Indian J.Sci.Res. 17(2): 416 - 420, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

WIRELESS NETWORKS : AUTHENTICATION VIA BIOMETRIC VIDEO- OBJECT STEGANOGRAPHY

[1]Aisha Khatoon, [2]Begum, [3]F.Asma begum
[1,2,3]NSAKCET

Abstract-Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, human voice, and so on). This paper proposes a robust authentication mechanism based on semantic segmentation, chaotic encryption, 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 secure force algorithm. 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. Experimental results regarding: 1) security merits of the proposed encryption scheme; 2) robustness to steganalytic attacks, to various transmission losses and JPEG compression ratios; and 3) bandwidth efficiency measures indicate the promising performance of the proposed biometrics-based authentication scheme.

Keywords- Biometrics hiding, steganographic system, remote authentication, QSWTs, video object

I. INTRODUCTION

Authentication involve confirming theidentity of a person or software program, tracing the originsof an artifact, or ensuring that a product is what its packagingand labeling claims to be, confirming the truth of an attribute of a datum or entity. The two main directions in the authentication field are positive and negative authentication.Positive authentication is well-established and it is appliedby the majority of existing authentication systems. Negativeauthentication has been invented to reduce cyber attacks.The difference is explained by the followingexample: Let assume password-based authentication.In positive authentication, the passwords of all users thatare authorized to access a system are stored, usually in a file. Thus the passwords space includes only users passwordsand it is usually limited (according to the number of users).If crackers receive the passwords file, then their work is torecover the plaintext of a very limited number of passwords.On contrary, in negative authentication the anti-passwordspace is created, (theoretically) containing all strings that are not in the passwords file. If crackers receive the very large anti-password file, their work will be much harder. Thisway, negative authentication can be introduced as a new layerof protection to enhance existing security measures withinnetworks. This allows the current infrastructure to remainintact without accessing the stored passwords or creatingadditional vulnerabilities. By applying a real-valued negativeselection algorithm, a different layer is added for authentication,preventing unauthorized users from gaining networkaccess[1].

The proposed scheme is a positive authentication systemand for security reasons elements from at least two, and preferably all three, of the following factors should beverified:

- 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.)

The security based on passwords or smart cards has pros and cons,the use of biometrics is suggested as an alternative.Biometrics have already been incorporated in remote authentication, [2] but only as password substitutionin smart cards.In order to investigate their full potentiality, biometrics canbe incorporated in hybrid crypto-steganographic schemes.In particular, cryptographic algorithms can scramblebiometric signals so that they cannot be understood, whilesteganographic methods can hide the encrypted biometricsignals so that they cannot be seen. In this paper webuild further on this principle to confront the problemof remote human authentication over wireless channels,under loss tolerant protocols. In particular an effectivewavelet-based steganographic method isproposed for hidingencrypted biometric signals into semantically meaningfulVOs such as the head-and-shoulders VO, which is common inseveral teleconferencing applications.

II. RELATED WORK AND CONTRIBUTION

A. REMOTE AUTHENTICATION

Different solutions have been proposed. For instance, Liao et al. [3] proposed a scheme that utilizes the Diffie-

[1]Corresponding Author

Hellman key agreement protocol over insecurenetworks, which allows the user and the system to agree on asession key to encrypt/decrypt their communicated messagesusing a symmetric cryptosystem.However several passwords aresimple and they can be easily guessed or broken. Furthermore, most people use the same password acrossdifferent applications; if a malicious user determines a singlepassword, they can access multiple applications. Additionally: users should always have their smart cards with them in order to do transactions, if a user loses his/hersmart card, he/she will not be able to do any transactions and should wait for the reissuing of the card (sometimes several days).

B. STEGANOGRAPHIC METHODS

Steganographic algorithms can be roughly divided into those performed in the spatial domain and those applied in a transform domain. Among transform-based data hiding approaches, DCT [4] and DWT [5] methods are, by far, the most popular since they are related with popular digital image and video compression schemes (i.e., JPEG, MPEG, JPEG-2000, H264, etc).In [6] fingerprints are hidden in the region of interest of images. Both DFT and DWT domains areexamined. However, again, no encryption is incorporated. Object-oriented data hiding is more secure and robust against deciphering attacks but it usually creates visually sensitive artifacts, thus, lowering the capacity of encryption. Detection of skin like color and feature descriptors are quite robust but rarelylead to large compact objects, reducing further encryption capacity.

