www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18916-18920

A Survey on Secret Data Transmission Using Various Steganographic Aspects

Ajin P Thomas, Sruthi P.S,Jerry Rachel Jacob,Vandana V Nair,Reeba R

Sreebuddha College Of Engineering,Alappuzha ,India
ajinpthomas@gmail.com , sruthips395@gmail.com, jerryjacobsbce@gmail.com, Vandananair1295@gmail.com, Reeba.amjith @gmail.com

Abstract

The security of Transmission of data becomes a huge issue in information and communication Technology. So ,to ensure the security of data during transmission, Two major techniques are adopted. They are Cryptography and Steganography. In these, the input data is encrypted using encryption algorithms and embedded into carrier image then transmitted through a communication channel, at the receiver side, data decrypted using data decryption algorithms is restored with error free. We are conducting a survey in this paper based on different steganographic and cryptographic methods for Data security.

Keywords:-*Cryptography, Steganography, Image encryption*

INTRODUCTION

To improve the security of data,The information we want to is embedding with in an image. This type of data hiding mechanisms provides additional security. Steganography and Cryptography are the two major techniques enable secure data transmission over the Internet. Both these techniques similar in the sense that, they are used to transmit information securely. Cryptography involves encryption of the message using an encryption key and send it as a cypher text while steganography involves hiding the information within a seeming harmless message. Steganography provides more security than crptography if the transmission of data is through an untrusted medium.

2. LITERATURE SURVEY

Rishay Ray and Tripti Das,Nath [I] provides a system that uses a randomized data hiding technique where the bit pattern

is hidden in random locations of the cover file. Two algorithms are used: (i)MVGCM proposed by Nath to encrypt secret message, (ii)To insert the encrypted secret message in the standard CF by changing the least significant bit (LSB) of bytes at random locations in CF. The offset matrix is generated from the text key provided by the user, using MSA randomization method. The 16x16 offset matrix determines the distribution of SM. A block of three 256 bytes sub-block are considered for embedding the SM. The sub-blocks are randomly chosen and the bits are embedded in the locations of the sub-blocks, corresponding to the respective elements of the offset matrices for

the sub-blocks. Two separate key strings are entered by the user for both the hiding and un-hiding process .

Rakesh sukla,Hari om Prakash [II] introduces a Unconditionally Secure and AuthenticatedOneTime pad Cryptosystem. In one time pad the plain text is combined with random key. It has a property of perfect secrecy. It is known as one time pad because the pad or key can be used only once. One time pads are used in pairs, one copy is kept by each user. The key must be exchanged via secure channel. Each generated key contains a Status and the Segment Information. This ensures that each encryption uses unused part of the Pad. Status information is used to identify own and imported keys and their validation. Segment information to store info about the already used bytes of that key. For generation the random mouse movements are taken on a white empty screen. Based on the random movements of the user mouse and the system time and date, a random seed is fed into a CSPRNG which generates a random set of pads. The plain text is encrypted with one time pad and the output being base64 encoded for final result.

Prashant Johri, Amba Mishra, Sanjoy Das, Arun kumar[III] provides a study on various steganographic methods to improve data security. **Text steganography** involves changing format of an existing text within a file. Here we use text file as a cover media. It is more vulnerable for attack as it is easy for an attacker to detect the pattern. **Image steganography** hides the secret message inside an image file. Secret message is embedded within the image pixels depending upon its low or high frequency distribution.

Audio steganography uses audio file as a cover medium to hide the secret message. It is more difficult than hiding data in image file as human auditory system is more sensitive compared to human visual system. Various methods involve LSB coding, Parity coding, Echo data hiding. **Video steganography** is a technique used to transmit a hidden message within a video file. It is less prone for attacks as video file is a combination of text, image and audio. Inorder to embed the message video is first converted to consequent images or frames. Then masking and filtering is applied to the selected frame to analyse which area will be appropriate to hide the information. Hence it is difficult for an attacker to identify which frame of the video is containing the hidden information.

R .Nivedhitha , Dr. T Neyyappan[IV] propose a scheme that includes the encryption of image done by DES (Data Encryption Standard)algorithm. Here, the encrypted image is hide in another image using LSB method to increase the degree of security. In this, the encrypted image is embedded within another image is called cover image. Cover image carrying the embedded secret image is called stego image. DES algorithm encrypts an 8 bit block of plain text to an 8 bit cypher text with the help of a 10 bit key. The algorithm includes Initial permutation, a complex function fk, simple permutation function, and finally Inverse permutation. Embedding the encrypted image in the carrier image is done by

the LSB method. In this, the combination of steganography and cryptography is achieved By the DES algorithm and LSB method.

Md.Rashedul Islam, Ayassha siddiqa [V] proposed a system involves AES Cryptography and image Steganography. The technique has two main parts; (i) Changing the plain text to cipher text.(ii) Hiding the cipher into a image by steganographic techniques. In this, introducing a new concept status bit. It is an improvement over normal LSB method. Here we use MSB bits for the filtering the pixel, whether it is capable of hiding the message bit or not. Instead of embedding the message in the LSB bit positions of the carrier image, the system uses status massage for the embedding process.

