ISSN No:-2456 –2165

An Enhanced Information Security System Using Orthogonal Codes and MRJTC

[1]G H Ghazia ,[2]Kanjana G
[1]P G Scholar,L.B.S Institute of Technology for women Poojapura , Trivandrum.
[2] Assistant Professor,L.B.S Institute of Technology for women Poojapura , Trivandrum.

Abstract:-The growth of digital technology has resulted in the confidentiality and information integrity problems. Thus data hiding became an important process for secured information transmission. Information security needs high authenticated techniques for the prevention of unauthorized access. Personal information like Bio- metric signatures are efficient tools in revealing an individual identity since they has unique human characteristics. An efficient and secured approach for multiple binary biometric signatures is encrypting, multiplexing and then embedding them into a color image. The embedding process is confidential since information cannot be accessed without knowing the process and the correct keys for encryption. Orthogonal coding technique in turn results in enhanced security with increase in robustness and information integrity which makes it practically impossible to access the information without respective authorization. Orthogonal codes are mainly a set of sequences with correlation properties. It implements encryption along with a multiple phase shifted reference based joint transform correlation technique. It produces more faithful reproduction of data and also helps in better hidden transmission.

Keywords:-Data Hiding, Biometrics, MRJTC-Multiple Phase Shifted Reference Joint Transform Correlation, Orthogonal .

I. INTRODUCTION

The issues with the confidentiality and integrity of information are also growing at an alarming rate with increase in the digital technology. To overcome security and privacy issues ,a biometric cryptosystem approach has been proposed to protect biometric templates. Personal identification information requires robust security techniques to prevent from any unauthorized access. a great challenge with biometrics-based security systems is the variation and distortion of biometrics with time, place, and environment. Biometric information can be preserved and protected through steganography technique, where the least significant bit (LSB) of a cover image is replaced by the corresponding information bit.

Traditional steganography techniques are vulnerable to steganalysis attacks where an intruder try to retrieve the secret information by monitoring the LSBs of the cover image [11,12]. A number of digital encryption techniques have also been proposed in the literature to protect biometric information [13,14]; however, they are typically linear processes, where there are always chances of decoding, completely or at least partly, the confidential information without knowing the secret keys.

The objective of this paper is to develop a novel and robust technique to protect biometric information employing orthogonal coding scheme, encoded steganography and nonlinear encryption process. Multiple biometric signatures are encoded and then multiplexed together in the form of a single image using orthogonal codes [15]. Then the encoded information is embedded into a color image, which is decomposed into three color channels, namely, red, green and blue, each of which is used to embed a set of bio-metric signatures. The proposed security system also employs a second set of keys to select one bit from the three LSBs of the cover image pixels for information hiding purpose [14,13]. Finally, the stego image is encrypted using a multiple phase-shifted reference joint transform correlation (MRJTC) technique, which incorporate a nonlinear transform-based encryption process [11].

This system yields a high level security of threefold encryption-orthogonal coding, random bit replacement, and nonlinear encryption process.

ISSN No:-2456 –2165

II. LITERATURE REVIEW

Studies on image compression and steganography have been an active area of research from the beginning of the digital image processing. The use of preprocessing methods for improving compression rate and elevating the level of encryption has interested many researchers. Here we briefly explain some articles. In a research done by in 2012, he used a method of embedding in consecutive pixels. According to his technique, the message with the hidden data is saved in the difference between the values of the consecutive pixels' gray levels. Here the gray level range is within 0 to 255. Selecting this range according to the sensitivity of the human visual system leads to the color change. After that the image is divided to anon-overlapping two pixels blocks. Then the difference between the gray levels of the consecutive pair of pixels d is calculated. Thus in parts of the image that the difference between the consecutive pixels is high, the sensitivity of the human visual system is low and therefore more information are saved. In an article by Reddy and others in 2004, he offered a steganography method according to singular value decomposition and discrete wavelet transform. In this type of steganography which is driven from the composition and decomposition of the singular value and discrete wavelet transform, two domains of spatial and frequency steganography were compounded. In this method, discrete wavelet transform is applied on both image and image In this approach, it applies discrete wavelet transform to both images. In a paper submitted in 2012 by d.rajedi and others, they proposed a simple method of hiding information. This method includes the involvement of different secret keys in various stages with the implementation of various matrixes and summing a series of handwritten codes.