C. CONTRIBUTION OF CURRENT WORK

To summarize the contents of this paper, in contrast to existing methods mentioned in the previous sections, its main contributions are analyzed below:

1) Biometrics-based human authentication over wireless channels under fault-tolerant protocols: The overriding majority of current works does not consider fault-tolerant protocols during transmission of stego-objects. With the proposed approach several mobile applications could benefit. For example, in an emerging scenario, let us imagine that a user would like to be authenticated via her cell phone, tablet etc. Her mobile device has a camera, while its touch-screen collaborates with a fingerprints capturing application. In case the signal strength is low, erroneous packets may arrive at the receiver. Thus, a scheme like the proposed one is required.

*2) Automatic extraction of semantically meaningful video objects embedding the encrypted biometric information:*Most of the existing schemes do not consider semantically meaningful VOs as hosts, but a whole image. The proposed scheme offers some possible advantages. Firstly, the scheme provides a secondary complementary authentication mechanism in case when the person under authentication is also captured by the camera. Thus her face and body is transmitted together with another biometric feature forpossible double authentication. Secondly, in every recenttransaction, the overall architecture can store the latest samplepictures of one's face and body. This could help in casesof hybrid remote authentication, when both a machine anda human remotely authenticate a person. The machine canauthenticate the fingerprint and the human can authenticatethe face (like the teller does in a bank). Another advantage has to do with more efficient bandwidth usage, especiallyin the aforementioned case of hybrid remote authentication.An image usually does not only contain semantically meaningfulinformation but also background blocks. On the otherhand, in order to hide a specific amount of information,a host with proper capacity should be selected. If the hostis an image, then irrelevant blocks will also be transmitted,occupying valuable bandwidth. On the contrary, whenthe host is a semantic VO, all transmitted information isrelevant to the authentication task. Last but not least, theproposed scheme allows for more efficient rate control and can better confront traffic congestions. On the other hand, the proposed scheme is content-aware. In case of traffic congestion, the rate control mechanism could discard blocks from the body region that do not also contain hidden information, instead of discarding face areas.

3) Secure force algorithm which works like a one-time pad, to encrypt biometric identifiers: Symmetric encryption is faster, thus in contemporary systems a key of size 2*n* bits is produced (usually *n* 2 [6 11]) and it is exchanged between the communicating entities, using public key cryptography. However, even though large keys are considered to be safe, it has been proven that any cipher withthe perfect secrecy property must use keys with effectively the same requirements as one-time pad keys. In our case, biometric identifiers are encrypted by a secure force algorithm. In the proposed scheme this exchange is also performed by incorporating public key cryptography.

III. THE PROPOSED METHOD

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 biometricsignals to allow for natural authentication, (c) involve aChaotic Pseudo-Random Bit Generator (C-PRBG) to createthe keys that trigger the whole encryption to increase security,and (d) the encrypted biometric signal is hidden in a VO,which can reliably be detected in modern applications thatinvolve teleconferencing.Initially the biometric signalis encrypted by incorporating a chaotic pseudo-random bitgenerator and a chaos-driven cipher, based on mixed feedbackand time variant S-boxes. The use of such an encryption mechanism is justified since,

1) Chaos presents sensitivity to initial conditions,

2) A C-PRBG statistically works very well as a one-timepad generator,

3) Implementations of popular public key encryptionmethods, such as RSA or El Gamal, cannot providesuitable encryption rates. This is why almost all ofthe contemporary encryption algorithms combine symmetricand public key cryptography. On the otherhand the security of these algorithms relies, in theory, on the difficulty of quickly factorizing large numbersor solving the discrete logarithm problem, and, in practice, on the difficulty of recording acoustic emanations from computers during operation.

4) Private-key bulk encryption algorithms such asTriple-DES or Blowfish, similarly to chaotic algorithms,are more suitable for transmission of large amounts ofdata.

