ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

AUTHENTICATION USING STEGANOGRAPHIC AND WATERMARKING TECHNIQUES VIA BIOMETRICS

V.DEEPA[1], R.GAYATHRI[2]
[1]PG Student, [2]Associate Professor of ECE, Mailam Engneering college

Abstract-**The authentication scheme is an important mechanism, through which two communication parties could authenticate each other. To satisfy the requirement of practical applications, many authentication schemes using passwords and smart cards have been proposed. However, passwords might be divulged or forgotten, and smart cards might be shared, lost, or stolen. In contrast, biometric methods, such as fingerprints have no such drawbacks. The key idea behind the proposed approach is to remote authentication which involves the submission of encrypted biometric signal, along with visual and audio cues. The scheme involves secure force (SF) algorithm for encryption and the encrypted signal is further inserted to the most significant wavelet coefficients of the video object (VO), using its Qualified Significant Wavelet Trees (QSWTs) and stego-image is obtained. Digital watermarking is used for providing the double security of obtained image. Implementation is done using MATLAB with sample images for proving the proposed model's distinction. The simulation results show that, the proposed system provides high level of security.**

Index terms-**Remote Authentication, Biometrics, Stego-image, QSWTs, Video Object, Watermarking, and Secure Force algorithm**

I. 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 it's 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 difference between the two is explained by the following example: Let us assume password-based authentication. In positive authentication, the passwords of all users that are authorized to access a system are stored, usually in a file. Thus the passwords space includes only user's passwords and it is usually limited (according to the number of users). If crackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords.

On the contrary, in negative authentication the anti-password space 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. This way, negative authentication can be introduced as a new layer of protection to enhance existing security measures within networks. This allows the current infrastructure to remain intact without accessing the stored passwords or creating additional vulnerabilities. By applying a real-valued negative selection algorithm, a different layer is added for authentication, preventing unauthorized users from gaining network access. Interested readers can also check [2].

According to [3], in 2012 identity fraud in US affected 12.6 million consumers, and resulted in a loss of $4.6 billion ($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 the most important issues of contemporary societies and several works have been proposed in the literature to effectively tackle it. The majority is based on passwords or smart cards. In Section II-A, the pros and cons of these systems are explained and the use of biometrics is suggested as an alternative. Biometrics has already been incorporated in remote authentication (see [4], [5], [6]) but only as password substitution in smart cards.

In order to investigate their full potentiality, biometrics can be incorporated in hybrid crypto-steganographic schemes. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood, while steganographic methods can hide the encrypted biometric signals so that they cannot be seen. In this paper we build further on this principle to confront the problem of remote human authentication over wireless channels, under loss tolerant protocols. In particular an effective wavelet-based steganographic method is proposed for hiding encrypted biometric signals intosemantically meaningful VOs such as the head-and-shoulders VO, which is common in several teleconferencing applications.

Watermarking is the technique of embedding secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

extract Watermarks . Generally, robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth.

Watermarking techniques can be categorized into different types based on a number of ways. Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret key(s) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of invisible watermarking; nevertheless, it can be extracted by a computer program.

The rest of this paper is organized as follows: Section II focuses on the related work and contributions. In Section III the proposed system is presented. Experimental result is provided in Section IV while Section V concludes the paper.

II. RELATED WORK AND CONTRIBUTIONS

A. Remote Authentication

In 1981, Lamport [7] proposed a remote password authentication scheme, by employing a one-way hash function. However, in his scheme a verification table should be maintained on the remote server and if intruders break into it, they can modify the table. Therefore, many different solutions have been proposed, the most popular of which is based on long and random cryptographic keys. For instance, Liao et al. proposed a scheme that utilizes the Diffie-Hellman key agreement protocol over insecure networks, which allows the user and the system to agree on a session key to encrypt/decrypt their communicated messages using a symmetric cryptosystem. Random cryptographic keys are difficult to memorize, thus they are stored somewhere and they are released based on some alternative authentication mechanism (e.g. password). However several passwords are simple and they can be easily guessed or broken [9]. Furthermore, most people use the same password across different applications; if a malicious user determines a single password, they can access multiple applications.

