Biometric Information Security System Based On Nonlinear Encryption Scheme

Gayathri S P, Sajeer M

Abstract—With the growth of multimedia and digital technology the transmission over public channel become more common and also the issues with the confidentiality and integrity of data increases in an alarming rate. Biometric characteristics such as fingerprint , iris , palm print, gestures, handwritten signature and hand geometry have to be considered as an efficient tool for establishing the identity of an individual. Because they contain the unique characteristics of a person. So we proposed a method, to protect the biometric information from any of the unauthorized access. Which utilizes an orthogonal coding and multiplexing technique, direct LSB replacement steganography technique and finally a chaotic encryption method. Multiple biometric signatures are encoded and then multiplexed together in the form of a single image using orthogonal encoding and multiplexing.The encoded image is embedded in to the colour cover image ,which is decomposed in to three plane namely red ,green ,blue respectively. In steganography technique, the multiplexed image pixel is used to replace the LSB of corresponding colour cover image pixel for information hiding purpose. Finally, the stego image is encrypted using a non linear encryption technique.The objective of this paper is to develop a novel and efficient technique to protect the Biometric Information from any unauthorized access and also reduces the vulnerability of an intruder to retrieving any information through any steganalysis attack .In addition to this technique can also accommodate a number of different biometric information in the same cover image while maintaining the negligible amount of distortion when compared with original colour cover image. The encrypted images are random, non repeated and unpredictable. Chaotic encryption have excellent diffusion and confusion properties and can resist the any plaintext attack. The Performance of the proposed technique was investigated through matlab simulation using various biometric signatures and colour cover images.

Keywords: orthogonal transform, steganography, nonlinear encryption , chaotic system

I. INTRODUCTION

Biometric signatures such as fingerprints, iris, hand geometry, palm print and gestures are considered as efficient tools in establishing the identity of an individual. Because they contain unique characteristics of a human. However, the great challenges associated with biometric signature based security systems is the variation and distortion of biometrics with place, time, and environment, another limitations are non cooperation of individuals for preservation of biometric characterestics.

Revised Version Manuscript Received on April 30, 2017.

Gayathri S P, Department of Electronics and Communication Engineering, Sree Chitra Thirunnal College Of Engineering, Trivandrum, India, E-mail: gayathrisp1994@gmail.com

Sajeer M , Department, of Electronics and Communication Engineering, Sree Chitra Thirunnal College Of Engineering, Trivandrum, India, E-mail: sajeermuhammed@gmail.com

Biometric information requires robust security techniques to prevent from any unauthorized access. Biometric informations can be preserved and protected by a threefold encryption method involving orthogonal coding scheme, encoded steganography and chaotic encryption process. Multiple biometric signatures are orthogonally encoded and then multiplexed together in the
form of a single image . The encoded image is embedded in to the colour cover image ,which is decomposed in to three plane namely red ,green ,blue respectively. In steganography technique, the multiplexed image pixel is used to replace the LSB of corresponding colour cover image pixel for information hiding purpose. Finally, the stego image is encrypted using a new one dimensional chaotic encryption technique. The objective of this paper is to develop a novel and efficient technique to protect the Biometric Information from any unauthorized access and also reduces the vulnerability of an intruder to retrieving any information through any steganalysis attack .In addition to this security system can also accommodate a number of different biometric characteristics in the same colour cover image, while maintaining the negligible amount of distortion when compared with original colour cover image.. Chaotic encryption have excellent diffusion and confusion properties and can resist the any plaintext attack.

II. LITERATURE SURVEY

M.N. Islam, proposed [1] a new cryptographic technique for information security of fingerprint. An orthogonal coding scheme is developed to encrypt the fingerprint image. Multiple encrypted fingerprint images are then mixed together to form a single image by multiplexing process.

M.N. Islam, proposed " Colour image encryption using multiple reference joint transform correlation"[2] method. Which involves a novel colour encryption for colour information using a modified joint transform correlation (JTC) scheme. The colour image is first decomposed in to three components, red ,green, blue respectively.

M.F. Islam, M.N. Islam proposed [3] , the main objective of this paper is to provide compression and encryption of biometric information utilizing orthogonal coding and steganography technique. Multiple biometric signatures are encrypted individually using orthogonal codes and multiplexed together. Which is then embedded in acolourcover image using proposed steganography technique .Anil K. Jain, Karthik, Nandakumar and Abhishek Nagar proposed[4].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Biometric recognition offers a reliable and natural solution to the problem of user authentication in identity management systems. There are increasing concerns about the security and privacy of biometric signatures.

