FACE RECOGNITION USING FINGERPRINT - STEGANOGRAPHIC MECHANISM

V.Ezhilarasi [1], G.Jayanthi[2] , Ms.J. Gayathri [3] M.Tech
1,2- final year ECE, 3-Assitant professor
[1]Department Of ECE , Prince Shri Venkateshwara Paadmavathy Engineering College , ponmar, Chennai, India.
[2]Department Of ECE , Prince Shri Venkateshwara Paadmavathy Engineering College , ponmar, Chennai, India
.[3]Assistant professor , ECE Department , Prince Shri Venkateshwara Paadmavathy Engineering College , ponmar, Chennai, India.

ABSTRACT

In wireless communications, sensitive information is frequently exchanged, requiring remoteauthentication. Remote authentication involves the submission of encrypted information, along with visual. This paper proposes a robust authentication mechanism based on semantic segmentation, Arnold transform, and data hiding. Assuming that user X wants to be remotely authenticated, initially X's video object (VO) is automatically segmented, using a head-and-body detector. Next, one of X's biometric signals is encrypted by a chaotic cipher. Afterwards, the encrypted signal is inserted to the most significant wavelet coefficients of the VO, using its qualified significant wavelet trees (QSWTs). QSWTs provide both invisibility and significant resistance against lossy transmission and compression, conditions that are typical of wireless networks. Finally, the inverse discrete wavelet transform is applied to provide the stego-object. bandwidth efficiency measures indicate the promising performance of the proposed biometrics-based authentication scheme.

Keyword ***:Biometrics hiding*****, steganographic system, remote authentication, biometrics, QSWTs,video object.**

INTRODUCTION :

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. The two main directions in the authentication field are positive and negative authentication. Positive authentication is well-established and it is applied by the majority of existing authentication systems. Negative authentication has been invented to reduce cyber attacks the following factors should be verified: the ownership factor: Something the user has(e.g. ID card, security token, cell phone etc.) the knowledge factor: Something the user knows(e.g., a password, a PIN, a pattern etc.)the inherence factor: Something the user is or does(e.g. Fingerprint, retinal pattern, DNA sequence, face,other biometric identifier etc.) In 2012 identity fraud in US affected 12.6 million consumers, and resulted in a loss of $4.6billion($365/consumer). Furthermore, the probability of becoming an identity fraud victim is approximately

5.3%. As a result, robust remote human authentication becomes one of themost important issues of contemporary societies and severalworks have been proposed in the literature to effectively tackle it. The majority is based on passwords or smart cards. The pros and cons of these systems are explained and the use of biometrics is suggested as an alternative. Biometrics have already been incorporated in remote authentication but only as password substitution in smart cards.

2. PROPOSED SYSTEM:

The proposed remote human authentication scheme over wireless channels under loss tolerant transmission protocols, aims to ensure: (a) robustness against deciphering, noise and compression, (b) good encryption capacity, and (c) ease of implementation. For this purpose we:

(a) employ wavelet-based steganography, (b) encrypt biometric signals to allow for natural authentication,

(c) involve Arnold transform for encryption to increase securityand (d) the encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing. The overall architecture and data flow of the proposed scheme is illustrated in Figure 1. Initially the biometric signal is encrypted The use of arnold transformencryption mechanism is used. By applying the SA-DWT once to an area of arbitrary shape, four parts of low, middle, and high frequencies, i.e., *LL*1, *HL*1, *LH*1, *HH*1, are produced. Band *LL*1 (*HH*1) includes low (high) frequency components both in horizontal and vertical direction, while the *HL*1 (*LH*1), includes high (low) frequencies in horizontal direction andlow (high) frequencies in vertical direction. Sub band *LL*1 can be further decomposed in a similar way into four different subbands, denoted as *LL*2, *HL*2, *LH*2, *HH*2 respectively. This process can be repeated several times, depending on the specific application. Subbands *LHN* ,. . . , *LH*3, *LH*2, *LH*1 follow a parent-child relationship. The coefficient at the highest level is called the parent and all coefficients corresponding to the same spatial location at the lower levels of similar orientation are called children. For a given parent, the set of all coefficients at all scales of similar orientation corresponding to the same location are called descendants. Furthermore the wavelet coefficients can be distinguished into two types; the `In-Node' coefficients which belong to the video object area and the `Out-Node' coefficients which do not belong tothe video object.

