SECURE REMOTE AUTHENTICATION USING BIOMETRIC DATA WITH STEGANOGRAPHY FOR WIRELESSNETWORK.

S. M. Chougule.
PG Student, Dept. of Electronics Engineering.
Smchougule9591@gmail.com

Prof. S. R. Mahadik.
Professor, Dept of Electronics and Telecommunication Engineering
Dr. J. J. Magdum college of Engineering,
Jaysingpur, Shivaji University, Kolhapur, India

ABSTRACT
In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Many authentication schemes using passwords and smart cards have been proposed. However, passwords might be forgotten and smart cards might be shared, lost, or stolen. This paper tries to givesan idea about the previous researches and authentication scheme using hybrid crypto-steganographic schemes. Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, human voice etc.)

KEYWORDS: remote authentication, crypto-steganographic, audio cues.

INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a datum or entity[1].The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. In remote password authentication scheme verification table should be maintained on the remote server.Ifintruders break into it, they can modify the table. Several passwords are simple and they can be easily guessed or broken. Most people use the same password across different applications, if a malicious user determines a single password, they can access multiple applications[2].In remote authentication using smart cards , users should always have their smart cards with them in order to do transactions. If a user loses his smart card, he will not be able to do any transactions ,should wait for the reissuing of the card.It will require extra money and effort each time they are (re)issued.

This system focuses on hybrid crypto-steganographic schemes[3]. 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. Steganography by itself does not ensure secrecy, it was combined with encryption system. However, the security and integrity of the biometric data itself are important issues. Encryption and steganography are possible techniques to secure biometric data. This system proposes an effective wavelet-based steganographic method for hiding encrypted biometric signals into semantically meaningful video objects such as the head and shoulders video object, which is common in several teleconferencing applications. This method is more reliable and secure than other method. Biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share and distribute. 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 video object, using its Qualified Significant Wavelet Trees (QSWTs)[4]. QSWTs provide both invisibility and significant resistance against lossy transmissionand compression, conditions that are typical in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego-object (SO).

AN INTRODUCTION TO BIOMETRIC RECOGNITION

Anil K. Jain, Arun Ross and Salil Prabhakar proposed idea of Biometric Recognition[1]. In this paper, they give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns. A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor.A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identityRobust biometrics-based authentication scheme for multi-server environment

ROBUST BIOMETRICS-BASE AUTHENTICATION SCHEME FOR MULTI-SERVER ENVIRONMENT

Debiao He and Ding Wang given information about authentication scheme for multi-server environment[2]. In this paper,they proposed a robust biometrics-based authentication scheme for multiserver environment using elliptical curve cryptography. The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. Security analysis shows that the proposed scheme could satisfy security requirement of multiserver environment. Performance analysis shows that the proposed scheme could overcome weaknesses in previous schemes at the cost of increasing computational cost and communicational cost slightly. Therefore, the proposed scheme is suitable for use in distributed multi server network environments.

There are four phases in the proposed scheme, which are the server registration phase, user registration phase, authentication phase, and password change phase.InServer Registration Phase ,server sends the registration request to registration center(RC)and obtains his secret key from RC.In User Registration Phase, user sends the registration request to RC and obtains a smart card containing his secret key from RC.InAuthentication Phase,userand server authenticate each other in the help of RC. In addition, a session key for future communication is generated between userand server.In Password Change Phase, user could change the old password PWito anew password PWnew

CAPACITY ESTIMATES FOR DATA HIDING IN COMPRESSED IMAGES

M.Ramkumar and A. N. Akansu proposed a method to obtain an estimate of the number of bits that can be hidden in still images, or the capacity of the data-hiding channel[3]. They show how the addition of the message signal or signature in a suitable transform domain rather than the spatial domain can significantly increase the channel capacity. Most of the state-of-the-art schemes developed for data-hiding have embedded bits in some transform domain. Though most methods uses DCT or wavelet decomposition for data embedding. They compare the achievable data-hiding capacities for different decompositions like DCT, DFT, Hadamard and subband transforms**.**