Another interesting and very promising category of remote user authentication schemes involves smart cards using dynamic users' identities per transaction section [11], [12], [13]. These methods aimed to overcome a common drawback of older remote authentication schemes using smart cards: user's identity was static in all the transaction sessions, which may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel. However, vulnerabilities of those methods were also found. Madhusudhan and Mittal [14] proposed a set of security requirements and goals for dynamic ID-based remote user password authentication schemes, and through their respective cryptanalysis, proved that both Wang's et al. [11] and Khan's et al. schemes [12] are insecure against the insider attacks while password authentication is delayed and inefficient. Weaknesses of Yoon's et al. [13] method were also reported . Some of the latest schemes, such as [16], [17] seem very interesting. Still their virtues should be thoroughly investigated by applying cryptanalysis, differential power analysis, physical disassembly (photomicrographs of encryption hardware) etc. Additionally: (a) users should always have their smart cards with them in order to do transactions, (b) if a user loses his/her smart card, he/she will not be able to do any transactions and should wait for the reissuing of the card (sometimes several days), (c) smart cards cost money and effort each time they are (re)issued, (d) due to low power they cannot perform very complex computations, (e) according to cardwerk.com their memory should retain data for up to 10 years without electrical power and (f) they should support at least 10,000 read-write actions during the life of the card.

Many of the aforementioned password-based authentication problems can be confronted using biometrics [18]. Biometrics are inherently more reliable, since biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute and they do not require the person being authenticated to be present at the time and point of authentication [19], [20]. Recently, the biometrics have been extensively applied in remote authentication and several methods were reported [4], [5], [6], [12]. In the majority of these schemes ([4], [5], [6]) biometrics are used simply as an authentication tool in smart card technology. Thus, the drawbacks mentioned in the previous paragraph still hold. Furthermore, as reported in [21] they cannot provide anonymity and three-factor security while they are vulnerable to the privileged insider and the user impersonation attacks.

B. Steganographic Methods

Steganographic algorithms can be roughly divided into those performed in the spatial domain and those applied in a transform domain. Given that the latter are more robust against low-pass filtering and compression attacks [22] , they became the preferred approach. Among transform-based data hiding approaches, DCT [23] and DWT [24] 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 [25] the message is hidden in the sign/bit values of insignificant children of the detail subbands, in non-smooth regions of the image. Using this technique steganographic messages can be send in lossy environments,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

with some robustness against detection or attack. However, low losses are considered and the problem of compression remains. In [26], the message is comprised of two components:a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression. The approach is implemented as a DCT-DWT dual domain, but the authenticator watermark is not encrypted. A similar approach combining DWT and Integer Wavelet Transform (IWT) was recently proposed by Hemalatha et al. [27], where both the secret image and the key are encrypted in a cover image. However, the embedding algorithm is quite complex and sensitive to lossy transmissions.

C. Digital Watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself.

III. THE PROPOSED MODEL

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 a secure force algorithm for encryption to increase security, and (d) the encrypted biometric signal is hidden in a VO.

The overall architecture and data flow of the proposed scheme is illustrated in fig 1. Initially the biometric signal is encrypted by incorporating a secure force algorithm (see also Fig. 2).

Afterwards, a head-and-body image of the biometric signal's owner is analyzed and the host VO is automatically extracted by converting into frames. Next a DWT-based algorithm is proposed for hiding the encrypted biometric signal to the host VO. The proposed algorithm hides the encryptedinformation into the largest-value QSWTs of energy-efficient pairs of subbands. Compared to other related schemes, the incorporated approach has the following advantages :

- it is one of the most efficient algorithms of literature that facilitates robust hiding of visually recognizable patterns, it is hierarchical and has multiresolution characteristics,
- the embedded information is hard to detect by the human visual system (HVS), and
- it is among the best known techniques with regards to survival of hidden information after image compression.

Initially the extracted host object is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of subbands (HL_2, HL_1), (LH_2, LH_1) and (HH_2, HH_1). Afterwards, the pair of subbands with the highest energy content is detected and a QSWTs approach is in-corporated in order to select the coefficients where the encrypted biometric signal should be casted. Finally, the signal is redundantly embedded to both subbands of the selected pair, using a non-linear energy adaptable insertion proce-dure. Differences between the original and the stego-object are imperceptible to the human visual system (HVS), while biometric signals can be retrieved even under compression and transmission losses.

PHASES OF PROPOSED SCHEME

We are proposing a new scheme for secure data communication using steganography, watermarking technique to embed the secret information into any cover image.