The proposed method in this paper can be thought as a ladder, in which the normal and encrypted texts are embedded upon the first and final steps. Furthermore in this paper, d.rajedi applied his method on the three-dimensional image. First the typical text simply and without any changes enters to this model and then is followed by a series of transformations, operations of changing information and handwritten codes. Finally it converts to an object with the name of RNS coded object. We can use the produced RNS object as the background of images. This approach is implemented on the images with the use of the alpha factor (the alpha character is connected to the clarity character of the images). Ultimately we have a clear image in the background of the main image. This scheme consists of three main parts which are the simple text encryption, the method of decryption of the encrypted text and the RNS model.

III. PERFORMANCE ANALYSIS

The overall block diagram of the proposed information security system is shown in Fig. 1. The input biometric signatures are first encoded using individual orthogonal codes and then multiplexed together. The encoded and multiplexed image is now embedded into the cover image by using a secret key for bit selection and replacement purpose. The stego image is finally encrypted using another set of keys employing the MRJTC technique. The orthogonal encoding scheme is depicted in Fig. 2, where the input images containing biometric information are expanded in one dimension and then multiplied by the respective orthogonal code. The individual encoded images are then superimposed on a common spatial domain. If gi(x, y) is the expanded form of the i_th input image fi(x, y), and ki(x, y) is the respective orthogonal code, then the encoded and multiplexed image can be obtained as (1)A Walsh code is employed in this paper to produce the orthogonal codes, which can be implemented by applying the Hadamard transform on 0 (zero) repeatedly as described below [12]. (2) (3)The set of codes are generated in the form of a square matrix, where the length of the matrix is 2mand m is the number of independent codes. Then a color cover image is selected as the cover image to hide the confidential biometric information. The cover image can be any image, even another biometric image like face image.

