrollment and verification.

3.2 Vein Image Preprocessing

3.2.1 Image Enhancement Sub-module

It enhances the wanted vein pattern and reduces unwanted information such as background noise, irregular shades due to muscle and bones in the fingers and intensity fluctuations. *It* is done by applying *Mean filter* to remove noise pattern. Images contain spurious cell (pixel cell) values (much brighter or darker than their surroundings) that represent "noise" imposed by the imaging system. Mean filter is a simple sliding window that replaces the center value in the window with the average of all pixel values in the window. For example a single 3x3 window, this placed on the desired pixel with covering its eight neighbor pixels. The desire pixel value is replaced by the mean of all nine values.

i.e. $f(x, y) = (a1+a2+a3+a4+a5+a6+a7+a8+a9)/9$.

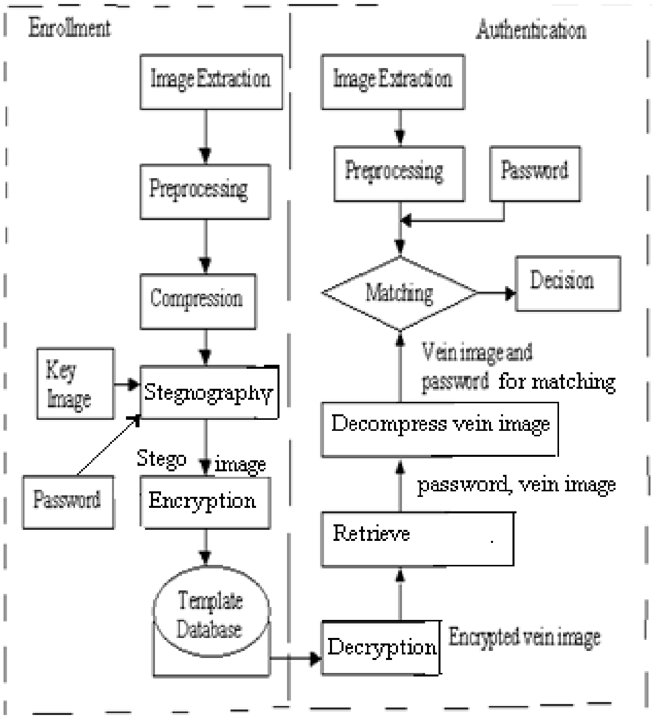

Figure1.Proposed System

3.2.2 Image Binarization Sub-module

This module is used to separate objects (vein) from background and convert the image into a black and white image (to binarize the image) with the help of *Threshold value. Pixels* in an image are marked as "background" pixels if their value is greater than some Threshold value and as "Object" pixels otherwise. Typically, an object pixel is given a value of "0" while a background pixel is given a value of "1". We have considered the average intensity of whole image as threshold.

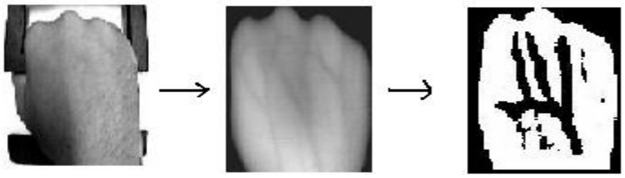

Figure 2: Vein Image Preprocessing Module

3.3 Vein Image Compression

Compression is used to encode information. Compression techniques Transform a sequence of characters into a new string of bits having same information content and length as short as possible. We compressed the vein image before stegnography and encryption so that space can be save and processing time is reduced.

The Proposed algorithm is a modified Run Length Encoding algorithm which scans one character (run) at a time. If a character is equal to its next character, then it checks for repetition and then store the outputs as the character with the no of repetition (length) that follows it. If a character is not equal to its next character, then it stores outputs as no of repetition with new character.