The forward transform block decomposes the image into its coefficients of bands. A component of the signature/ message signal is added to each band. The inverse transform block reconstructs the modified

image . The image then undergoes some processing (lossy compression) to yield the image . The hidden message signal/signature is to be extracted from . The image is decomposed into bands by the same forward transform block and each component of the signature is extracted separately. In this paper, estimate the capacity of data-hiding channel for different decompositions (different forward and inverse transform

SHAPE-ADAPTIVE DISCRETE WAVELET TRANSFORMS FOR ARBITRARILY SHAPED VISUAL OBJECT CODING

ShipengLiandWeiping Li given broad idea of a shape-adaptive wavelet coding technique for coding arbitrarily shaped still texture[4]. This technique includes shape-adaptive discrete wavelet transforms (SA-DWT's) and extensions of zero tree entropy (ZTE) coding and embedded zero tree wavelet (EZW) coding. Shape-adaptive wavelet coding is needed for efficiently coding arbitrarily shaped visual objects, which is essential for object-oriented multimedia applications. Comparison of shape-adaptive wavelet coding with other coding schemes for arbitrarily shaped visual objects shows that shape-adaptive wavelet coding always achieves better coding efficiency than other schemes.

There are two components in the SA-DWT. One is a way to handle wavelet transforms for arbitrary length image segments. The other is a sub sampling method for arbitrary length image segments at arbitrary locations. The SA-DWT allows odd or small-length image segments to be decomposed into the transform domain in a similar manner to the even- and long-length segments, while maintaining the number of coefficients in the transform domain identical to the number of pixels in the image domain. The scale of the transform domain coefficients within each sub band is the same to avoid sharp changes in sub bands. A proper sub sampling method is important for the SA-DWT too. One consideration is that it should preserve the spatial correlation and self-similarity property of wavelet transforms so that 2-D (horizontal and vertical directions) separable wavelet decompositions and pyramid wavelet decompositions can still be applied to the arbitrarily shaped image region without loss of spatial correlation. Another consideration is the effect of the sub sampling strategy on the efficiency of zero tree coding.

AN EFFICIENT FULLY UNSUPERVISED OBJECT SEGMENTATION SCHEME USING AN ADAPTIVE NEURAL NETWORK CLASSIFIER ARCHITECTURE

N. D. Doulamis, A. D. Doulamis, K. S. Ntalianis and S. D. Kollias proposed an unsupervised video object (VO) segmentation and tracking algorithm[5]. The proposed scheme comprises: 1) a VO tracking module and 2) an initial VO estimation module. Object tracking is handled as a classification problem and implemented through an adaptive network classifier, which provides better results compared to conventional motion-based tracking algorithms. Two different scenarios are investigated. The first concerns extraction of human entities in video conferencing applications, while the second exploits depth information to identify generic VOs in stereoscopic video sequences. Human face/ body detection based on Gaussian distributions is accomplished in the first scenario, while segmentation fusion is obtained using colour and depth information in the second scenario.

A NEW GENETIC ALGORITHM APPROACH FOR SECURE JPEG STEGANOGRAPHY.

M. Fard, M. R. Akbarzadeh-T, and F. Varasteh-A given an broad idea of algorithm usedfor Secure JPEG Steganography[6].Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient. In this paper they propose a novel GA evolutionary process to make a secure steganographicencoding JPEGimages. Their steganography step is based on OutGuess which was proved to be the least vulnerable steganographic system. A combination of OutGuessteganalysis approach and maximum absolute difference (MAD) for the image quality are used as the GA fitness function.

JPEG image format due to its good characteristics (having both reasonable quality and small size) is the most common image format for web and local usages. JPEG uses discrete
cosine transform (DCT) to transform successive 8×8 pixel blocks of the image into 64 DCT coefficients. Here, LSBs of the quantized DCT coefficients are used as redundant bits.The modification of even a single DCT coefficient affects all 64 image pixels. In some image formats such as GIF, the visual structure of the image exists to some degree in all bit layers
of the image. Steganographic systems which modify these formats are mostly vulnerable to visual attacks However this is not true about the JPEG format. As the modifications happen in the frequency domain rather than spatial domain, there is no visual attack against it.