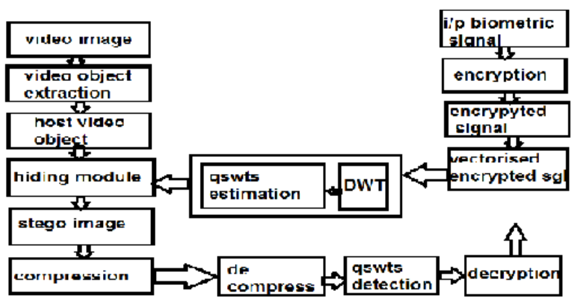

figure1:data flow in the proposed scheme

Afterwards, a head-and-body image of the biometricsignal's owner is analyzed and the host VO is automaticallyextracted based on the method proposed in [7]. Nexta DWT-based algorithm is proposed for hiding the encryptedbiometric signal to the host VO. The proposed algorithmhides the encrypted information into the largest-value QSWTs of energy-efficient pairs of subbands. Compared toother related schemes, the incorporated approach has thefollowing advantages [8]:

_ it is one of the most efficient algorithms of literaturethat facilitates robust hiding of visually recognizablepatterns,

_ it is hierarchical and has multiresolution characteristics,

_ the embedded information is hard to detect by the humanvisual system (HVS),

_ it is among best known techniques with regards tosurvival of hidden info after image compression.

Initially the extracted host object is decomposed intotwo levels by the separable 2-D wavelet transform, providingthree pairs of subbands (*HL*2, *HL*1), (*LH*2, *LH*1) and(*HH*2, *HH*1). Afterwards, the pair of subbands with thehighest energy content is detected and a QSWTs approachis incorporated [9] in order to select the coefficientswhere the encrypted biometric signal should be casted.Finally, the signal is redundantly embedded to both subbandsof the selected pair, using a non-linear energy adaptableinsertion procedure. Differences between the original and thestego-object are imperceptible to the human visual system(HVS), while biometric signals can be retrieved even undercompression and transmission losses.

IV. CHAOTIC ENCRYPTION

Before hiding, each biometric signal is initially encrypted.

A. ENCRYPTION KEYS' GENERATION

In this paper,the generated key has size equal to the size of each biometric signal. Each key is generated by a C-PRBG. In this paper we propose a PRBG based on a triplet of chaotic systems, which can provide higher security than other C-PRBGs [10]. The basic idea of the C-PRBG is to generate pseudo-random bits by mixing three different and asymptotically independent chaotic orbits. Towards this direction let $F1(x1; p1)$, $F2(x2; p2)$ and $F3(x3; p3)$ be three different *1-D* chaotic maps:

$x1(i+1) = F1(x1(i); p1)$

$x2(i+1) = F2(x2(i); p2)$

$x3(i+1) = F3(x3(i); p3)$

where$p1$, $p2$ and $p3$ are control parameters, $x1(0)$, $x2(0)$ and$x3(0)$ are initial conditions and $x1(i)$, $x2(i)$, $x3(i)$ denote thethree chaotic orbits. Then a pseudo-random bit sequence can be defined as:

$$k(i) = \begin{cases} 1 & F3(x1(i); p3) > F3(x2(i); p3 \\ k(i-1) & F3(x1(i);p3) = F3(x2(i);p3) \\ 0 & F3(x1(i); p3) < F3(x2(i); p3) \end{cases} \quad (1)$$

According to this scheme the generation of each bit is controlledby the orbit of the third chaotic system, having asinitial conditions the outputs of the other two chaotic systems [12].

B. THE ENCRYPTION MECHANISM

After generating the initial pseudo-random key, the ciphermodule is activated. Before encryption, the samples of eachbiometric signal are properly ordered. In case of 1-D signals (e.g. voice) the order is defined by the sequence of samples, while in 2-D signals (e.g. fingerprint image) pixels are line perline zig-zag scanned from top-left to bottom-right, providingplain text pixels Pi. Assume that Pi and Cirepresent the *i-th*plain text and *i-th*ciphertext samples respectively (both in *n-bit* formats). Thenthe encryption procedure is defined by:

$Ci = fS(fS(Pi; i) \text{ XOR } xi; i)$ (2)

Where $fS(Pi; i)$ are time-variant nxnS-boxes (bijections defined on0; 1; : : : ; $2n - 1$) and xi is produced from the states ofthree chaotic functions through the bit generation procedure defined in Eq. 1.