The proposed scheme involves (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 using secure force encryption (c) Embedding of the encrypted signal to the host video object using steganography (d) watermarking (e)Compression of the final content and simulated noisy transmission, (g)Decompression and extraction of the encrypted signal, (h) Decryption and removal of watermarking (i) Authentication.Proposed scheme consists of four phases which are described in the following subsections. The performance is evaluated by using histogram of image before and after embedding.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

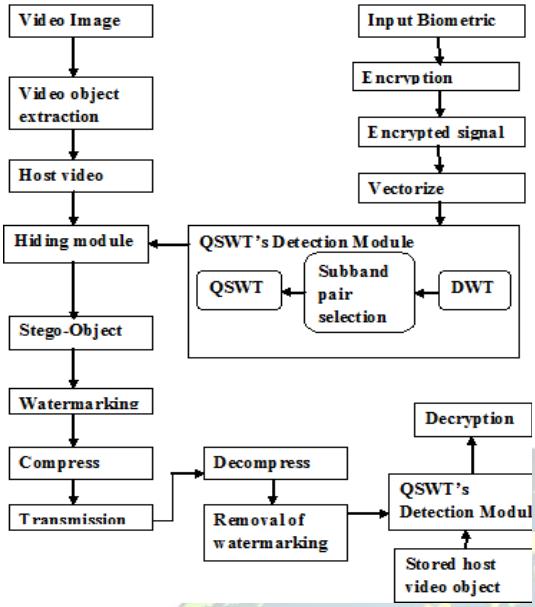


Fig. 1: Data flow in the proposed scheme

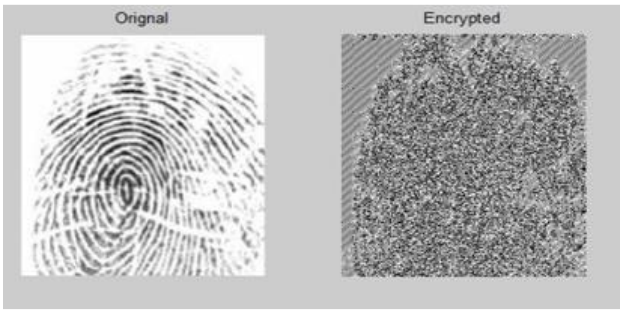
Phase 1- Video to Frames Conversion

In this very first phase, the video is converted into multiple frames and the host video object is obtained.

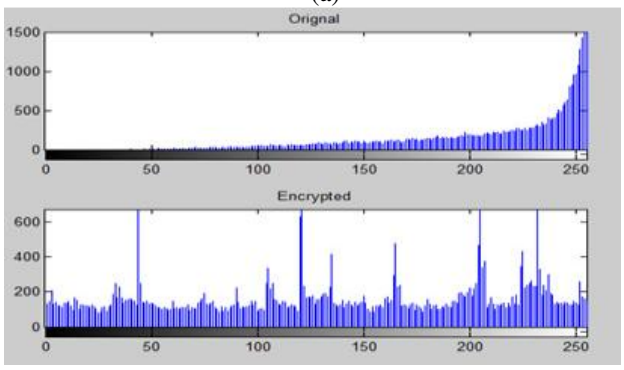
Phase 2-The Encryption Mechanism

. Initially the biometric signal is encrypted by incorporating a secure force algorithmshown in fig 2.The Secure Force algorithm is based on a Fiestel architecture where the process of encryption and decryption are nearly the same, which minimizes the code size to a great extent.

The key expansion process, which involves complex mathematical operations (multiplication, permutation, transposition and rotation) to generate keys for the encryption process, is implemented at the decoder. This shifted the computational burden to the decoder and indirectly, this will help to increase the lifespan of the sensor nodes. However, the generated keys must be transmitted securely to the encoder for the encryption process. In this case, the LEAP (Localized Encryption and Authentication Protocol) is adopted. It is an energy efficient, robust and secure key management protocol that is designed for the WSN.



(a)



(b)

Fig 2 (a) Original and encrypted biometric signal
(b) Histogram of original and encrypted signal

SF ALGORITHM PROCESS

The process of SF algorithm consists of 4 major blocks. The overall key transmission is depicted in Fig 3

Key Expansion Block

Key expansion is the prime process that is used to generate different keys for encryption and decryption. Different operations are performed in order to create confusion and diffusion. Christo Ananth et al. [15] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder.

Key Management Protocol

The key can be securely sent to the encoder with the aid of LEAP .It is a simple and energy efficient protocol designed for large scale WSN, which allows secure key establishment through the use of four types of keys. They are known as the individual key, group key, cluster key, and pair wise shared key.

