INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2319 - 2323
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

MULTILAYERED PASS KEY FOR SECURE IMAGE TRANSMISSION

S.Angelin Nivedita, PG Scholar, Dept Of Computer Science Engineering, Mailam Engineering College, Villupuram.

Dr.T.Priyaradhikadevi, M.Tech,Ph.D, Professor And Head, Department Of Computer Science Engineering, Mailam Engineering College,Villupuram.

Abstract:

In recent years due to the security concerns in the service oriented environments like cloud computing, compression of encrypted data has drawn much attention. A highly secure algorithm is used to encrypt the full image after which lossless compression is done on the encrypted image. To provide reasonably high level of security we couple image encryption scheme operated in prediction error domain with binary permutation. Huffman coding based approach is established for efficiently compressing the encrypted image. Hence a highly efficient image encryption then compression (ETC) scheme considering the lossless compression is designed. Experimental results shows that this encryption then compression scheme provides better performance than existing schemes.

Keywords: image compression, image encryption, lossless compression.

1. INTRODUCTION

Security of multimedia data has become more important as they are frequently transmitted over open networks. Our military, government, medical fields etc. deals with a large number of confidential images which fallen in to wrong hands may end in catastrophic conditions. Hence encryptions of images are both legal and ethical. The classical way of efficiently and securely transmitting redundant data is to first compress and then encrypt the data. At the receiver side decryption is done followed by decompression. However in some practical scenarios like service oriented environments (e.g., cloud computing), sensoring networks etc., encryption is to be done prior to compression due to its limited computational resources. To maximize the network utilization, the channel provider has an overriding affinity to compress all the network traffic. So it will be much desirable if compression task is carried out by the channel provider who is having plenty of computational resources. In recent years, processing of secured signals directly in the encrypted domain has gained a great attention. Since no semantic information about the image is available, compression in the encrypted domain was considered to be infeasible. Extensions of compression of encrypted videos were also studied later. Linear transformations were used to compress the cipher text produced by the stream cipher. Videos with higher irregular motions were compressed, which derives temporal side information from the previous slides and also generates spatial side information by having partial access to the current frame. Compared with the state-of-the-art lossless image coders that accept unencrypted inputs, the existing systems still fall short in compression performance. The major aim here is the construction of a pair of protocols to overcome any adversaries and various aspects of information

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2319 - 2323
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

security, coupled with compression of images which is almost equally efficient as compressing the unencrypted versions. Lossless compressions of 8-bit grayscale images are considered. Encryption scheme is permutation based approach over the prediction error domain which provides reasonably high level of security.

2. PROPOSED SYSTEM

The encryption algorithm considered here should consider both the security and the ease of compressing the encrypted image. The image encryption scheme operates in the prediction error domain. Schematic diagram of image encryption then compression is given in Figure-1. Consider a transmitter A needs to send a confidential image IM to receiver B with the help of the channel provide C. As the content owner A being a resource deprived mobile device has no incentive to compress the data before encryption while the channel provider C having plenty of computational resources increases the network utilization by compressing the protected data without any access to the secret keys. For each pixel IM(j,k) of the image IM, a prediction $\tilde{I}M(j,k)$ is to be found.

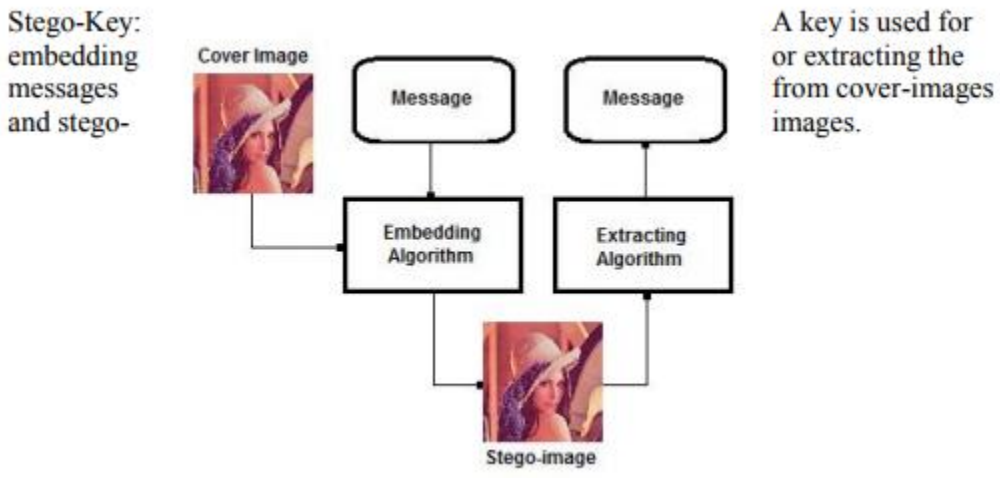

Fig.1. Image Basic Structure

This can be done with the help of an image predictor like GAP, MED etc. But here we use cumulative addition method which is simple and easy to implement while considering other methods. Cumulative addition method is defined as follows. Pixel value IM(1,2) will be replaced with IM(1,1). Similarly IM(1,3) will be replaced with IM(1,2) and it goes on. Coming to second row, elements will be replaced with the corresponding elements of previous row and this will be repeated throughout the image.

3. RELATED WORK

The channel provider does not have access to any of the secret keys. Compression has to be done in the encrypted domain. The major design challenge faced was the compression of encrypted image since no image structure is obtained to enable traditional compression. Less complexity has led to the selection of Huffman coding for lossless compression of encrypted image. Using Huffman coding channel provider C

simply compresses the encrypted image IMe into B. Huffman coding is a lossless compression standard in which frequently occurring values are given smaller codes and values that rarely occur are given larger codes. Algorithm works on the estimated frequency of occurrence for each possible value of the source symbol.