ISSN No:-2456 –2165

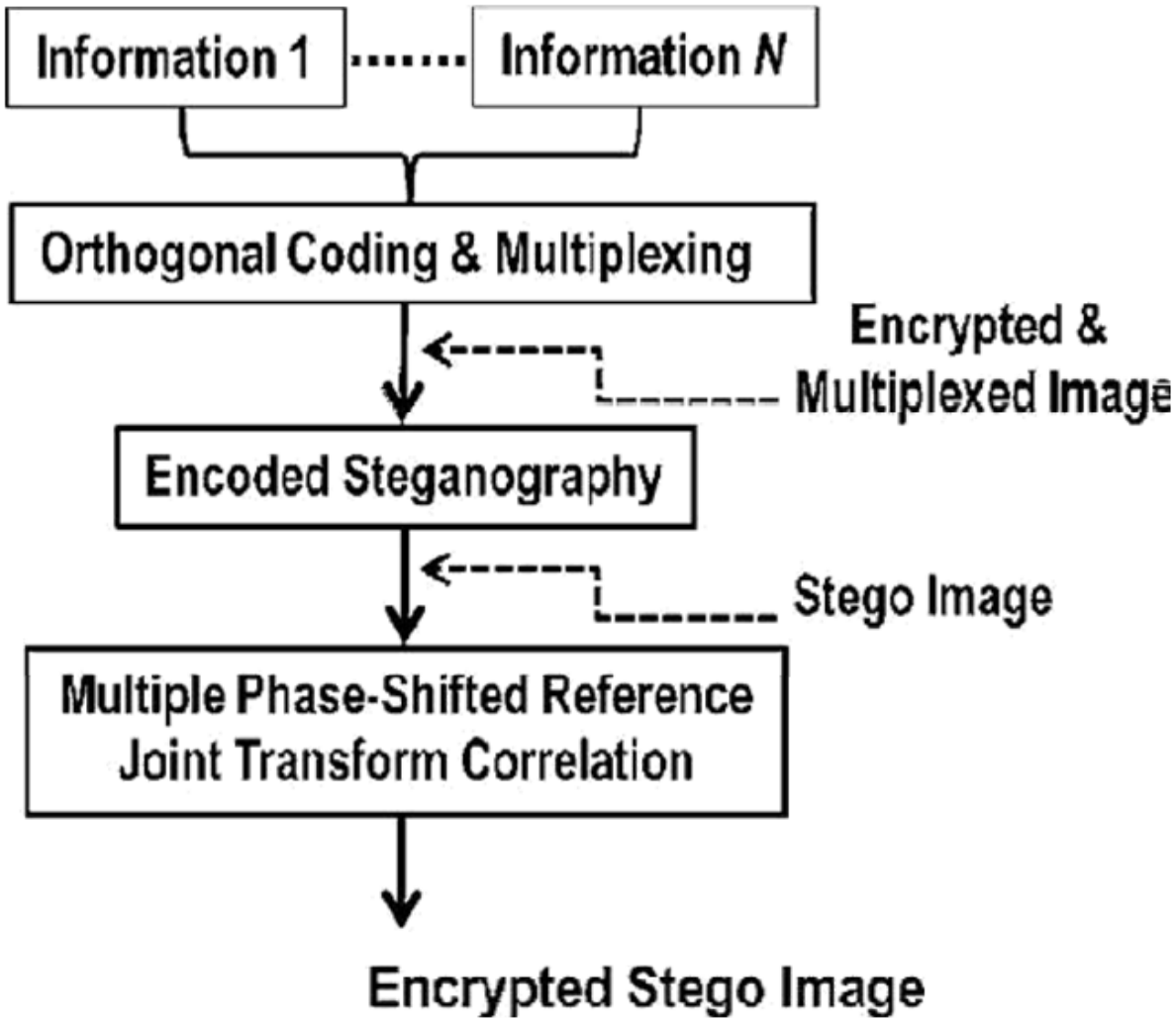

Fig 1 Block Diagram of the System

The proposed steganography process employs a pseudo-random plane generated using a secret key to select a bit from the three LSBs of each pixel. The selected bits from the cover image are then replaced by the corresponding bits of the encoded and multiplexed 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 plaintext stego image, d(x, y), is added to the phase-Shifted

Then a modified JPS signal is developed using the following relation. Inverse Fourier transformation yields the encrypted image as given by

keys in each channel, which yields four joint images as given Applying Fourier transformation to each of the joint images in Eqs., the magnitude spectra are recorded as four joint power spectrum (JPS) signals as given by

$$f1(x, y) = c(x, y) + d(x, y) \quad (1)$$

$$f2(x, y) = JC(x, y) + d(x, y) \quad (2)$$

$$f3(x, y) = -c(x, y) + d(x, y) \quad (3)$$

$$f4(x, y) = -JC(x, y) + d(x, y) \quad (4)$$

$$S(u, v) = S1(u, v) + jS2(u, v) - S3(u, v) - jS4(u, v) = 4C*$$

(u, v)D(u, v) (12) s (x, y) 4c (x, y) * d (x, y)

ISSN No:-2456 –2165

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.

The recovered hidden image from the above step contains multiple biometric signatures that were encoded and multiplexed together. To decrypt specific information, the recovered image is multiplied with the respective encryption key. Then a threshold operation is performed depending on the format of the orthogonal codes. Another salient feature of the proposed technique is that no additional processing step is required to demultiplex as this is automatically accomplished during the correlationoperation.

