ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

DATA HIDING AND BIOMETRICSMERGING METHOD USING FACE AND FINGER PRINT IMAGES

REKHA.N[1]
P.G Scholar
M.E-Communication systems,(Dept of ECE)
Idhaya engineering college for women,
Chinnasalem.

RANJITH MARIYAL.J[2]
Assistant professor,
Department of ECE,
Idhaya engineering college for women,
Chinnasalem.

ABSTRACT

The proposed work objective is accessing element through remote authentication by hiding the encrypted biometric signal within face image**.**The biometric input signal is encrypted by using the Arnold Transform algorithm and it is hided into the cover image(face) with Qualified Significant Wave Tree(QSWT).The cover image is the image of a person. The cover image is first compressed and transmitted through the wireless channel for remote authentication. The cover image and encrypted signal information is separately extracted using the IWT and the biometric signal is decrypted by Inverse Arnold Transform Algorithm.The Arnold Transform Algorithm increases the Normalized Cross Correlation (NCC) value to improve the quality of the reconstructed image. The proposed work has minimum error than the existing.The problems overcome by the proposed project are such as data loss, complexity and accuracy of biometric signal .**Applications**: In military areas for the confidential transmission of data in a secured manner.

KEYWORDS:RemoteAuthentication,Biometrics ,QSWT,Arnold Transform.

I. INTRODUCTION

The authentication is used to confirm the identity or originality of the person by ensuring the details which are given by that person. There are two types of authentication namely positive authentication and negative authentication. In this the positive authenticationis already implemented in the existing systems. In order to detect and eliminate In the example there is a system based on password based authentication. The system contains positive authentication with a set of limited passwords for each and every user which was saved in a separate file. If the intruders crack the file the may enter into the users account. Whereas in the negative authentication, there is a anti-password space which contains the user should undergo retinal pattern, facial reorganization, DNA sequence, other biometric identifier etc. These are inherence factor.Referring advantages and disadvantages of the remote authentication technique the biometric signal is found to be best technique for authenticating purposes. The biometric signals are already used in the existing system. For submitting as password in the smart cards alone the biometric signal is used. In the hybrid crypto-steganography schemes the biometric signal can be implemented. In order to make the people to not understand the image the cryptographic technique is used to scramble the original biometric signal into scrambled image, then hide the scrambled image from the intruders. Steganographictechnique is implemented to hide the scrambled biometricsignal into the cover image that is the image of the person.In the proposed system we implemented some methods and technique to overcome the problem which has been faced in the existing remote authentication system. Here the head-and-body detector is used to extract the face and body of the person from the image that is Video Object (VO).

I.IREMOTE AUTHENTICATION

The one-way hash function technique was implemented in the remote password

authentication scheme which was proposed by Lamport . In that system the user id and the passwords are maintained in separate verification table. It is difficult to maintain the verification table in the remote server. The attackers can modify the variables that are passwords by cracking the verification table. In order to overcome the weakness in this remote authentication technique Diffie-Hellman Key agreement protocol is reported . In this, the session key is used to encrypt and decrypt the message which have been communicated by using the symmetric encrypt system. In that the random cryptographic keys are generated, so that it is difficult to memorize that password as well as it is difficult to store random password in Whereas the passwords which are used here is simple and can be easily guessed by attackers. Some users will use same password for all applications. In such case if the attacker finds the password of the user in a single application means they can easily access the other applications of the same user. The remote authentication scheme in smartcards using dynamic user's identity is another technique which is proposed to overcome defects in the previous techniques. The use of static password in smartcards through wireless channels may leak the details about the user. In order to overcome the difficulties by using the static password that is constant password for the smart cards in the proposed scheme they are using dynamic passwords that is the password can be changed for each and every transactions. So there is no chance for intruders (or) attackers to guess the password.so the remote authentication is further improved by using it in secret information transformation in very confidential areas.

I.II STEGANOGRAPHY METHODS

The steganographic technique is the process of hiding data into the image in order to provide the security for the data. Many compression techniques are used in the literature for steganography. The Qualified Significant Wavelet Trees (QSWTs) is used in this technique to hide the image into the cover image.The Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are used to hide data into images which is in JPEG, MPEG etc., formats. By using this methods the lossy messages are send through wireless channels without any loss during transmission and it will protect the hided data from attacks. Even though the process will protect the data loss, the loss of data will occur in some minute area. There are two components used in steganography of the image namely soft-authenticator watermark and chrominance watermark. The soft authenticator watermark is used for authentication purposes to avoid image tampering. The chrominance watermark is used to enhance the compression efficiency of the image. The DWT and Integer Wavelet Transform (IWT). In that the encrypted key and the secret image is hided into the cover image. But it is quite complex to implement the embedding algorithm.The hided information can be easily found when the attacker knows the embedding algorithm.