3.3.1 Modified Run Length encoding algorithm:

```
1. Set Run Length = 0
2. Set i = 0;
3. Do
3.1 Set i=j
3.2 Set j = i  + Run Length
3.3 Read A[i]
3.4 Read B[j]
3.5 If A[ i]= End of  image pixel string array then
      Write Run Length
      Write A[i]
       Exit
3.6 Else
     3.6.1 If A[i]=B[j] then
          3.6.1.1 If Run Length= Length of Pixel array then
                    Write Run Length
                    Write A[i]
                    A[i]=B[j] // value of B[j] assign to A[i]
                    Set Run Length=0
                  Else
                    Run Length= Run Length+1
                  End if
          Else            //if A[i]!=B[j]
                 Write Run Length
                 Write A[i]
                 A[i]=B[j] // value of B[j] assign to A[i]
                 Set Run Length=0
           End if
     End if
3.7 While (i !=End of  image pixel string array)
```

3.4 Vein Image Stegnography

Stegnography means encodes Secret Messages in Images. In our proposed system user's vein image as well as password is taken under consideration. Here user's password is encoded into a bit stream and then hidden in a cover key image using LSB Insertion Algorithm. Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover file. It overwrites the LSB of an image's pixel with a Message's bit. Since standard cryptographic systems do not provide strong encryption, so we have applied a Stenographic technique as well as encryption technique. Our proposed system provides higher security as we have used vein pattern as well as password as our access identification.

3.4.1 LSB Hiding Algorithm

1. Read Cover Key image pixel array K [ ].
2. Read the password (stream of characters), Convert the character into equivalent ASCII Code and then Convert the ASCII Code into binary equivalent array A [ ].
3. Calculate the Size (no of bytes) of cover image i.e. N. Scan N (number of pixel) from A [ ] for hiding.
4. According to Size replace the last bit of each byte in image array (8^{th} bit) with Password array bit. i.e. hide the password bits with LSB bit of each byte.

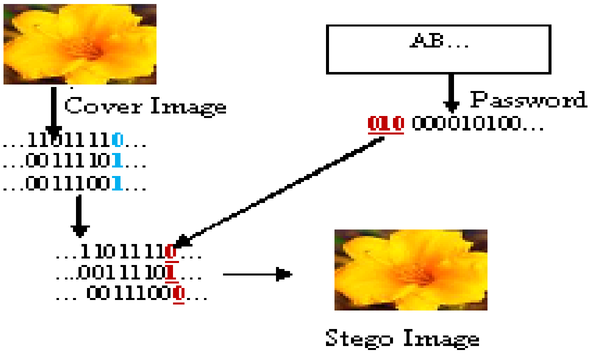

Figure 3: Embedded Password into Cover Image

Here we choose a 24-bit image as cover, so we can store 3 bits in each pixel. To the human eye, the resulting stego image will look identical to the cover image as shown in figure 3

3.5 Vein Image Cryptography

Cryptography protects information by transforming it into an unreadable format. The original image, or *plain image*, is converted into a coded equivalent called *cipher image* via an encryption algorithm. Cryptography systems can be broadly classified into symmetric-key systems (see Fig. 1) that use a single key (i.e., a secret image) that used for both *encryption* and *decryption* algorithm.

3.5.1 Vein Image Encryption

Encryption algorithm used a XOR function, which is applied on binarize vein pattern image and key image pixel by pixel.

```
1.   Read binarize Vein-image pixel array B [ ].
2.   Read Stego Key-image pixel array K [ ] of same size as
     Vein –image. i.e. M*N.
3.   for i=0 to M-1 do
4.     for j=0 to N-1   do
5.       B [ i , j] = B[ i , j] xor  K [ i , j].
```

Where B[i, j] is the ith row and jth column of the Vein-image,

K [i , j] is the ith row and jth column of the Key-image.

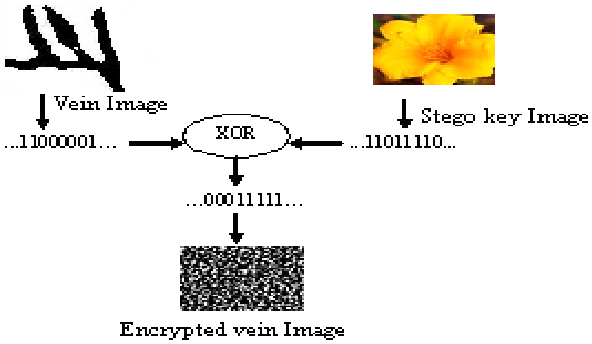

Figure 4: Vein Image Encryption

In this algorithm same size of Key-image and Vein-image is taken. First the size of two images are compared, if they have same size, then the Pixel by pixel XORing will occur to generate an encrypt image. The XOR operation will perform on each same positioned pixel of two images starting from the very first pixels and repeated until the last pixel. If the same positioned pixel of two image having same pixel value, then at that pixel position in vein image store the '0' value. Otherwise store '1'at that pixel position.