C. SECURITY ANALYSIS OF THE CHAOTICENCRYPTION SCHEME

For each biometric signal a key that has size equal to the sizeof the signal to be encrypted is produced. In particular, the first component of the proposed encryption module is theC-PRBG, which controls the encryption process.This component depends on three secret control parameters*p*1, *p*2 and *p*3 and three secret initial conditions *x*1(0), *x*2(0)and *x*3(0). These six variables are exchanged between thesender and receiver using public-key cryptography.

D. DECRYPTION

The decryption module receives at its input a vector ofencrypted samples, the initial control parameters and initialconditions for the triplet of chaotic maps (C-PRBG module)and the initial cipher value *C*0 (used at the first feedback).The procedure is terminated after the final sampleis decrypted.

V. HIDING THE ENCRYPTED BIOMETRIC SIGNAL

The encrypted biometric signal is robustly hidden inthe host video object.QSWTsprovide one of themost robust solutions to data recovery, after several signalprocessing manipulations. In particular let us assume thatthe host video object has been extracted using the methoddescribed in [7]. Next the host video object is decomposedinto two levels using the shape-adaptive discrete wavelettransform (SA-DWT) [11]. By applying the SA-DWT onceto an area of arbitrary shape, four parts of low, middle, andhigh frequencies, i.e., *LL*1, *HL*1, *LH*1, *HH*1, are produced.Band *LL*1 (*HH*1) includes low (high) frequency componentsboth in horizontal and vertical direction, while the *HL*1 (*LH*1),includes high (low) frequencies in horizontal direction andlow (high) frequencies in vertical direction.Subband*LL*1 can be further decomposed in a similarway into four different subbands, denoted as *LL*2, *HL*2,*LH*2, *HH*2 respectively.

Algorithm 1 QSWTs Estimation

```
procedure QSWTest(I ; S; L)
/* I = input frame */
/* S = subband selection (e.g. LH) */
/* L = subband level (e.g. 3) */
/* Thresholds T1 and T2 are globally defined */
[LL; LH; HL;HH] =DWT(S; L -1)
SL-1 =LH
[LL1; LH1; HL1;HH1] =DWT(LL; 1)
SL =LH1
t = 0
QSWT[t] = ϕ
N =rows(SL)
M =columns(SL)
for i = 1 to N do
for j = 1 to M do
if SL(i; j) is In_Node AND |SL(i; j)j|>T1 then
C1 =SL-1(2i - 1; 2j -1) is In_Node AND |SL-1(2i - 1; 2j -1)|>T2
C2 = SL-1(2i - 1; 2j) is In_Node AND |SL-1(2i - 1; 2j)|>T2
C3 = SL-1(2i; 2j - 1) is In_Node AND |SL-1(2i; 2j - 1)|>T2
C4=SL-1(2i; 2j) is In_Node AND |SL-1(2i; 2j)|>T2
if (C1 AND C2 AND C3 AND C4) then
QSWT[t] = SL(i; j) +SL-1(2i - 1; 2j - 1) +SL-1(2i - 1; 2j) +SL-1(2i; 2j - 1) +SL+1(2i; 2j)
t = t + 1
return QSWT
```

VI. EXPERIMENTAL EVALUATION

For evaluation purposes, the proposed video objects-orientedbiometric signals hiding scheme is examined in terms of security, effectiveness and robustness. The general methodology included: (a) extraction of the host video object from a videoconference frame and detection of the QSWTs to embed the encrypted signal, (b) encryption of the fingerprint, (c) embedding of the encrypted signal to the host video object, (d) compression of the final content and simulated noisy transmission, (e) decompression and extraction of the encrypted signal, (f) decryption and (g) authentication.

VII. LIMITATIONS OF PROPOSED SCHEME

In this paper, a robust remote authentication mechanism based on semantic segmentation, chaotic encryption and data hiding has been presented.

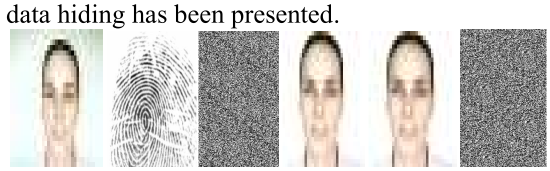

FIGURE 4.Indicative results: (a) The 1st video frame , (b) The (assumed) fingerprint, (c) Encrypted biometric signal, (d) The automatically extracted video object, (e) stego-object containing the encrypted biometric signal of Fig. 4c, (g) Decryption of pattern of Fig. 4c using a key thatdiffers by just one bit.