Khan Muhammad, Jamil Ahmad, Haleem Farman and Muhammad Zubair proposed [5]. This method involves the process of embedding text in images such that its existence cannot be detected by Human Visual System (HVS) and is known only to sender and receiver and then embeds secret data inside the Intensity Plane and transforms it back to RGB.

This technique is evaluated by subjective and Objective analysis. Experimentally it is found that proposed method have larger PSNR values, good imperceptibility and multiple security levels , which shows its superiority as compared to several existing methods.

Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt proposed [6]. This method involves hiding or embedding data in a transmission medium. Its ultimate objectives are undetectability, robustness and capacity of the hidden data are the main factors that distinguish it from other techniques, namely watermarking and Cryptography. It identifies current research problems in this area and discusses how current research approach could solve some of these problems. they propose using human skin tone detection in colour images to form an adaptive context for an edge operator which will provide an excellent secure location for data hiding.

SunitaBarve, Uma Nagaraj and RohitGulabani proposed a method [7] , introduces a new way of embedding secret data within the skin portion of the image of a person, as it is not that much sensitive to Human Visual System . This skin region shows excellent secure location for data hiding. The data embedding is performed in DWT domain than the DCT domain as DWT outperforms than DCT.Using Biometric characteristics resulting stego image is more tolerant to attacks and more efficient method than existing methods.

Mohammed abdulmajeed and Rossila watisulaiman proposed [8], which is very efficient in hiding data, because this technique is able to keep changes to the stegoimage to minimum. So, they conclude that proposed technique have good quality of invisibility and un detectability. In terms of security property, two additional levels of security were added to the standard LSB steganography.

The advantage of this technique is that the red colour will act as noise data, to the any possible attacker with the intention to extract the message. As a result, this will make the extraction process more difficult. In second level the new bit inversion technique, which reverses the bits of the stego image pixels after the standard LSB is applied. In this paper, they introduced a new type of bit inversion technique of steganography.

III. METHODOLOGY

A novel approach for securing multiple binary biometric signatures by multiplexing and then embedding them into a color image. Multiple binary biometric signatures, such as fingerprint, iris , signature, and personal identification text information, are encoded individually using orthogonal codes and then multiplexed together to form a single image,which is 2 dimensional matrix .

A colour cover image is then decomposed into three colour channel, namely, red, green and blue. The matrix is then embedded into one of the colour channel images using the direct LSB replacement technique.In this technique three least significant bits of the cover image is used to hide the bit of the biometric information. Three sets of encrypted binary characteristics are embedded into three colour component images.

Then all three decomposed stego images are combined to form the colour stego image, which hides a number of biometric characteristics inside the image and makes them invisible to intruders.

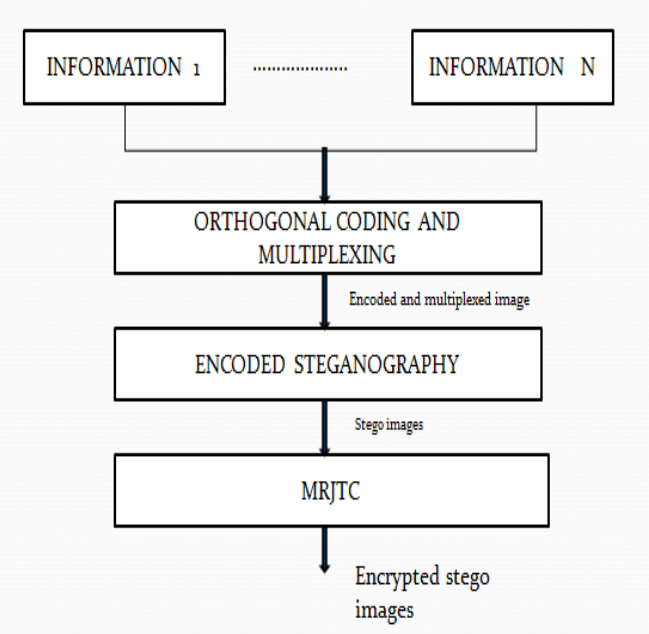

Fig.1. Overall Block Diagram

Then finally we uses an one dimensional chaotic system based encryption. This is because chaotic systems or maps have high sensitivity to their initial values and control parameters, chaotic property, nonconference, and state ergodicity. So many of the chaotic image encryption algorithms have been developed by directly utilizing existing chaotic maps to their encryption processes. In general, a chaos-based image encryption algorithm contains two portions such as chaotic system and image encryption.