IV. RESULTS AND DISCUSSION

The proposed information security system was simulated using MATLAB software. Three sets of different biometric signatures employed including fingerprints, iris scans, hand writing and text data. A Walsh code of length 4 was employed for encoding purpose.

(a)

A- Before Steganography

(b)

B-After Steganography

V. CONCLUSION

Thus an efficient method of biometric data hiding using steganography with the help of orthogonal codes as the secret key can be implemented in transform domain using joint transform correlation .It will result in efficient identification of biometric features and only authorized person can be able to access it effectively. It can also provides high security due to threefold encryption techniques, i.e., orthogonal coding, LSB substitution and MRJTC technique. It provides an efficient method for secure information transmission through long channels. It is helpful mainly in real time applications. As a future scope , this method can be used along with cryptographic systems to provide better copyright protection and also in applications that require personal identifications.

REFERENCES

[1]. A.K. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP J. Adv.Signal Process. 2008 (2008), ID. 579416.

[2]. R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, Biometric identifica-tion through hand geometry measurements, IEEE Trans. Pattern Anal. Mach.Intell. 22 (10) (2000) 1168–1171.

[3]. Y.C. Feng, P.C. Yuen, Binary discriminant analysis for generating binary facetemplate, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 613–624.

[4]. M. Fouad, A. El Saddik, Z. Jiying, E. Petriu, A fuzzy vault implementation forsecuring revocable iris templates, Proc. IEEE Int. Syst. Conf. (SysCon)(2011)491–494.

[5]. L. Delac, M. Grgic, A survey of biometric recognition methods, Proc. Int. Symp.Electron. Mar. (2004) 184–193.

[6]. D. Bala, Biometrics and information security, in: Proceedings of the Fifth AnnualConference on Information Security Curriculum Development (InfoSecCD '08)ACM, 2008, pp. 64–66.

[7]. J.E. Mills, S. Byun, Cybercrimes against consumers: could biometric technologybe the solution? IEEE Internet Comput. 10 (4) (2006) 64–71.

[8]. A. Chen, V. Chandran, Biometric template security using higher order spec-tra, in: Proceedings of IEEE International Conference on Acoustics, Speech andSignal Processing, 2010, pp. 1730–1733.

[9]. A. Cheddad, J. Condell, K. Curran, P. McKevitt, Biometric inspired digital imagesteganography, in: Proceedings of 15th Annual IEEE International Conferenceand Workshop on the Engineering of Computer Based Systems (ECBS 2008),2008, pp. 159–168.

[10]. X. Luo, Z. Hu, C. Yang, S. Ga, A secure LSB steganography system defeatingsample pair analysis based on chaos system and dynamic compensation, in:Proceedings of The 8th International Conference on Advanced CommunicationTechnology, 2006, pp. 1014–1019, 2

[11]. A.D. Ker, Steganalysis of embedding in two least-significant bits, IEEE Trans.Inf. Forensics Secur. 2 (1) (2007)46–54.

[12]. M. Goljan, J. Fridrich, T. Holotyak, New blind steganalysis and its implications,in: Proceedings of SPIE in Security, Steganography and Watermarking of Mul- timedia Contents VIII, 2006, pp. 1–13,6072.

[13]. F. Pernus, S. Kovacic, L. Gyergyek, Minutaie based fingerprint registration, IEEEPattern Recognit. (1980) 1380.

[14]. P.M. Mudegaonkar, R.P. Adgaonkar, A novel approach to fingerprint identifica-tion using gabor filter-bank, ACEEE Int. J. Netw. Secur. 2 (3) (2011)10–14.

[15]. M.N. Islam, Encryption and multiplexing of fingerprints for enhanced secu-rity, in: Proceedings of IEEE Long Island Systems, Applications and TechnologyConference (LISAT), 2011.[16] M.F. Islam, M.N. Islam, A secure approach for encrypting and compressing bio-metric information employing.