II.PROPOSED REMOTE SERVICE ACCESS WITH BIOMETRICS

The main process done here is steganography and cryptography is combined. The process of transforming a digital image into another meaningless image by scrambling the original image is known as Arnold scrambling algorithm. By this algorithm the digital image gets preprocessed before hiding the image into the cover image. The non-password technique can be followed by scrambling and hiding image into another image. So there is no need to memorize user id and password. This technique provides confidential and secure data transmission. To change the distribution of error bit in the image some watermarking techniques implies image scrambling method before hiding the image into another image. Many digital watermarking techniques uses Arnold transformation algorithm before it gets processed. This transformation algorithm undergoes images with (N* N) pixels. The order

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

of digital image matrix is representedasN. The transformation specified here is two-dimensional Arnold Scrambling. Here the coordinate (x, y) which is present in the right side is the coordinates of input image expressed in equation (1). Then the coordinate (x', y') which is given in the left side is the coordinates of output scrambled image. The iterative process should be done for n successive nodes which can be expressed in Equation (2),

$$PXY\ (n+1) = APXY\ n \quad (1)$$

$$(\text{mod } N)\ PXY\ n = (X,Y)T \quad (2)$$

Where n denotes the number of iterations, n = 1,2,3… the iteration process will continues until all the pixel in the given image gets transformed. Where cycles undergoes transformation is denoted as T whereas size of the image is represented by N. The Arnold Transform algorithm shows the transformation of original image into scrambled one. So that the intruders can't get the original image even though they hack the data while transmitting over wireless channels. Because after scrambling the image gets vectorized that is the original image is not visible to others. The sender and the receiver alone knows the rounds which was undergone while generating chaotic map. The key which was used to generate the chaotic map is very simple while comparing with other encryption technique. Then the original image will not get revealed in the wireless transmission. Therefore the Arnold transformation algorithm plays a major role in the overall encryption techniques. In this system before hiding image into another image the secrete image gets encrypted by the Arnold transformation algorithm. Because after scrambling the image gets vectorized that is the original image is not visible to others. The sender and the receiver alone knows the rounds which was undergone while generating chaotic map. Here, we hide a finger print behind the face image for accessing more secured manner and to prevent our account secrets.

FACE DETECTION

The skin-tone colors are limited to a small area of the Cr-Cb chrominance plane of the YCrCbcolorspace. Then all pixels of an image can be checked whether they belong to the skin tone color area or not by using a Bayesian Formula. In the proposed face watermarking scheme, face detection is automatically performed using the algorithm. According to this algorithm skin-tone colors distribution is approximated using a two-dimensional Gaussian density function. The adapted Gaussian model combined with a minimum risk threshold, estimated using the maximum likelihood criterion on the training set, is applied to the input image producing a binary image mask, which guides the face watermarking procedure. Afterwards morphological operations (opening and closing) are applied to spatially filter the obtained image masks, while the morphological distance transform and size distribution techniques are used to isolate the disconnected areas and provide separate skin segments. Shape features are also employed to discard skin segments that possess irregular shape. Finally remaining segments are bounded by rectangles and pixel verification is performed within each rectangle according to the adopted algorithm.

III. QUALIFIED SIGNIFICANT WAVELET TREE

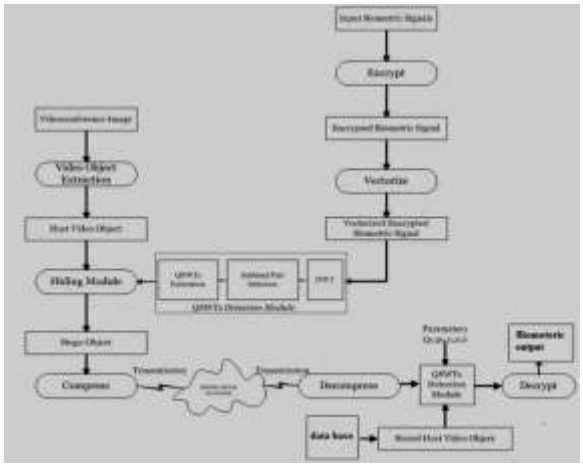
By applying the DWT once to an image, four parts of high, middle, and low frequencies (i.e. LL1, HL1, LH1, HH1) are produced, where sub bands HL1, LH1 and HH1 represent the finest scale wavelet coefficients. In the proposed face oriented watermarking scheme, coefficients belonging to the best Qualified Significant Wavelet Trees are chosen as the target coefficients for casting the watermark . Firstly a parent-child relationship is defined between wavelet coefficients at different scales, corresponding to the same location. Every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

corresponding to the same spatial location at thenext finer scale of similar orientation are called children. For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants.

From fig 1.b,the remote authentication using encryption ,QSWT module hiding information, DWT for compression and decryption of original information is clearly drawn.The biometric signal is encrypted using the Arnold Transform Algorithm and the host object image is taken and the biometric signal encrypted is hided in QSWT module. The image obtained is stego-object image. It is compressed and transmitted and receiver after receiving decompress and decryption is done to get original information and it is accessed as a secret code.