3.6 Vein Template Retrieve or Extraction

It follows the reverse procedure of hiding algorithm. Here the stego-image is scan from the first pixel and read the 8th most bit (LSB) and save it into an array until N numbers of pixels is scanned and save.

3.7 Template Decryption Algorithm

Decryption algorithm is follow the same procedure as the Encryption algorithm but here instead of arrived vein image template the decompressed vein template is XOR with key image pixel wise to provide original template.

3.8 Decompression Algorithm

This Technique decodes the compressed vein template into original vein template. The decompression gives character repeated until reach `length`.

3.9 Template Matching Algorithm

First the password given by user is matched with the retrieved password from retrieval module. If the passwords match properly then it go for further matching of vein patterns. The live vein template is compared pixel by pixel against at least one of the master templates stored within the vein pattern template database, depending on the operation mode. Then match score is count, which is the number of matched (mismatched) pixels between the potential arrived pixel block and the template pixel block. The best match is acceptable if its score is better than a pre specified threshold.

4. EXPERIMENTAL RESULT

The proposed system was implemented with a database consists of 9 different vein patterns and 9 different passwords of different sizes. The system showed promising results with accuracy above 90%. It tries to calculate best match score. The basic measures of performance system are false acceptance rate (FAR) and false rejectance rate (FRR). False Acceptance Rate refers to the total number of unauthorized persons getting access to the system over the total number of people attempting to use the system. False Rejection Rate refers to the total number of authorized persons not getting access to the system over the total number of people attempting to get access to the system. Capacity, security and robustness are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

PSNR (Peak Signal to Noise Ratio): It is the measurement of the quality between the cover Encrypted image E and stego-image S of sizes N × N is defined as:

$$PSNR = 10 * \log(255^{2} / MSE)$$

Where $$MSE = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}(f(x,y) - g(x,y))^{2} / N^{2}$$

Where f(x, y) is the pixel value at the position (x, y) in the cover-image and g(x, y) is the pixel value at the position (x, y) in the corresponding stego-image respectively. The PSNR is expressed in terms of db. The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego-image. The PSNR and Robustness for different size image with different size password is given in figure 5.

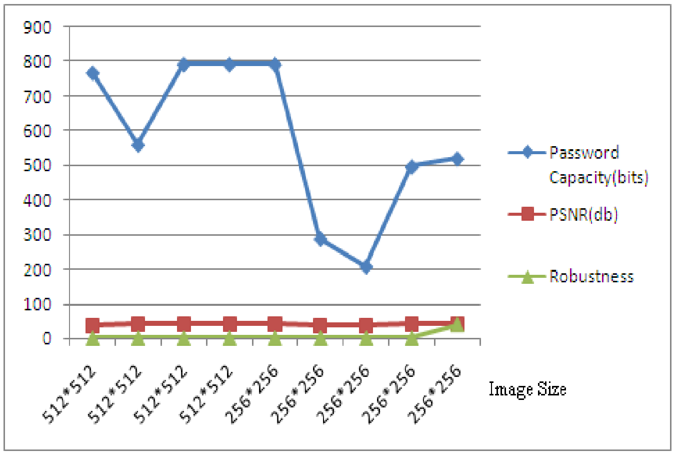

Figure 5. PSNR and Robustness for different size image

5. CONCLUSION

The proposed system influence the performance of the system, speed, accuracy, provides efficient memory, security and cannot be easily spoofed or damaged. We have proposed a novel robust lossless image data hiding technique, which employs a statistical quantity as a parameter for data embedding. Its Data embedding capacity is above 512 bits (often sufficient for authentication purpose and the capacity can be adjusted according to requirement). Original image and the embedded data are extracted exactly without any loss because our method is completely reversible. Furthermore, the implementation of various security measures provides a high level of protection for the hidden data. This system satisfies the characters of convenient realization, less computation complexity and good security. We can further improve the Template Encryption technique by providing secure and longer key, Quantum cryptography, which uses quantum mechanics, Watermarking technique, Stenography to hide our Vein template behind another image.

6. REFERENCES

[1] Han Shuihua and Yang Shuangyuan ,"An Asymmetric Image Encryption Based on Matrix Transformation",ECTI TRANSACTIONS ON COMPUTER AND INFORMATION TECHNOLOGY, VOL.1, NO.2 NOVEMBER 2005,pp.126-133.