Encryption Block

The encryption process is initiated once the keys generated by the key expansion block are securely received by the encoder through the secure communication channel created by the LEAP protocol. In the encryption process, simple operations, which include AND, OR, XOR, XNOR, left shift (LS), substitution (S boxes) and swapping operations, are performed to create confusion and diffusion.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

Decryption Block

The decryption process is just the reserve of the encryption process described above.

Phase 3- Hiding the Encrypted Biometric Signal using steganography and watermarking

The encrypted biometric signal is robustly hidden in the host video object. Towards this direction we aim at producing a stego-video object that could protect its hidden message even in cases of compression or lossy transmission. QSWTs can play such a role, since they provide one of the most robust solutions to data recovery, after several signal processing manipulations. In particular let us assume that the host video object has been extracted using the method described in . Next the host video object is decomposed into two levels using the shape-adaptive discrete wavelet transform (SA-DWT) [51]. 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, whiles the HL_1 (LH_1), includes high (low) frequencies in horizontal direction and low (high) frequencies in vertical direction.Subband 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. SubbandsLH_N ,..., LH_3, LH_2, LH_1 follow a parent-child relationship. Christo Ananth et al. [10] proposed a system in which the complex parallelism technique is used to involve the processing of Substitution Byte, Shift Row, Mix Column and Add Round Key. Using S- Box complex parallelism, the original text is converted into cipher text. From that, we have achieved a 96% energy efficiency in Complex Parallelism Encryption technique and recovering the delay 232 ns. The complex parallelism that merge with parallel mix column and the one task one processor techniques are used. In future, Complex Parallelism single loop technique is used for recovering the original message.

In the proposed video object steganographic scheme, co-efficients with local information in the subbands are chosen as target coefficients for casting the encrypted biometric sig-nal. Coefficients' selection is based on Qualified Significant Wavelet Trees (QSWTs) derived from the Embedded Zerotree Wavelet algorithm (EZW).

In the proposed scheme, we select the pair of subbands that contains the highest energy content. Finally, the QSWTs are estimated for the highest energy pair of subbands.

A. The Hiding Strategy

After selecting the pair of subbands containing the highest energy content, QSWTs are found for this pair and the encrypted biometric signal is embedded by modifying the values of the detected QSWTs. Finally the 2-D IDWT is applied to the modified and an un-changed subband to form the final stego-object.The obtained stego-object is additionally watermarked with some data to provide double security as shown in fig 4.

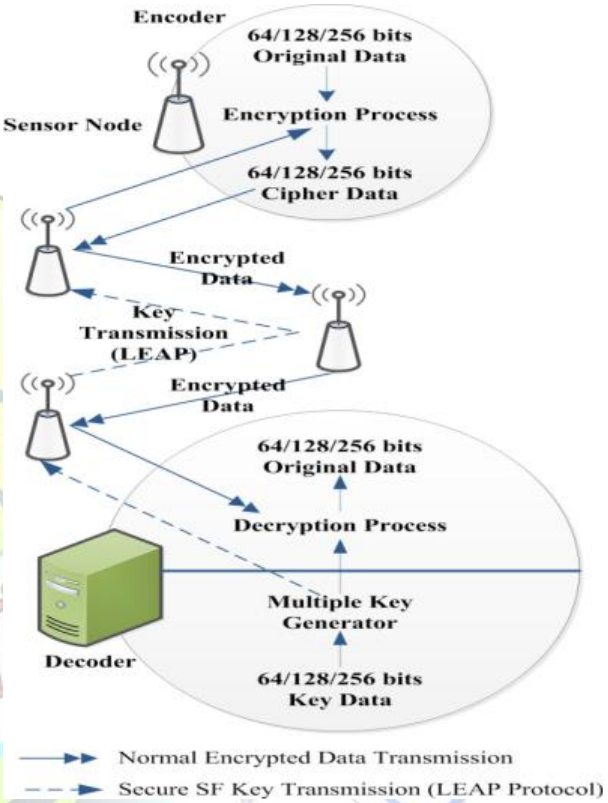
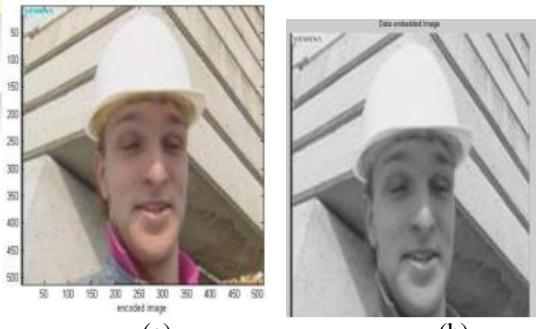
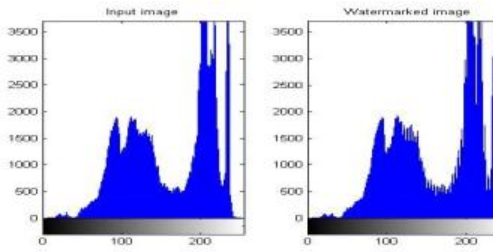