Anderson and Fabien[VI]. Here, it is defining Steganography. Steganography has introduced from a greek word meaning "hidden writing". Least significant byte (LSB) substitution is widely used. Inorder to secure the stegosystem algorithm atleast a bit more, we can with some of the conventional pseudo random number generator supplied password or key will give us the initial factor. The number that is generated will specify which pixel should be used for encoding next bit of embedded data. Data which hold effective information often has some redundancy. End user will think that this redundancy cost extra money and this is one of major limits. The entropy of the stegotext S is equal to sum of the convertext C entropy and the embedded material E entropy.

Mohammad Ali Bani and Aman Jantan[VII] introduces a technique for protecting the transmitted data are encryption and steganography. In this method exchange of information between the sender and receiver is done. It is done inorder to hide the information. Here it is done by two techniques. First is data mixing which is done on the sender side second is the data extraction in the receiver side.Here the information appears to be nothing out as usual and should be available to the receiver to rebuild the same secret transformation table, which is needed to rebuild the transformed image. The insertion positions of this information will be randomly selected. Thus it will be used to reduce the chance of encrypted data being detected. An Efficient Data Hiding Scheme Using Steganography and Cryptography Technique .

Mangesh Kulkarni, Prasad Jagtap, Ketan Kulkarni[VIII]. In this system,A Least Significant Bit (called LSB) method is used for hiding the information. The 8th bit of carrier files every byte is substituted by 1 bit of secret information. The Proposed system provides high level of security by dual ciphering method. In this system we are substituting the original message by using fourteen square substitution algorithms and after that we are applying the RSA encryption algorithm on substituted text and that encrypted cipher text is embedded in image. Hence the message is dual enciphered thus taking the security measures of information to next level. It provides three level securities one at substitution level, second at cryptog-raphy level, and third at Steganography level. If at

all the intruder suspects data it is very difficult for him to steal data. The degradation in image is not noticeable. The size of the image is not increase after embedding process.

K.B Shivakumar ,Y.Manjula[IX] introduces an enhanced secure image steganography using double encryption algorithms. It includes two encryption methods,ie the message is first encrypted using Advanced Encryption Standard symmetric encryption technique and further encrypted using public cryptographic method, Elliptic Curve Cryptography(ECC).This encrypted data is compressed with Lempel Ziv Welch(LZW) technique. Using knight tour algorithm, the compressed data is is embedded in selecting a cover image .Implementing two cryptographic algorithms followed by compression algorithm and unique knight tour algorithm LSB Steganography technique increases the quality and capacity of the image.

Mundra mounika,Bhagya pillai [X] propose a system using K mens algorithm in image steganography. In this method ,the image is clustered into various segments and hide the data in each of the segment.so various clustering algorithms can be used for the image segmentation. segmentation includes huge set of data in the form of pixels.where each pixel is again consist of three components, namely red,green,blue. In this method,we adopt k -means clustering technique to get a better performance in a small amount of time.

3. CONCLUSION

A combination of Steganography and Cryptography is a powerful technique for security of Data transmission. It provides additional security to the data.All these existing systems contains some problems,so we need to improve the secure data transmission by using powerful and efficient algorithms and combination of cryptographic and steganographic techniques.Hence data encryption and data decryption become error free.

Acknowledgments

We are grateful to our project guide and Asst Prof. Reeba.R for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department of Computer Science & Engineering of Sree Buddha College of Engineering, Alappuzha.

References

I. A new randomized data hiding algorithm with encrypted secret message using modified generalized Vernam Cipher Method: RAN-SEC algorithm,Rishav Ray, Jeeyan Sanyal, Tripti Das, Kaushik Goswami, Sankar Das, Asoke Nath(year 2011)

II. Unconditionally Secure And Authenticated One Time Pad Cryptosystem**,**Rakesh Shukla, Hari Om Prakash, R.Phani Bhushan, S. Venkataraman, Geeta Varadan(yr 2013)

III. Survey on steganography methods,Prashant Johri, Amba Mishra, Sanjoy Das, Arun kumar(yr 2016)

IV. ImageSecurityUsing Steganography And Cryptographic Techniques .R.Nivedhitha1,Dr.T.Meyyappan,M.sc.,M. Phil.,M.BA.,Ph.D2ResearchScholar1,Asso ciateProfessor2DepartmentofComputerSci ence&Engineering,AlagappaUniversity,Ka raikudi.Tamil Nadu,India.

V. An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit alongwith AES Cryptography,Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain5.

VI. On the limits of steganography ,Anderson and Fabien.

VII. New steganography approach for image encryption exchange by using the least significant bit insertion, Mohammad Ali Bani and Aman Jantan.

VIII. An Efficient Data Hiding Scheme Using Steganography and Cryptography Technique ,Mangesh Kulkarni, Prasad Jagtap, Ketan Kulkarni.

IX. Enhanced secure image steganography using double encryption algorithms, K.B Shivakumar ,Y.Manjula

X. Image steganography method using K-Means Clustering and Encryption techniques, Bhagya Pillai, Munda Mounika