ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

VIDEO-OBJECT STEGANOGRAPHY MECHANISM TO OVERCOME COMPRESSION LOSS IN BIOMETRIC BASED AUTHENTICATION.

E. P. PRAKASH[1], C. DEEPTHI NIVETHA[2].

1. Assistant Professor, SNS College of Engineering, Coimbatore, India.
2. MEScholar, SNS College of Engineering, Coimbatore, India.

Manuscript Info

Manuscript History:

Received: 14 February 2016
Final Accepted: 26 March 2016
Published Online: April 2016

Key words:
video-object, QSWT (Qualified Significant Wavelet Tree), IDWT (Inverse Discrete Wavelet Transform), Integrate Region Matching.

Corresponding Author

E. P. PRAKASH.

Abstract

When sensitive information is exchanged through wireless communication, it requires remote authentication. The Authentication is obtained by the biometric signal, which is difficult to forge copy and share. The method of steganography is employed in providing the authentication. The biometric signals is encrypted with a video-object and sent. The remote authentication is based on the semantic segmentation, chaotic encryption and data hiding. To authenticate user X remotely, X video-object is extracted then the biometric signal is encrypted by chaotic encryption. The encrypted biometric signal is inserted to the most significant wavelet coefficient of video-object by using QSWT (Qualified Significant Wavelet Tree). QSWT provide invisibility and resistant against lossy transition and compression. Now video-object along with biometric signal is extracted as stego-object which is compressed and sent to receiver. While decryption, IDWT (Inverse Discrete Wavelet Transform) is used to retrieve the biometric signal from video-object. One of the challenging problem in decrypting is the biometric signal is not clear for authentication. This loss occurs due to compression of stego-object. To overcome the above issue, Image Coder is used to detect the compression loss and Integrate Region Matching is used to reduce the compression loss. This method provides security in encryption and robustness against steganalytic attacks to various transmission losses and JPEG compression issues. This proposed method of biometric based authentication uses bandwidth in an efficient manner.

Introduction:-

In digital world nowadays, the security of digital images/videos becomes more and more important since authentication is made with those digital images/videos. 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. In this paper authentication is provided through biometric signal (i.e.) finger print. When using this biometric signal it's difficult to copy, forge and share [6]. Hence the security of the biometric signal increases. Steganography mechanism is used to hide the information. Steganography is the branch of information hiding. It embeds the secret image in the cover image to hide the existence image [7].

In early days, remote authentication [3] is provided through password authentication methods and smart cards. While using these methods the chance of attackers to hack the password is very high. After this the remote authentication is provided through biometric signal which is more reliable and it provides three factor securities against attacks. Biometrics-based remote authentication uses fault tolerant protocols. The semantic extraction of meaningful video-object from the host video-object for hiding the biometric signal is automatically extracted. Chaotic encryption is used to hide the biometric signal. This chaotic encryption works like a one-time pad. Discrete Wavelet Transform (DWT) is used to select the sub bands to hide the biometric signal in the video-object.

Existing system:-

The existing system tries to overcome a common drawback of older remote authentication schemes [3]. By using smart cards user's identity was static in all the transaction sessions. The smart card is a printed circuit board it contains the users authentication information. This printed information could be invisible to a person. While showing this smart card to the authentication system the information could be read and verified by the sensor in the authentication system.

When using smart cards the information can be hacked or attacked but when using biometrics for authentication purpose it is very difficult to hack. When biometrics alone used it does not provide security hence it is combined with chaotic encryption. The biometric signal is combined along with the host video-object and it is transmitted as stego-object. The stego-object is compressed while transmitted.The compression loss is one of the challenging issues. The obtained biometric signal by decrypting the stego-object is not so clear and the authentication fails. Many methods are followed to reduce the compression loss. In existing systems many new steganographic methods are used to overcome the compression losses. Steganographic algorithms [1] are performed in spatial domain and transform domain in order to overcome the compression loss. Among which transform based data hiding approach uses DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) to hide the digital image and video compression images. The compression loss is minimized by hiding in non-smooth regions of the image.