Orthogonal coding technique further enhances the security by increasing robustness and making it practically impossible to access the information without authorization. Simulation experiments prove that most steganalysis methods would fail in detecting any meaningful information from the stego image.

3.1. Orthoganal Encoding

Orthogonal code is one of the coding technique, which detect as well as correct the corrupted data.The transform used here is Walsh Hadamard transform. It is a real, orthogonal, symmetric and fast transform and also have good energy compaction property for highly correlated images. Applications of orthogonal codes are in image data compression, filtering and design of codes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

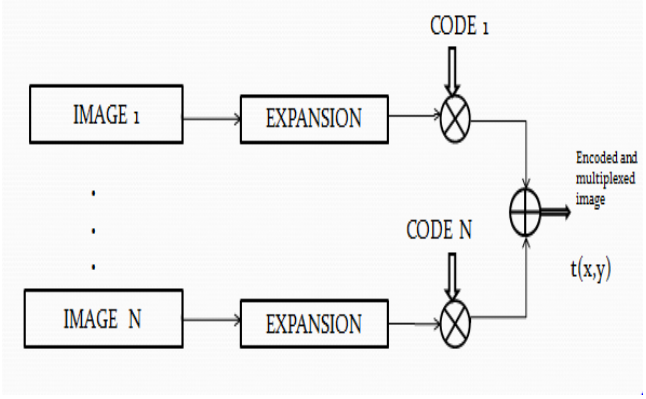

Fig.2.Orthogonal Encoding and Multiplexing Technique

Fig.2. shows the block diagram of orthogonal encoding and multiplexing .Image 1 ,Image2 .....Image N are the biometric characteristics. which is fed in to an expansion block. This technique is used to convert two dimensional matrix to an one dimensional array and then multiplied by the respective orthogonal code and then added together to form a single image.

Let gi(x, y) is the expanded form of the ith input image fi(x, y), and ki(x, y) is the respective orthogonal code,then the encoded and multiplexed image can be obtained as

$$t(x,y)=\sum_{i=1}^{N} ki(x,y)gi(x,y) \quad (1)$$

3.2. Encoded Steganography

Steganography deals with composing hidden messages by suitably alter the pixels in an image. Then a colour image is selected as the cover image to hide the confidential biometric signatures. The cover image can be any colour image, even another biometric image like face image. The colour image is first split into its three colour components, namely, red, green and blue respectively, each of which is used to hide one set of multiplexed biometric characteristics.

The encoded steganography technique for one colour channel, the same scheme will be repeated for all the three colour channels. The proposed security system also employs a steganography technique ,multiplexed image pixel is used to replace the LSB of corresponding cover image pixel for information hiding purpose.

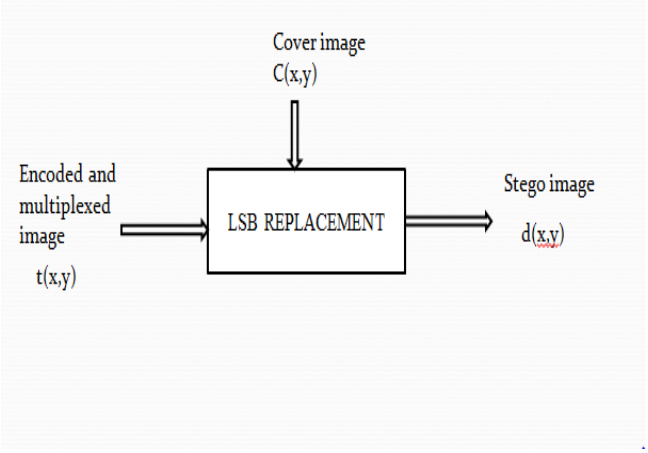

Fig.3. Encoded steganography technique

3.4. Chaotic System Based Mrjtc Encryption Method

Some simple mathematical equations exhibit complex behaviour ,which has been called as chaotic. Chaotic systems are extremely susceptile to changes in initial conditions. Here the secret key generation can be done with the help of chaotic system.which is a dynamic system. A chaos based image encryption algorithm contains two portions such as a chaotic system and image encryption.