ARNOLD TRANSFORM :

Pixels‟ positions are altered and if done a number of times, the appearance of the image becomes messy when this scrambling technique is used. It requires the height or width (N x N) of the image that needs to undergo the process. The periodic trait of the Arnold Transform has much to do with the dimension of the image to be decoded depending on the transformation time (T), which also alters according to the image ‟ dimension. Image iterations occur when this technique is applied. A secret key derived from this iteration number is used to encrypt and extract the secret image. If some hackers detect the watermark signal, they need to use this key to get the watermark. Even if they have the key, they still have to undergo a lot of testing to recover the original watermark data. Thus, security and concealment of the watermark is further improved by the use of this scrambling technique. Thus defined, 2 - D Arnold transform for an N X N image is

$$[X';Y'] = [\,1\ 1\ ;\ 1\ 2\,] * [\,x\ ;\ y\,] \bmod(N)$$

$x, y \in \{0,1,..., N - 1\}$, (x, y) and (x′, y′) are the coordinate s of the pixels before - and - after scrambling

BLOCK DIAGRAM

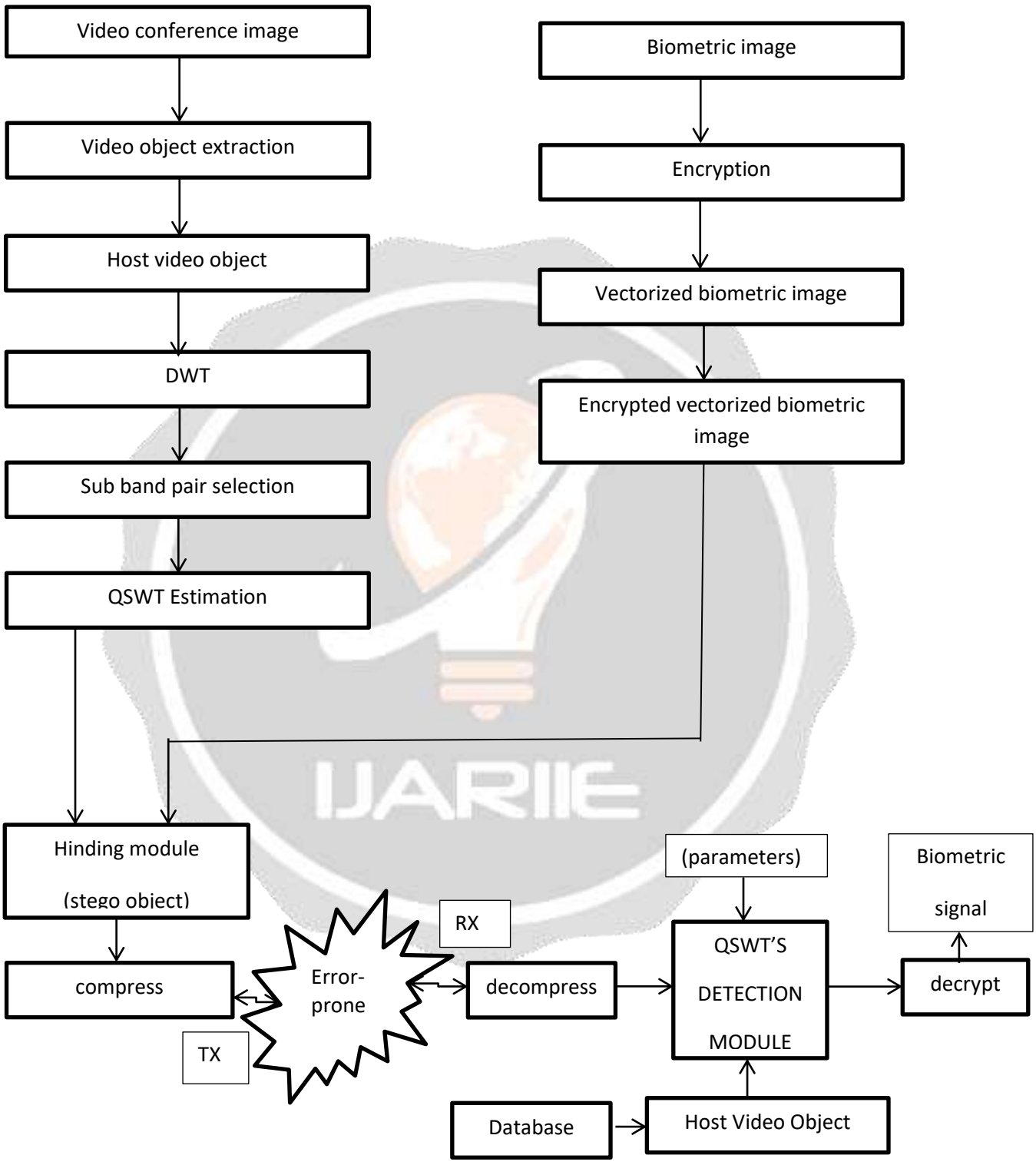


Figure 1: Block diagram of proposed system

Arnold transform:

1) Only two dimensions allowed.
2) Arnold Transform is defined only for squares.

Encryption:

p = [1 1 ; 1 2] * [x ; y];

out(mod(p(2), m)+1, mod(p(1), m)+1) = in(y+1, x+1)

x=row, y=column, out=encrypted image, in=input image

Decryption:

p = [2 -1 ; -1 1] * [x ; y];

out(mod(p(2), m)+1, mod(p(1), m)+1) = in(y+1, x+1);

Advantages of this algorithm:

a) Addresses both spatial and temporal domains.
b) Faster and less complex.
c) Hiding Capacity of the secret data bits is high.
d) Hiding capacity is based on the pixel number.