Dual DCT-DWT methods divide the image into two components soft-authenticator watermark for authentication purpose and chrominance watermark to improve the efficiency of compression.DWT (Discrete Wavelet Transform) and IWT (Integer Wavelet Transform) uses both the secret image and key are encrypted in cover image but this method is sensitive to lossy compression. The loss due to compression cannot be minimized.

When steganography is performed with biometric signal, amplitude modulation based steganography is used along with embedded algorithms. In case of hiding the fingerprints DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) is used but it is not resistant to compression.DCT (Discrete Cosine Transform) and SVD (Singular Value Decomposition) method is proposed for multimodal biometrics framework [1]. This method is used for ownership protection in biometrics. Even though many techniques were used to combine biometrics with video-object image the problem due to compression exists.

Drawbacks of existing system:-

Smart cards may leak some information about that user and and also create risk of ID-theft during the message transmission over an insecure channel [1]. User need to always have their smart cards with them in order to do transactions. 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).Smart cards cost money and effort each time they are (re)issued. Due to low power they cannot perform very complex computations.

When using biometrics based authentication the recipient should posses the original host video object. In case of C-PRBG (Chaotic Pseudo-Random Bit Generator) [12], several combinations are used as control parameter and it is possible that some parameters of control parameters may mislead in to non-chaotic way. This result of cryptosystem may provide confusion and diffusion properties.

Many new algorithms are experimented to overcome the loss due to compression in host video-object and biometric signal. When problem of lost biometric signal is of high interest it is very difficult to perform the authentication module and when authentication fails the legal entities cannot could not access the centralized authentication service and the biometric signal.

The steganographic scheme is based on QSWTs, if image has several homogeneous areas its capacity or the robustness can be reduced.

These are several methods which are used to against the compression losses in the existing system.

3.proposed system

This scheme essentially more reliable, since biometric characters cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute [12]. They require the person being authenticated to be present at the time and point of authentication. Recently, the biometrics has been broadly applied in remote authentication. In this case of biometrics all the existing system use the whole image whereas in video-object detection the meaningful VO

is extracted. The person is captured by camera for authentication and then the face and skin areas are extracted as the video-object.

Next the fingerprint of the user is used to authenticate the person [6]. In this method the bandwidth is used efficiently and equal importance is given for both the biometrics and video-object image. On the other hand, it is content-aware scheme and in case of traffic congestion , the rate control mechanism discards unwanted blocks from the body region that do not contain hidden information, instead of discarding the face areas. Object oriented data hiding is used which is more secure and robust against attacks and sensitive towards lossy compression. From the image the video-object is detected and the data is hided into the skin areas of cover image. The detection of hidden data in skin areas are hard to detect by human visual system (HVS).
The proposed method is designed to overcome the compression loss at the authentication module. The robust remote authentication mechanism based on five factors [6] [7]. At sender side three factors could be used they are semantic segmentation, chaotic encryption data hiding, compression. At receiver side two factors are used they are decompression and Data Extraction. In this case, biometric entities are encrypted by a chaotic cipher scheme generate the binary image it contains only a black and white pixels. Since the generated key has size equal to the size of the data to be encrypted chaotic systems are good for encryption tasks, because they present an infinite number of unstable bits in form of black and white pixel for a finite number of stable values.

QSWT (Qualified Significant Wavelet Tree) and DWT (Discrete Wavelet Transform):-

The band selection and the transmission of stego-object is done through the QSWTs, this method is used because even though the attackers try to hack the host video-object it's difficult to decrypt the biometric signal [16]. This is a content-aware bandwidth friendly scheme. The hiding module hide the encrypted the information into the largest-value QSWTs of energy-efficient pairs of sub bands [8].

ADVANTEGES OF QSWT (Qualified significant Wavelet Trees):-

- 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).
- 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 sub bands (HL2, HL1), (LH2, LH1) and (HH2,HH1). Afterwards, the pair of sub bands with the highest energy content is detected and a QSWTs approach is incorporated, in order to select the coefficients where the encrypted biometric signal should be casted [8] [14]. Finally, the signal is redundantly embedded to both sub bands of the selected pair, using a non-linear energy adaptable insertion procedure. 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.