A STENOGRAPHIC FRAMEWORK FOR DUAL AUTHENTICATION AND COMPRESSION OF HIGH RESOLUTION IMAGERY

D. Kundur, Y. Zhao, and P. Campisiproposed anapproach for the combined image authentication and compression of color images by making use of a digital watermarking and data hiding framework[7]. The multipurpose watermark was designed by exploiting the or thogonality of various domains used for authentication, color decomposition and watermark insertion. The approach is implemented as a DCT-DWT dual domain algorithm. Simulations and comparisons of the proposed approach with the state-of-the-art existing work demonstrate the potential of the overall scheme.

The color image is first decomposed into the YIQ color space. The luminance component is passed through a soft authenticator generation algorithm to produce *W*a. The chrominance components *I* and *Q* are subsample using a 2-D discrete wavelet transform (DWT) to form *W*c. Then *W*a and *W*c are embedded in turn to produce the watermarked image which is then compressed using an adaptive wavelet based compression algorithm .

HIDING DIGITAL WATERMARKS USING MULTIRESOLUTION WAVELET TRANSFORM

Ming-Shing Hsieh, Din-Chang Tsengand Yong-Huai Huang given the method of an image accreditation technique[8]. The method for the digital watermarking was based on the wavelet transform which used a random number of a sequence of bits as a watermark and where the watermark can only be detected by comparing an experimental threshold value to determine whether a sequence of random signals is the watermark.

The proposed approach embeds a watermark with visual recognizable patterns, such as binary, gray, or color image in images by modifying the frequency part of the images and an original image decomposed into wavelet coefficients. Multi-energy watermarking scheme based on the qualified significant wavelet tree (QSWT) is used to achieve the robustness of the watermarking. Unlike other watermarking techniques that use a single casting energy, QSWT adopts adaptive casting energy in different resolutions. The performance of the proposed watermarking is robust to a variety of signal distortions, such as JPEG, image cropping, sharpening, median filtering, and incorporating attacks.

Awavelet-based watermarking approach by adding visually recognizable images to the large coefficients at the high and middle frequency bands of the DWT of an image. This approach has the following advantages: 1) the extracted watermark is visually recognizable toclaim one's ownership; 2) the approach is hierarchical and has multiresolution characteristics; 3) the embedded watermark is hard to detect by human visual perceptivity; and 3) the approachmatches the upcoming image/video compression standards. Experimental results show that the watermarking approach is very robust to image compression and complicatedimage distortions.

CONCLUSION

By the literature review importance of Biometric authentication for wireless network is seen.In earlier researches remote password authentication and remote authentication using smart cards have been used. Passwords might be forgotten and smart cards might be shared, lost, or stolen In contrast, biometric methods, such as fingerprints or iris scans, have no such drawbacks. Therefore, biometrics-based authentication schemes gain wide attention. Biometric methods for authentication are used in both the commercial and private sector.

REFERENCES

[1] 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.
[2] D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," IEEE Systems Journal, pp. 1–8, 2014
[3] 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.
[4] S. Li and W. Li, "Shape-adaptive discrete wavelet transforms forarbitrarily shaped visual object coding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 10(5), pp. 725–743, Aug. 2000.
[5] N. D. Doulamis, A. D. Doulamis, K. S. Ntalianis, and S. D. Kollias, "An efficient fully-unsupervised video object segmentation scheme using anadaptive neural network classifier architecture," IEEE Transactions onNeural Networks, vol. 14(3), pp. 616–630, 2003.
[6] A. M. Fard, M. R. Akbarzadeh-T, and F. Varasteh-A, "A new geneticalgorithm approach for secure jpeg steganography," in Proc. of IEEEInt'l Conference on Engineering of Intelligent Systems. IEEE, 2006.
[7] D. Kundur, Y. Zhao, and P. Campisi, "A steganographicframeworkfor dual authentication and compression of high resolution imagery,"in Proceedings of the IEEE International Symposium on Circuits andSystems, vol. 2. IEEE, 2004, pp. 1–4.
[8] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, vol. 48(5), pp. 875–882, 2001.