[2] Lala Krikor,Sami Baba,Thawar Arif,Zyad Shaaban," Image Encryption Using DCT and Stream Cipher"European Journal of Scientific Research ISSN 1450-216X, Vol.32 No.1 (2009), pp.47-57.

[3] Mehdi Kharrazi, Husrev T. Sencar,"Performance study of common image steganography and steganalysis techniques", Journal of Electronic Imaging, 15(4), 041104 (Oct–Dec 2006), pp.041104-1- 041104-16.

[4] Chander Kant, Ranjender Nath & Sheetal Chaudhary," Biometrics Security using Steganography",International Journal of Security, Volume (2) : Issue (1) pp.1-5.

[5] Mohit Soni, Sandesh Gupta, M. S. Rao, Phalguni Gupta," A New Vein Pattern-based verification System", International Journal of Computer Science and Information Security, Vol. 8, No. 1, pp.58-63, 2010.

[6] Maleika Heenaye-Mamode Khan, Naushad Mamode Khan and Raja K.Subramanian,"Feature Extraction of Dorsal Hand Vein Pattern using a fast modified PCA algorithm based on Cholesky decomposition and Lanczos technique", World Academy of Science, Engineering and Technology, vol. 61, pp.279-282, 2010.

[7] Amioy Kumar M. Hanmandlu Vamsi K. Madasu Brian C. Lovell, "Biometric Authentication based on Infrared Thermal Hand Vein Patterns", Digital Image Computing: Techniques and Applications, pp.331-338, 2009.

[8] Debnath Bhattacharyya, Poulami Das, Tai-hoon Kim, Samir Kumar Bandyopadhyay." Vascular Pattern Analysis towards Pervasive Palm Vein Authentication", Journal of Universal Computer Science, vol. 15, no. 5, pp. 1081-1089, 2009.

[9] Dr.M.Umamaheswari,S.Sivasubramanian, S.Pandiarajan, "Analysis of Different Steganographic Algorithms for Secured Data Hiding" ,IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010,pp.154-160.

[10] Kshitiz Agarwal,Karm Veer Arya,"An Image Compression Algorithm for Discontinuous Series of Similar Pixels", International Journal of Computer Applications (0975 - 8887),Volume1-No. 17,2010,pp. 89-90.

[11] Ms.Mansi Kambli, Ms.Shalini Bhatia," Comparison of different Fingerprint Compression Techniques",Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.1, September 2010,DOI : 10.5121/sipij.2010.11.03 27,pp. 27-39.

[12] Eman Abdelfattah, Asif Mohiuddin ," PERFORMANCE ANALYSIS OF MULTIMEDIA COMPRESSION ALGORITHMS", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010,DOI : 10.5121/ijcsit.2010.2501 1, pp. 1-10.

[13] Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi ,M.Sharif and Hamdan.O.Alanazi ," Optimization Digital Image Watermarking Technique for Patent Protection", Journal of Computing (JOC), Vol.2, Issue 2, ISSN: 2151-9617, February 2010, Lille, France. P.P 142-148

[14] Hamdan.O.Alanazi, A.A.Zaidan, B.B.Zaidan, Hamid A.Jalab and Zaidoon Kh. AL-Ani, "New Classification Methods for Hiding Information into Two Parts: Multimedia Files and Non Multimedia Files", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617,pp. 144-151.

[15] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb,Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, 3 Aug 2009, USA, P.P 73-78,

[16] Kussay Nugamesh Mutter, Zubir Mat Jafri ,Azlan Bin Abdul Aziz," Hybrid Hopfield Neural Network, Discrete Wavelet Transform and Huffman Coding for Image Recognition", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009 ,pp. 73-78.

[17] Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File",International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, 30 January, Vienna, Austria, P.P 46-54.

[18] B.B Zaidan , A.A Zaidan ,Alaa Taqa , Fazidah Othman ," Stego-Image Vs Stego-Analysis System", International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5 , ISSN:1793-8163, December (2009), Singapore,pp.572-578 .

[19] Alaa Taqa, A.A Zaidan, B.B Zaidan ,"New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm", International Journal of Computer and Electrical Engineering (IJCEE) ,Vol.1 ,No.5, ISSN: 1793-8163, December (2009). Singapore, p.p. 566-571.

[20] Hamid.A.Jalab, A.A Zaidan and B.B Zaidan," Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation", Journal of Computing (JOC), Vol.1, Issue 1, ISSN: 2151-9617, December 2009, Lille, France, P.P 108-113.