I.b) Remote Authentication activity diagram.

DISCRETE WAVELET TRANSFORM

The Discrete Wavelet Transform is used to hide information like text, audio, video, images etc., into cover image. The Discrete Wavelet Transform is also known as DWT. Analysis on multi resolution of image is done by Discrete Wavelet Transform. The steganography technique is implemented in the discrete wavelet transform. In this technique the cover image is divided into four equal parts with respect to the resolution of the image that is (128*128) bits. The four parts is represented as low, middle and high frequencies that is represented as LL, HL, LH and HH. There are two operation which undergoes in DWT namely Horizontal operation and vertical operation. First step undergoes horizontal operation that is the analysis done in horizontal direction the pixels from left to right and then stores the addition of the nearby pixels in the left side. The subtraction of the neighboring pixels is done and the difference value is stored into the right side. In the original image left side that is sum denotes Low frequency part (L) and the right side that is the product denotes High frequency part (H).

Vertical operation is done in second step. The pixels are analyzed in vertical direction that is from top to bottom. The addition of the nearby pixels is performed and on the top the sum valued gets stored. Then the subtraction of the neighboring pixel is performed and on the bottom the difference value gets stored. Then LL, LH, HL, HH are the four sub-bands will generated after this process. The original image is same as the low frequency band in sub-bands. The higher level DWT is obtained after decomposing the LL sub-bands. The vertical, horizontal, diagonal sub-bands are represented as LH, HL, HH respectively. The DWT is the process of hiding image into another image. Then the image is divided into four different parts with respect to the pixels (240*240 pixels). Then the image is inserted to the parts with lowfrequency level.

THE IMAGES TO BE PROCESSED

III.A) i)Finger Print Image ii)Face Image

MESSAGE RECOVERY

Consider the Stego-object has reached the destination, the encrypted biometric signal is extracted by inverse DWT. The decryption isperformed to get the hided information and original image.

RESULT

III.B) Original finger print image recovered.

SECURITY ANALYSIS FOR THIS METHOD

The security analysis deals with the secret transformation of message without any loss and cannot be accessed by the attackers. As we use the Arnold Transform and DWT methods there is accuracy for the secret information transferring and accessing.The transform will perform no of transformations and the attacker cannot access the signal transferred which is hided in aimage.The finger print is not accessed easily and more secured.

CONCLUSION

The Biometric signals were used very common in our day to day life and in accessing in a more secured manner we use steganography along with the encryption model so the attackers can't get any information. QSWT provides high level of robustness in compression standards. In future research,the loss in biometric signal accuracy should be made much less and the biometric with different mode signals can be tried for accessing with security for highly authenticated information's and legal authentications.

REFERENCES

[1] A. Madero, ''Password secured systems and negative authentication,'' Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Technol., Cambridge, MA, USA, 2013. [Online]. Available: http://hdl.handle. net/1721.1/90691

[2] A. Pascual and S. Miller, ''Identity fraud report: Data breaches becoming a treasure trove for fraudsters,'' Javelin Strategy Res., Pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.

[3] E.-J. Yoon and K.-Y. Yoo, ''Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,'' J. Supercomput., vol. 63, no. 1, pp. 235–255, Jan. 2013.

[4] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, ''Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme,'' in Computational Science and Its Applications (Lecture Notes in Computer Science), vol. 7335. Berlin, Germany: Springer-Verlag, 2012, pp. 391–406.

[5] M.-C. Chuang and M. C. Chen, ''An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,'' Expert Syst. Appl., vol. 41, no. 4, pp. 1411–1418, Mar. 2014.

[6] L. Lamport, ''Password authentication with insecure communication,'' Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

[8] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, ''A password authentication scheme over insecure networks,'' J. Comput. Syst. Sci., vol. 72, no. 4, pp. 727–740, Jun. 2006.

[9] M. Jakobsson and M. Dhiman, ''The benefits of understanding passwords,'' in Mobile Authentication (SpringerBriefs in Computer Science). New York, NY, USA: Springer-Verlag, 2013, pp. 5–24.

[10] M. Weir, S. Aggarwal, M. Collins, and H. Stern, ‘‘Testing metrics for password creation policies by attacking large sets of revealed passwords,’’ in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 162–175.

[11] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, ‘‘A more efficient and secure dynamic ID-based remote user authentication scheme,’’ Comput. Commun., vol. 32, no. 4, pp. 583–585, Mar. 2009.

[12] M. K. Khan, S.-K. Kim, and K. Alghathbar, ‘‘Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme,’’’ Comput. Commun., vol. 34, no. 3, pp. 305–309, Mar. 2011.

[13] E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, ‘‘A security enhanced remote user authentication scheme using smart cards,’’ Int. J. Innovative Comput., Inf. Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.