Fig 3 Key transmission of secure force algorithm



(a) (b)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016



(c)

Fig 4 Hided image using (a) Steganography (b) watermarking (c)Histogram of stego-image and watermarked image

Phase 4 –Message recovery

Considering that the stego-object and data embedded image (or a distorted version of it) has reached its destination, the encrypted biometric signal is initially extracted by following a reverse (to the embedding method) process. Towards this direction let us assume that the recipient of the stego-object has also received the size of the encrypted 2-D biometric signal (axb), the scaling constants (c_1, c_2) and possesses the original host video object (or he/she has the algorithm to segment it from the initial head-and-body image). Then the following steps are performed in the recipient's side:

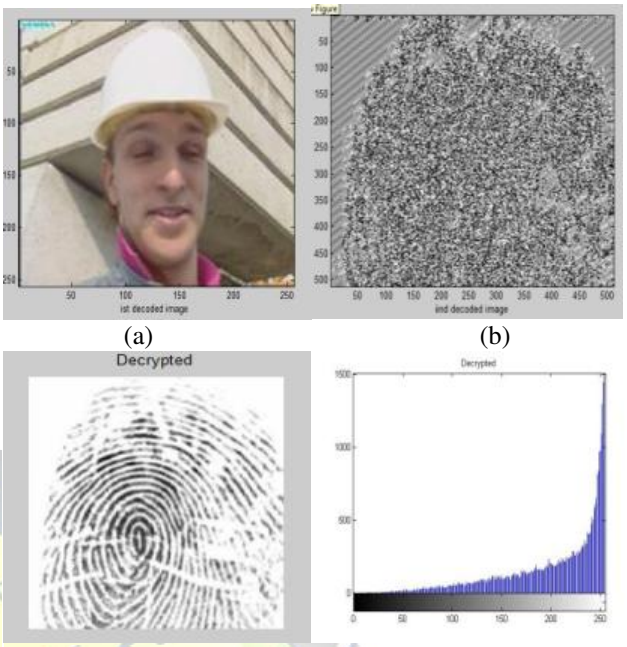
Step 1: Initially the received stego-object X' and originalvideo object X are decomposed into two levels with seven subbands using the DWT,

$$Y = DWT(X) \quad Y' = DWT(X') \qquad (1)$$

Step 2: Using the size axb, the embedded positions are detected by the hiding process.

Step 3: The resulting hidden message coefficients are averaged and rearranged to provide the encrypted biometric signal.

Step 4: The original biometric signal is recovered by decrypting the enciphered signal (see subsection IV-F). Here it should be mentioned that if the same video object X is used for every authentication attempt, the scheme may become vulnerable to attacks. In order to confront this problem the sender and receiver may share multiple video objects (poses) for each user. In each authentication session, the sender may select one pose and inform the receiver of the selected pose's ID. This is a more resistant to attacks methodology, which can become even more efficient if new poses of the users are periodically collected.



(a) (b)

(C) (D)

Fig.5 Decrypted signal (a) Host video object (b) encrypted signal (C) original biometric signal (D) Histogram of decrypted signal

IV. Experimental Results

For simulation we have used MATLAB 8.1 For evaluation purposes, the proposed video objects-oriented biometric signals hiding scheme is examined in terms of security, effectiveness, robustness and bandwidth usage ef-ficiency. The authentication setting, which focused on fingerprints, was simulation-based and included different scenarios that are described in the following paragraphs. 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.

(A) Security merits of SF algorithm

The design of SF algorithm provides low-complexity architecture for implementation in WSN. To improve the energy efficiency, the encryption process consists of only five encryption rounds. It has been suggested in that a lower number of encryption rounds will result in less power consumption. In order to improve the security, each encryption round encompasses six simple mathematical operations operating on only 4 bit data (designed to be compatible with 8-bit computing devices for WSNs). This is to create an adequate amount of confusion and diffusion of data to encounter different types of attacks. The key expansion

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

process, which involves complex mathematical operations (multiplication, permutation, transposition and rotation) to generate keys for the encryption process.