Chaotic encryption

Chaotic encryption [12] works like one-time pad to encrypt the biometric signal. Symmetric encryption is faster and is used for producing keys. The keys are exchanged between communicating entities through public key cryptography. The generated key has size equal to the size of the data to be encrypted. The chaotic encryption produces infinite number of unstable orbital's and infinite number of different values. The evolution of chaotic cipher depends on the initial conditions and the encrypted values of the biometric identifiers. When steganographic algorithm is performed in pixel domain with low bit rate images there is a need for more embedding space, reliability and controllability in encoding and decoding of hidden messages.

In CVES (Chaotic Video Encryption Scheme), there are three essential features to ensure the high security [12].

- The stream sub-cipher is made of 2n asymptotically independent chaotic maps, and the sequence of chaotic iterations is controlled pseudo-randomly by another independent chaotic map. This makes statistical cryptanalysis much more difficult for attackers.
- For different cluster, the entirely different S-Box is pseudo-randomly key is determined by the current 2n states, which makes CVES similar to a one-time-a-pad cryptosystem.

- The product of the stream sub-cipher and the block sub-cipher makes the known-plaintext and chosen-plaintext attack impossible. Extremely, even when the 2n states of are well known, it is impossible to hack.

In order to take these advantages of chaotic encryption, chaos-based cipher mechanism and C-PRBG (Chaotic Pseudo-Random Bit Generator) is used for real-time digital video based on multiple digital chaotic maps, which can overcome the problem between the encryption speed and high security existing in video encryption systems. The security of the encrypted content mainly depends upon size of the key [1]. The generated key size is equal to the size of biometric signal. Each key id generated by C-PRBG (Chaotic Pseudo-Random Bit Generator). The produced pseudorandom sequence is based on triplet of chaotic systems which provides high security. After generating the initial pseudo-random key, the cipher module is activated. Before encryption, the samples of biometric of signal are properly ordered [12]. To avoid security problems while maintain high standards, the chaotic encryption scheme combines three chaotic cipher to implement a complex product cipher. The secret key provides the initial conditions and control parameters for chaotic system.

Region matching:-
There is a loss in embedded data and the compression loss is high when the image is transformed to transform domain. The method of low bit rate image coder is used to hide the steganographic message into the base layer of object image. This coder determines the wavelet coefficients in the sub bands of these three regions for messaging by using steganographic mask for transmission of image. The ability to send steganographic message in lossy environment is high and compression loss is minimized. Integrated region matching is used to correct the images obtained from decryption. This method compares the biometric image with the image in the centralized database and the corrections are made in the biometric image to authenticate. The decryption module receives stego-object, the initial control parameters and initial conditions for the triplet of chaotic maps (C-PRBG module) and the initial cipher value C0 (used at the first feedback). Then the IDWT (Inverse discrete wavelet transforms) is performed. Afterwards the digital chaotic systems produce the same onetime pad used during encryption, but now it is used for decryption purposes.

Now the host video object is obtained and image handler is used to detect the loss in video-object and biometric signal. This image handler is used to detect the loss in images due to compression standards such as JPEG-2000 and H.264 [5]. Integrated region matching is used to correct the images obtained from decryption. This method compares the biometric image with the image in the centralized database and the corrections are made in the biometric image to authenticate.Integrated region matching method is used to compare the images with the previously available images in the database. The comparison is based upon the set of regions and is characterized by the reflecting color, texture, shape and location.
Initially the obtained fingerprint image is segmented along with the lost region of images
Segmented image is then compared with the other images in the database. The images with greater similarities are retrived.dynamic programming is used to minimize the error caused due to geometric consistency and appearance similarities.

Union of corresponding images is performed to find out the set of matches between the 2 images.
Final match score between the two images is evaluated to find the mutual geometric consistency of final match points.
The image with maximum match score points is retrieved.

