INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

IMAGE-OBJECT ORIENTED BIOMETRICS FOR USER AUTHENTICATION

Computer Science

L.M.Merlin Livingston Professor, Jeppiaar Institute of Technology

ABSTRACT

In the emerging modern world, there is a need for fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. In wireless communication, in order to share secret information between 2 or more entities, remote authentication could be used. It internally contains three works. The first one is the encryption of finger print image in the form of chaotic image, then internally converts that chaotic image into set of vectors. The second one is the extracting human object from the image. The third one is hiding those vector value into the extracted object. Trojan horse and other attacks could be mostly occurring in cases of remote examinations or in interviewing or in personnel hiring, which may create serious threats. This paper aims at in a robust remote authentication mechanism based on semantic segmentation, chaotic encryption and data hiding. Remote authentication is a method to authenticate remote users over insecure communication channel. Password-based authentication schemes have been widely deployed to verify the legitimacy of remote users. In this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a secure force encryption. 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 stego-analytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security.

KEYWORDS

I.INTRODUCTION

Biometrics authentication refers to establishing identity based on the physical and/or behavioral characteristics of a person such as face, fingerprint, hand geometry, iris, voice, way of walking, and so forth. Biometric systems offer several advantages over traditional password-based schemes. They are inherently more reliable, since biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute, and they require the person being authenticated to be present at the time and point of authentication. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional systems, and it can be easily combined with password techniques to enhance the offered security. Steganography utilizes typical digital media such as text, images, audio, or video files as a carrier (called a host or cover signal) for hiding private information in such a way that unauthorized parties cannot detect or even notice its presence.

An efficient Steganographic method for biometric signals hiding in image objects focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. In the proposed system, the biometric signal is initially enciphered using a chaotic pseudorandom bit generator and a chaos-driven cipher, based on mixed feedback and time-variant S-boxes. Use of a chaos-based cryptographic module is justified by the following facts. (a) Chaos presents many desired cryptographic qualities, such as sensitivity to initial conditions, a feature that is very important to an encryption scheme, (b) a chaotic pseudo-random bit generator works very well as a one-time pad generator, and one-time pads have been proven to be information-theoretically secure, (c) implementations of popular public key encryption methods, such as RSA or El Gamal cannot provide suitable encryption rates, while security of these algorithms relies on the difficulty of quickly factorizing large numbers or solving the discrete logarithm problem, topics that are seriously challenged by recent advances in number theory and distributed computing and (d) private-key bulk encryption algorithms such as Triple DES or Blowfish, similar to chaotic algorithms, are more suitable for transmission of large amounts of data. However, due to the complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be concisely and clearly explained, so as to enable detection of cryptanalytic vulnerabilities.

After encryption, an image, containing the owner of the biometric signal, is analyzed, and the host image object (IO) is automatically extracted based on the method proposed. Next, a DCT-based algorithm is proposed for hiding the encrypted biometric signal to the host image object. Compared to other related schemes, the incorporated approach has the following advantages. (a) It is one of the most efficient algorithms of the literature that better support robust hiding of visually recognizable patterns, (b) it is hierarchical and has multiresolution characteristics, (c) the embedded information is hard to detect by the human visual system (HVS), and (d) it is among the best-known techniques with regards to survival of hidden information.

Finally, the signal is redundantly embedded to both sub bands of the selected pair, using a nonlinear energy-adaptable insertion procedure. Differences between the original and the Stego-object are imperceptible to the HVS while biometric signals can be retrieved even under compression and transmission losses. Experimental results exhibit the efficiency and robustness of the proposed scheme. At last, the hidden image is decrypted using inverse DCT technique. After decryption, the original image is seen by the user.

In this method (C-PRBG) is used to create the keys that trigger the whole encryption to increase security, and the encrypted biometric signal is hidden in a VO, which can reliably be detected in modern applications that involve teleconferencing. In this work they proposed a biometric signal is encrypted by a chaotic cipher. Afterwards the encrypted signal is inserted to the most significant wavelet coefficients of the VO, using its Qualified Significant Wavelet Trees (QSWTs). They find the QSWT estimation for to find the high-energy band to find the sub-band to hide the data of encrypted signals QSWTs provide both invisibility and significant resistance against lossy transmission and compression, conditions that are typical in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego-object (SO). After extracting the biometric from stegno-object authenticate human face and biometric with data-base.

II. SYSTEM DESCRIPTION

This paper proposes a robust authentication mechanism based on semantic segmentation, secure force encryption and data hiding. Assuming that user X wants to be remotely authenticated, initially X's image is automatically segmented, using a head and body detector. Next, one of X's biometric signal is encrypted by a secure force algorithm. Afterwards the encrypted signal is inserted to the image object, using its Discrete Cosine Transform (DCT). DCT used to calculate frequency complexity of image (i.e., Group images with similar frequency components). Finally, the Inverse Discrete Cosine Transform (IDCT) is applied to provide the stego-object(SO). Experimental results, regarding: (a) security merits of the proposed encryption scheme, (b) robustness to steganalytic attacks, to various transmission losses and JPEG compression ratios and (c) bandwidth efficiency measures, indicate the promising performance of the proposed biometrics-based authentication scheme.