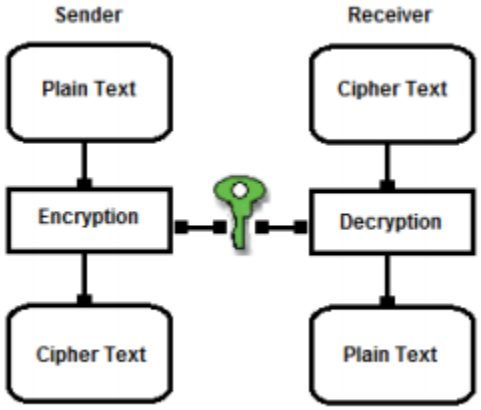

Fig.2.Structure

Steganography means is not to modify the structure or layout of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor, it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Stegano analysis. It is also known as asymmetric encryption; it uses two keys one for encryption and second for decryption. In public key cryptography, both keys work in pairs of public and private keys. Sender uses the public or known key of receiver to encrypt the message and receiver decrypt the message with his/her private or secret key.

4. ANALYSIS

In our case, user enters its user name and password into the client browser, a JavaScript code run on client machine to encrypt password characters [14], secondly prepare the image buffer (BMP 64x64 size) into the memory and then embed the encrypted password into image data using basic LSB method. After embedding the data into images from JavaScript call back function further encode it into the base64 data format. This base64 data further sent to the server end as a regular image tag. On the other side server retrieves the request from the client end. It fetches the image tag data (in base64 format) for further processing. This base64 encoded data decoded by base64 decoder using ASP.net on the server end. Apply the de-stego algorithm on image data and extract the encrypted password, secondly that encrypted password further decrypted and finally retrieve the actual password. This actual password is further used to match with SQL Database server for verification purpose against its user name. If actual password matched with the user name database then server generates the response signal to the client as a legitimate user otherwise forbade for further processing.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2319 - 2323
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

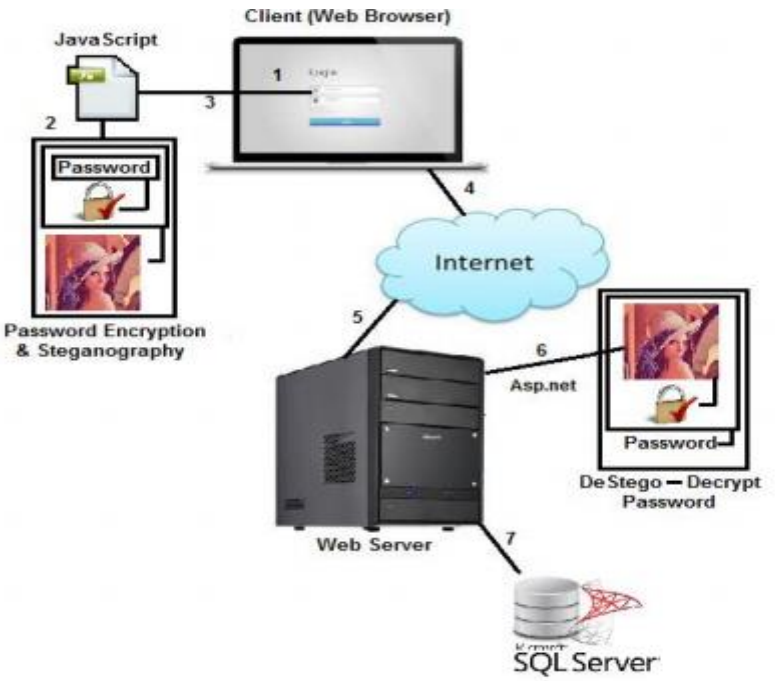

Fig.3. Main System Analysis

According to the proposed model, we notice the computation complexity is quite high due to image data manipulation for both client and server ends, but the security level is high due to multi-layer secure method over untrusting networks. In case, if any intruder monitors or fetches the request and responses of communication between server-client he/she are unable to find the password for authentication due to image steganography and further encryption of the password. Server and client already synchronized by encryption and stegano graphic algorithms before handshaking.

CONCLUSION

Web application over unsecured internet using encryption with image steganography. To achieve experiments results, for sending and securing passwords, used encryption and steganography algorithms in JavaScript at the client end. On the receiving end (the server side) also implemented above algorithm in ASP.Net, which further extracts the password from stego-image and verifies it with the SQL database server. The main target of the proposed scheme is to secure the password for authentication in server/client environment in multi-layer security such as encryption, and further encrypted password embedded in image using steganography. In case, if the intruder steals the image over network he will still not be able to decode the password from the image file.

REFERENCES

[1] Anderson, R. J. Stretching the limits of Steganography, in Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, (1996), pp. 39-48.

[2] Mehdi Hussain and Mureed Hussain, A Survey of Image Steganography Techniques, International Journal of Advanced Science and Technology Vol. 54, May (2013).

[3] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Transactions on Information Forensics and Security 5 (2) (2010) 201–214.

[4] Hussain, M. Hussain, M, Pixel intensity based high capacity data embedding method, IEEE International Conference Information and Emerging Technologies (ICIET), Pakistan, June (2010).

[5] Hussain, M. and Hussain, M, Embedding data in edge boundaries with high PSNR, Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept (2011).

[6] Mehdi Hussain, M. Hussain, Information hiding using edge boundaries of objects, International journal of security and application, (2011).

[7] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., (1999).