The goal of Integrated Region Matching is to reduce the loss due to compression. The obtained biometric signal by using Integrated Region Matching is less than 40%.Whereas; in all existing methods which tries to overcome the data loss in biometric signal. The authentication fails in all those stages because the data loss is greater than 60%.

Conclusion:-

In our daily lives biometrics signal plays a vital role. The development and integration of biometric authentication techniques used into practical applications increases nowadays. If the steganography scheme is alone applied it does not ensure secrecy when it was combined with a chaotic encryption system it provides additional security. In the proposed procedure when the images send through networks that are imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Remote authentication depends up on fingerprint which is obtained. This paper presents an enhanced method to overcome the compression loss in the receiver side.

References:-

1. Klimis Ntalianis and Nicolas Tsapatsoulis (2015), "Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks" in IEEE Transactions on Emerging topics on computing.
2. Areepongsa .S, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao,(2000) "Steganography for a low bit-rate wavelet based image coder," in Proceedings of the IEEE International Conference on Image Processing, vol. 1. IEEE, 2 pp. 597–600.
3. Chen, C-H. Ling, and M.-S. Hwang,(2014) "Weaknesses of the yoonkim-yoo remote user authentication scheme using smart cards," in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications. IEEE, pp. 771–774.
4. Doulamis .N.D, A. D. Doulamis, K. S. Ntalianis, and S. D. Kollias,(2003) "An efficient fully-unsupervised video object segmentation scheme using an adaptive neural network classifier architecture," IEEE Transactions on Neural Networks, vol. 14(3), pp. 616–630.
5. Fard .M, M. R. Akbarzadeh-T, and F. Varasteh-A,(2006) "A new genetic algorithm approach for secure jpeg steganography," in Proc. of IEEE Int'l Conference on Engineering of Intelligent Systems.
6. He.D and D.Wang,(2014) "Robust biometrics-based authentication scheme for multi-server environment," IEEE Systems Journal, pp. 1–8.
7. Hoang .T, D. Tran, and D. Sharma, (2008) "Remote multimodal biometric authentication using bit priority-based fragile watermarking," in Proceedings of the 19th International Conference on Pattern Recognition. IEEE Computer Society, pp. 1–4.
8. Hsieh .M.S, Tseng, and Y.-H. Huang, (2001)"Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, vol. 48(5), pp. 875–882.
9. Jain .K and U. Uludag,(2003) "Hiding biometric data," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25(11), pp. 1494– 1498.
10. Jain .K, A. Ross, and S. Prabhakar, (2004) "An introduction to biometric recognition," IEEE Transactions on Circuits Systems for Video Technology, vol. 14(1), pp. 4–20.
11. Klimis Ntalianis and Nicolas Tsapatsoulis (2015), "Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks" in IEEE Transactions on Emerging topics on computing.
12. Li .S, X. Zheng, X. Mou, and Y. Cai, (2002,) "Chaotic encryption scheme for real-time digital video," in Proceedings of Real-Time Imaging VI, vol. 4666. SPIE, pp. 149–160.
13. Murdoch .S, M. Bond, and R. J. Anderson,(Nov 2012) "How certification systems fail: Lessons from the ware report," IEEE Security and Privacy, vol. 10, no. 6, pp. 40–44.
14. Ntalianis .K .S, N. D. Doulamis, A. D. Doulamis, and S. D. Kollias, (2002)"Automatic stereoscopic video object-based watermarking using qualified significant wavelet trees," in Proceedings of the IEEE International Conference on Consumer Electronics. IEEE, pp. 188–189.
15. Ramkumar .M and A. N. Akansu,(2001) "Capacity estimates for data hiding in compressed images," IEEE Transactions on Image Processing, vol. 10(8), pp. 1252–1263.
16. Shapiro J. M.,(1993) "Embedded image coding using zero trees of wavelet coefficients," IEEE Transactions on Signal Processing, vol. 41, no. 12, pp. 3445–3462, Dec.