B. Bandwidth Usage Efficiency

As stated in the Introduction, most existing schemes do not consider semantically meaningful video objects as hosts, but whole images. On the other hand the proposed scheme con-siders semantically meaningful video objects, offering possible advantages such as: (a) A secondary complementary authen-tication mechanism by recording with a camera the person under authentication, (b) efficient bandwidth usage, since most of the used bandwidth transmits information relevant to the authentication process, and (c) efficient rate control, since in case of traffic congestion/reduction of QoS, the rate control mechanism could discard blocks from the body region that do
not also contain hidden information, instead of discarding face blocks. This is the content-awareness merit of the proposed bandwidth-friendly scheme.

C. Robustness of the Steganographic Module

Next the robustness of the proposed biometrics hiding method has been extensively evaluated under various simu-lation tests, performed using MATLAB. In particular, during experimentation the host video objects were used, in which, the encrypted biometric signals were hidden respectively. Then according to the size of the encrypted biometric signals, the top 186x158 QSWTs were selected for both host video objects to embed the signals.

The proposed scheme achieves effective embedment of the encrypted information into the host images. The proposed scheme also has high level of security.

V. 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 (e.g. citizen authentication). Thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Steganography and Watermarking is the current area of research where lot of scope exists. Towards this direction in this paper the domain of biometrics authentication
over error-prone networks has been examined. Since steganography and watermarking by itself does not ensure secrecy, it was combined with a secure force system. 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.

REFERENCES

[1] KlimisNtalianis, and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks ," in Proceedings of the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING , JANUARY 2015.
[2] A. Madero, Password secured systems and negative authentication. Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, Engineering Systems Division, 2013.
[3] 2013, "Identity fraud report: Data breaches becoming a treasure trove for fraudsters," Javelin Strategy and Research, Tech. Rep., 2013.
[4] E.-J. Yoon and K.-Y.Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," The Journal of Supercomputing, vol. 63, no. 1, pp. 235– 255, Jan. 2013.
[5] 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, ser. Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, 2012, pp. 391–406.
[6] 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 Systems with Applications, vol. 41, no. 4, pp. 1411–1418, Mar. 2014.
[7] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.
[8] I.-E. Liao, C.-C.Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," Journal of Computer and System Sciences, vol. 72, pp. 727–740, 2006.
[9] M. Jakobsson and M. Dhiman, "The benefits of understanding passwords," in Mobile Authentication, ser. SpringerBriefs in Computer Science. Springer New York, 2013, pp. 5–24.
[10] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795
[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," Computer Communications, 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'," Computer Communications, vol. 34, no. 3, pp. 305–309, Mar. 2011.
[13] E.-J. Yoon, S.-H.Kim, and K.-Y. Yoo, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme'," International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.
[14] R. Madhusudhan and R. C. Mittal, "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, Jul. 2012.
[15] Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07
[16] A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," Networking Science, vol. 2, no. 1-2, pp. 12–27, May 2013.
[17] T.-Y. Chen, C.-C.Lee, M.-S.Hwang, and J.-K. Jan, "Towards secure and efficient user authentication scheme using smart card for multiserver environments," The Journal of Supercomputing, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.
[18] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1–5, Jan. 2010.

[19] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits Systems for Video Technology, vol. 14(1), pp. 4–20, 2004.
[20] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 3, pp. 145–151, Sep. 2011.
[21] D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," IEEE Systems Journal, pp. 1–8, 2014.
[22] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hiding in compressed images," IEEE Transactions on Image Processing, vol.10(8), pp. 1252–1263, 2001.
[23] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy, vol. 1(3), pp. 32–44, 2003.
[24] P.-Y. Chen and H.-J. Lin, "A dwt based approach for image steganography," International Journal of Applied Science and Engineering, vol.4(3), pp. 275–290, 2006.
[25] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, "Steganography for a low bit-rate wavelet based image coder," in Proceedings of the IEEE International Conference on Image Processing, vol. 1. IEEE, 2000, pp. 597–600.
[26] D. Kundur, Y. Zhao, and P. Campisi, "A steganographic framework for dual authentication and compression of high resolution imagery," in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 2. IEEE, 2004, pp. 1–4.
[27] S. Hemalatha, U. Dinesh Acharya, A. Renuka, and P. R. Kamath, "A secure color image steganography in transform domain," International Journal on Cryptography and Information Security, vol. 3(1), 2013.