Even though several successfulexperiments have been carried out, the proposed scheme hasstill its limitations and open issues, which should be further,investigated in future research. In particular:

_ Since the recipient should possess the original host videoobject, the method is non-blind, a feature that is undesirablein some specific applications.

_ Secure force algorithm encryption is a relatively new field of research,and it will take some time for its security analysis tomature.

_ In case of the C-PRBG, even though several combinationsof control parameters have been tried, a systematictheory about chaos in discrete space is needed.

_ The iteration of the chaotic systems implies workingwith real numbers. Since our implementation is donewith finite precision arithmetic, round-off operationscould lead to a non-invertible encryption procedure.

_ Last but not least, the steganographic scheme is basedon QSWTs. Thus if an image has several homogeneousareas, then either its capacity or its robustnessmay be greatly reduced.

VIII. CONCLUSION

Biometric signals enter more and more into our everydaylives, to their use in accomplishing usage (e.g. citizen authentication). Thus there is an urgent needto further develop and integrate biometric authenticationtechniques into practical applications.In future research, the effects of compression and mobiletransmission of other hidden biometric signals (e.g. voice oriris) should also be examined. The problem of lost biometricdata is also of high interest.

REFERENCES

[1] A.Madero, ``Password secured systems & negative authentication,"Ph.D. dissertation, Dept. Eng. Manage., Massachusetts Inst. Tech,Cambridge, MA, USA, 2013. http://hdl.handle.net/1721.1/90691

[2] E.-J. Yoon and K.-Y.Yoo, ``Robust biometrics-based multi-server authenticationwith key agreement scheme for smart cards on elliptic curvecryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235_255, Jan. 2013.

[3] M.-C. Chuang and M. C. Chen, ``An anonymous multi-server authenticatedkey agreement scheme based on trust computing using smart cards andbiometrics," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1411_1418, Mar. 2014.

[4] N. Provos and P. Honeyman, ``Hide and seek: An introduction to steganography,"*IEEE Security Privacy*, vol. 1, no. 3, pp. 32_44, May/Jun. 2003.

[5] P.-Y. Chen and H.-J. Lin, ``A DWT based approach for image steganography,"*Int. J. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 275_290, 2006.

[6] K. Zebbiche and F. Khelifi, ``Region-based watermarking of biometricimages: Case study in fingerprint images," *Int. J. Cryptography Inf. Security.*,vol. 2008, Jun. 2008, Art. ID 492942.

[7] N. Doulamis, A. Doulamis, K. Ntalianis, and S. Kollias, ``An efficient fullyunsupervised video object segmentation scheme using an adaptive neuralnetwork classifier architecture," *IEEE Trans. Neural Networks.*, vol. 14, no. 3,pp. 616_630, May 2003.

[8] M.-S. Hsieh, D.-C.Tseng, and Y.-H. Huang, ``Hiding digital watermarksusing multiresolution wavelet transform," *IEEE Trans. Ind. Electron.*,vol. 48, no. 5, pp. 875_882, Oct. 2001.

[9] K. S. Ntalianis, N. D. Doulamis, A. D. Doulamis, and S. D. Kollias,``Automatic stereoscopic video object-based watermarking using qualified significant wavelet trees," in *Proc. IEEE Int. Conf. Consumer. Electronics.*,June. 2002, pp. 188_189.volume 4, no. 1, March 2016.

[10] S. Li, X. Zheng, X. Mou, and Y. Cai, ``Chaotic encryption scheme for realtimedigital video," *Proc. SPIE*, vol. 4666, pp. 149_160, Mar. 2002.

[11] S. Li andW. Li, ``Shape-adaptive discretewavelet transforms for arbitrarilyshaped visual object coding," *IEEE Trans. Circuits Syst. Video Technol.*,vol. 10, no. 5, pp. 725_743, Aug. 2000.

[12] KlimisNtalianis and Nicolas Tsapatsouli, "remote authentication via biometrics: a robust video-object steganographic mechanism over wireless networks," *ieeetransactions on emerging topics in computing,*volume 4, no. 1, March 2016.