Chaotic system in the image encryption algorithms can be divided into two, one-dimension (1D) and multi-dimension (MD).In one dimensional system contain only one parameter. But in multi dimension there are multiple parameters. multiple parameters increase the difficulty of their hardware/software implementations and computation complexity.

chaotic systems/maps have high sensitivity to their initial values and control parameters.

i. Logistic map

The mathematical definition can be expressed in the following equation

$$Xn+1 = L(r,Xn) = r\,Xn\,(1-Xn), \quad r \in (0,4] \quad (2)$$

ii. Tent map

The Tent map is known as its tent-like shape in the graph of its bifurcation diagram. It can be defined by the following equation

$$Xn+1=T(u,Xn) = \begin{cases} uXn/2, & Xn<0.5 \\ u(1-Xn)/2, & Xn\geq 0.5 \end{cases} \quad (3)$$

, u € (0,4]

iii.Sine map

The Sine map has a similar chaotic behavior with the Logistic map. The definition can be described by the following equation:

$$Xn+1=S(a,Xn) = aSin(\Pi Xn)/4, \quad a \in (0,4] \quad (4)$$

The above logistic map is used as encryption key for the multiple reference joint transform correlation (MRJTC) encryption technique. Which is a nonlinear encryption technique based on phase shifting and fourier transform.

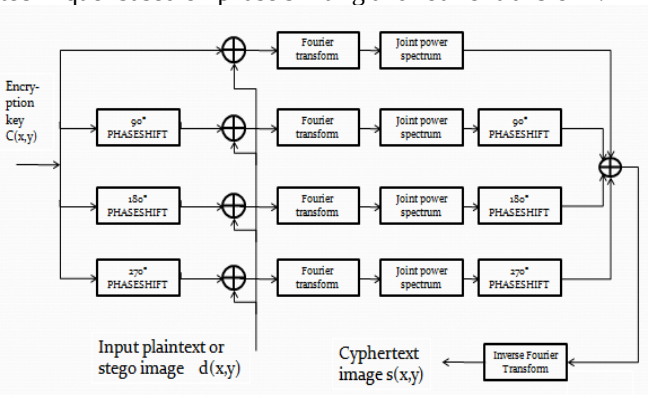

Fig.4. MRJTC Encryption Algorithm

Fig.4 shows the block diagram of the nonlinear MRJTC-based encryption technique for securing the stego image. An encryption key is formed in the shape of an image having the same dimensions as the image to be encrypted but having random pixel values. The encryption key, c(x, y), is fed to four parallel processing channels after phase shifting by 0◦, 90◦, 180◦, and 270◦, respectively.

The input plain text stego image, d(x, y), is added to the phase-shifted keys in each channel, which yields four joint images as given by

$$f1(x,y)=c(x,y)+d(x,y) \quad (5)$$

$$f2(x,y)=jc(x,y)+d(x,y) \quad (6)$$

$$f3(x,y)=-c(x,y)+d(x,y) \quad (7)$$

$$f4(x,y)=-jc(x,y)+d(x,y) \quad (8)$$

Applying Fourier transformation to each of the joint images in Equations. (9) to (12), the magnitude spectra are recorded as four joint power spectrum (JPS) signals as given by

$$S1(u,v)=|F1(u,v)|^2 \quad (9)$$

$$S2(u,v)=|F2(u,v)|^2 \quad (10)$$

$$S3(u,v)=|F3(u,v)|^2 \quad (11)$$

$$S4(u,v)=|F4(u,v)|^2 \quad (12)$$

where u and v are the Fourier domain variables. The above JPS signals are again phase-shifted by 0◦, 90◦, 180◦, and 270◦, respectively. Then a modified JPS signal is developed using the following relation.

$$S(u,v)=S1(u,v)+jS2(u,v)-S3(u,v)-jS4(u,v)$$
$$=4C^*(u,v)D(u,v) \quad (13)$$

Then taking the inverse fourier transform to the result

$$s(x,y)=4c(x,y)d(x,y) \quad (14)$$

Now an authorized user having the correct set of keys can easily retrieve the original biometric information from the encrypted stego image .Fourier transformation is applied on the encrypted stego image and the result is multiplied by the encryption key. Then an inverse Fourier transformation can yield the decrypted image as given by

$$e(x,y)=IFT\ [C(u,v)\ D(u,v)] \quad (15)$$

IV. EXPERIMENTAL RESULT

The proposed image encryption of biometric characteristics using MRJTC encryption system was investigated through computer simulation program developed in MATLAB software.