Application:

a) Confidential communication and secret data storing
b) Protection of data alteration
c) Access control system for digital content distribution
d) Media Database systems
e) Banking applications
f) Military applications

RESULT AND DISCUSSIONS

We have compared our approach with various compression schemes in order to show the worthiness of the considered scheme in table 1.

Table 1.Biometric signal retrieval results for the stego-object

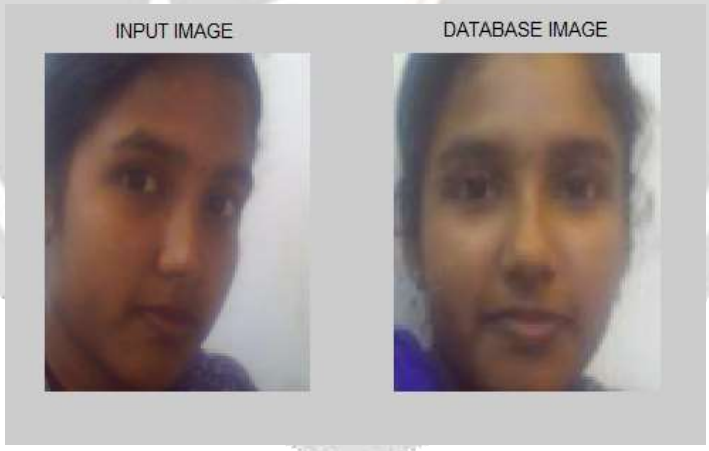
JPEG COMPRESSION RATIO=0.6		
BER1	BER2	BER3
R	R	R

JPEG COMPRESSION RATIO=3.3		
BER1	BER2	BER3
R	R	R
JPEG COMPRESSION RATIO=10.7		
BER1	BER2	BER3
NR	NR	NR

The use of a specific statistical steganalsis method may not be reasonable instead a universal statistical steganalysis technique may work, provided it successfully determines the steganographic algorithm. Regarding more specific

Table 1: comparison of various BER techniques or schemes

RESULT OBTAINED,



BIOMETRIC OUTPUT

4.CONCLUSION

Biometric signals enter more and more into our everyday lives, since governments, as well as other organizations, resort to their use in accomplishing crucial procedures. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. The scheme offers possible advantages that is it provides a secondary complementary authentication mechanism in case when the person under authentication is also captured by the camera and in every recent transaction the overall architecture can store the latest sample pictures of one face and body that could help in cases of hybrid remote authentication.

Since steganography by itself does not ensure secrecy, it was combined with a Arnold transform encryption method. The proposed procedure, except of providing results that is imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security

5.REFERENCES

1. *Arun Ross and Salil Prabhakar(2004), 'An Introduction to Biometric Recognition,' IEEE Transactions on Circuits Systems for Video Technology, vol.14(1), pp. 4-20.*
2. *Chen. T.-Y, Ling.C.-H, and Hwamg.M.-S.,(2014) 'Weakness of the yoon-kim-yoo remote user authentication scheme using smart cards,' in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications, pp. 771-774.*
3. *Chuang.M.C and Chen.M.C,(2014) 'An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,' Expert Systems with Applications, vol.41, no. 4, pp. 1411-1418.*
4. *Kim.H, Jeon.W, Lee.K, Lee.Y, and Won.D,(2012) 'Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme,' in Computational Science and Its Applications, ser. Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, pp. 391-406.*
5. *Liao.I.-E, Lee.C-C, and Hwang.M.-S, (2006) 'A password authentication scheme over insecure networks,' Journal of Computer and System Sciences, vol. 72, pp. 727-740.*
6. *Madero.A,(2013)'Password secured systems and negative authentication.' Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, Engineering Systems Division.*
7. *Madhusudhan.R and Mittal.R.C, (2012), 'Dynamic id-based remote user password authentication schemes using smart cards: A review,'Intelligent Algorithms for Data-Centric Sensor Networks, vol. 35, no. 4, pp. 1235-1248.*
8. *Ramkumar.M and Akansu.A.N,(2001) ' Capacity estimates for data hiding in compressed images,' IEEE transactions on Image Processing , vol. 10(8), pp. 1252-1263.*
9. *Wang.Y.-y., Liu. F.-x Xiao and Dan.J,(2009) ' A more efficient and secure dynamic id-based remote user authentication scheme,' Computer Communications, vol. 32, no. 4, pp. 583-585.*
10. *Weerackody.V, Podilchuk. C and Estrella. A,(1996) 'Transmission of jpeg coded images over wireless channels,' Bell Labs Technical Journal, vol. 1(2), pp. 111-126.*
11. *Yoon.E.J, Kim.S.H, and Yoo.K.Y, 'Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme,' International Journal of Innovative Computing, Information and Control,May 2012.*
12. *Yoon.E.J and Yoo.K.Y.(2013), 'Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,' The Journal of Supercomputing, vol.63*