Block Diagram: (proposed system)

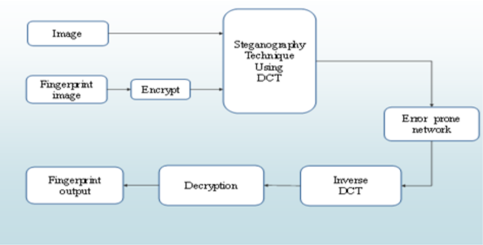


Fig. Proposed system

Steganographic system

The Steganographic system comprises of a stego system encoder that accepts the cover image, the message to be hidden and the optional key to generate the stego image that is identical to cover image as per the human visual systems (HVS). The encoder implements the algorithm for steganographic data hiding, it may use substitution technique or transform technique. The cover can be transmitted via a channel or uploaded to the internet. At the other end the decoder works on the stego image with the optional key to extract the hidden message.

Algorithm of Steganography:

The DCT based steganography encoding algorithm had been developed as follows:

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8*8 block of pixels.
Step 4:Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.

The DCT based steganography decoding algorithm has been developed as follows:

Step 1: Read stego image
Step 2: Stego image is broken into 8*8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.

Decryption:

The decryption module receives at its input a vector of encrypted samples, the initial control parameters and initial conditions for the secure force algorithm which produce the same onetime pad used during encryption, but now for decryption purposes. The procedure is terminated after the final sample is decrypted and all decrypted samples are reordered, to provide the initial biometrics signal.

Module names

1. Image processing
2. The encryption mechanism
3. Hiding the encrypted biometric signal
4. Message recovery

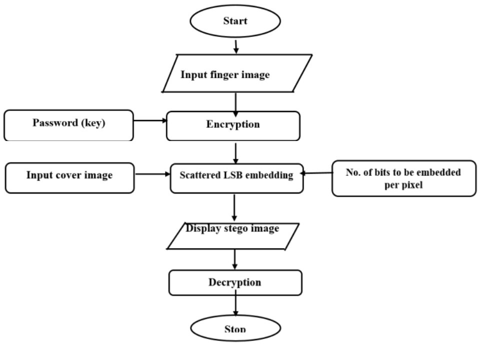


Fig. Flow chart

III.PERFORMANCE ANALYSIS

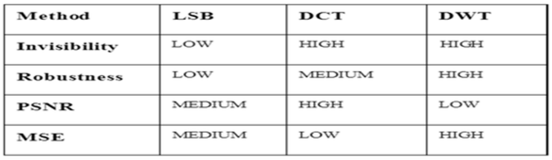
The performance analysis of LSB, DCT and DWT algorithms are carried out on steganography using PSNR and MSE. PSNR computes the peak signal to noise ratio, in decibels, between the two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high, then images are best of quality.

Images	PSNR			MSE		
	LSB	DCT	DWT	LSB	DCT	DWT
Jet	50.9015	52.9532	46.7309	0.5325	0.3320	1.3912
Baboon	51.3214	53.2092	46.8262	0.4834	0.3130	1.3610

Table : LSB, DCT, DWT Technique

The DCT algorithm is more suitable for the steganography application compared to the LSB and the DWT based algorithms.

The following table shows the parameter analysis of steganographic methods.



Method	LSB	DCT	DWT
Invisibility	LOW	HIGH	HIGH
Robustness	LOW	MEDIUM	HIGH
PSNR	MEDIUM	HIGH	LOW
MSE	MEDIUM	LOW	HIGH

Table : Parameter analysis of Steganography methods

PSNR value shows the quality of image after image after embedding the data. From the experiment results it is observed that the PSNR of DCT is high as compared to other two algorithms.

IV.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 authentications). Thus, there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a secure force encryption. 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 stego-analytic attacks. Experimental evaluation and detailed theoretical security analysis illustrate the performance of the proposed system in terms of security.

In future research, the effects of compression and mobile transmission of other hidden biometrics signals (e.g. voice or iris) should also be examined. The problem of lost biometrics data is also of high interest. Techniques from the areas of image error concealment, region restoration or region matching can be used for this purpose. For instance, the lost biometrics data can be concealment from the authentication module, so that it attempts to perform authentication even though parts are missing (parts that do not contain any crucial information (e.g. terminations/bifurcation in case of fingerprints).

References

[1] 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, 4, pp, 1411-1418, Mar 2014.
[2] H. C. Hsiang and W.K. Shih, Weaknesses and improvements of the YOON Ryu-YOO remote user authentication scheme using smart cards, Computer Communications no 32, pp.649-652, 2009.
[3] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transaction on Circuits Systems for video technology, vol, 14(1), pp.4-20, 2004.
[4] 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, Lecture Notes in Computer science, vol.7335. Spinger-Verlag, 2012, pp.391-406.
[5] P. Kocher, J. Jare, and B. Jun, Differential power analysis, "proceedings of advance in cryptology" (crypto'99) vol.54, pp, 388-397, Santa Barbara, USA.
[6] I. E. Liao, C-C. Lee, and M-S. Hwang," A password authentication scheme over insecure networks," Journal of Computer and System Science, vol.72, pp.727-740, 2006.
[7] Leung KC, Cheng LM, Fong AS, Chan CK: Cryptanalysis of a modified remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 2003.
[8] R. Madhusudhan and R.C. Mittal," Dynamic id-based remote user password authentication scheme using smart cards: A review," Intelligent algorithms for Data-Centric Sensor Networks, vol.35, no, 4, pp.1235, jul.2012
[9] M. Ramkumar and A.N. Akansu, "capacity estimates for data hiding in compressed images," IEEE Transaction on image processing, vol.10(8), pp, 1252-1263, 2001.
[10] K. R. Rao, P. Thrimurthy, and B. R. Babu, "A novel scheme for digital rights management of images using biometrics," International Journal of computer science and Network Security, vol, 9(3), pp, 157-167, 2009.
[11] E-J Yoon and K-Y, Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for cards on ellipse curve cryptosystem," The journal of supercomputing, vol.63, no, 1, pp, 235-255, jan 2013.