Fig.7. Input Colour Cover Image

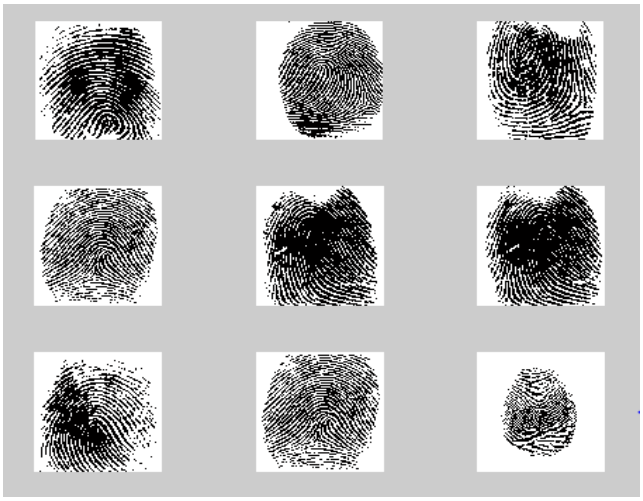

Fig. 8. Input fingerprint sample

Fig.9.Cover Image Decomposition

Fig.10. Encoded Steganography Image

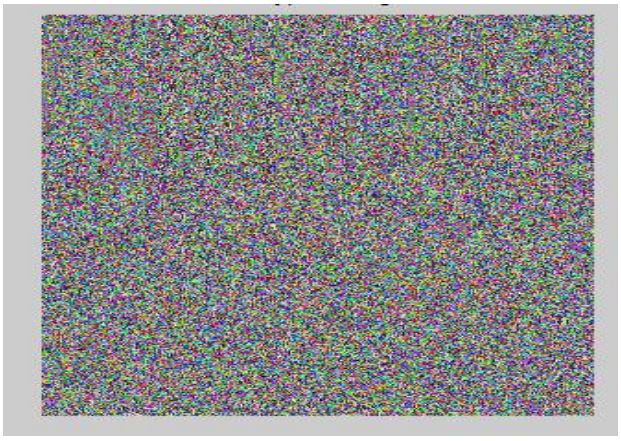

Fig.11. MRJTC Encrypted Image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Computer simulation results using sample colour images and biometric information show no visual distortion in stego image as compared to cover image.

Also the histogram analyses of cover and stego images confirm that there are no significant changes in the image because of these embedding processes. The proposed embedding process is highly secure such that no information can be retrieved without knowing the process and the correct keys used for encryption.

V. CONCLUSION

In this paper we proposed a novel and efficient technique to protect the biometric information from any of the unauthorized access and also it reduces the vulnerability of an intruder to retrieving any of the information through steganalysis attack. In addition to this ,technique can accommodate a number of biometric information in the same cover image , while maintaining a negligible amount of distortion , when compared with the original colour cover image. The proposed biometric information security scheme yields a high level of robustness against any security attacks by employing threefold encryption. The orthogonal encoding scheme enhances the robustness by making the biometric information almost inaccessible without any authorization. The encoded steganography process reduces the vulnerability of an intruder retrieving any information through any steganalysis attack. Chaotic system based MRJTC encryption have excellent diffusion and confusion properties .It can resist the chosen plaintext attack and also withstand the data loss and noise attacks.

REFERENCE

1. M.N. Islam, “Encryption and multiplexing of fingerprints for enhanced security”,in: Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2011.
2. M.N. Islam,” Color image encryption using multiple reference joint transform correlation”, in:Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2012.
3. M.F. Islam, M.N. Islam, “A secure approach for encrypting and compressing biometric information employing orthogonal code and steganography,” in: SPIE Proceedings in Optical Pattern Recognition XXIII, 2012.
4. Yicong Zhou n, Long Bao, C.L. Philip Chen ,” A new 1D chaotic system for image encryption “ in: SignalProcessing,97(172–182), 2014.
5. Khan Muhammad, Jamil Ahmad, Haleem Farman, Muhammad Zubair , “A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model”,in: International Journal of Advanced Science & Technology, vol. 54, 2013.
6. Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, “Biometric Inspired Digital Image Steganography”,in: 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems ,2008.
7. SunitaBarve, Uma Nagaraj and RohitGulabani ,” Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform” in: International Journal of Computer Science & Communication Networks,Vol 1(1),September-October, 2011.
8. Mohammed abdulmajeed and Rossilawatisulaiman , “An improved lsb image steganography Technique using bit-inverse in 24 bit colourImage”,in: Journal of Theoretical and Applied Information Technology,. Vol.80. No.2 , 20th-October 2015

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.