International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 04, April 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Image Transmission using Stegnography in MANET's : A Review

M.krishnamoorthy[1], S.Nandhini[2], V. Ezhilarasu[3]
[1]*Assistant professor, Dept of CSA, SCSVMV University.*
[2,3.] *PG Students, Dept of CSA, scsvmv University.*

Abstract
Image Data is one of the most relevant and important term from the ancient Greek age to modern science and business. The amount of data and use of Image transformation for organizational work is increasing. So, for the sake of security and to avoid data loss and unauthorized access of data we have designed an image Stegnographic algorithm implementing both Cipher text and Plain text in Mobile Adhoc Networks(MANET) . This algorithm imposed a cipher text within a cover image to the stegno-image which is transferred from sender to intended receiver by invoking a distributed connection among them to achieve the Image data authentication.

Keyword: *Cryptography, Stegnography, RSA, Dedicated connection, JPEG image ,MANET.*

1. INTRODUCTION

As a part of information security "Steganography" is a wellknown concept, literally which signifies the meaning "Image writing" [12]. Steganography imposes the secret information within a cover object termed as stegno-image to escape detection and to retain the original information with minimum distortion. This stegno- image appears like a non-secret file in the MANET's and manages data to avoid drawing the attention towards itself as a content of security. *secret-information* + *cover*- image = *stegno*- image (1) Steganography had been widely used for secure communication [3]. The schemes used at this age are the physical process of Steganography. In modern digital steganography information is first encrypted. Then using an embedding algorithm in the transport layer encrypted information is embedded with the cover medium and transmitted over the network [10] [11]. Both cryptography and steganography provides data security and authenticity in MANET's. In contrast to cryptography which focuses on keeping the message secret while the existence of secret message may tempt the attacker whereas Steganography hides a message as well as the very existence of secret information [5]. Cryptography ensures privacy of message and structure of the message alter whereas stegnography ensures the secrecy of message and the structure of message does not alter [7] [3]. Stegnography may use in conjunction with cryptography by concealing the existence of the ciphered text so that the information is more secure in MANET's[4].
Media formats .JPEG, .BMP, .GIF, .MP3, .text etc. are suitable as cover medium because of their high degree of redundancy and availability and popularity over MANET's [6]. Depending on what type of cover-medium used, steganography is classified as audio steganography uses .WAV, .MP3 media formats, video steganography uses .MPEG, .AVI, image steganography uses .JPEG, .BMP, .GIF media formats. Audio steganography utilize the Psycho acoustical property of human auditory system (i.e. the presence of low-pitched sound is undetected in presence of a louder sound) and inserting data into digitalized audio-signals. LSB coding, phase coding, spread spectrum are some popular method of audio

steganography in MANET's. Video Steganography embedded the message within the video files. Due to its large size video Steganography is eligible to hide large amount of data in MANET'S. Image steganography technique utilize the weakness of human visual system [8] and embedded the information with a minor modification in image pixels. LSB coding, masking and filtering etc. are the image steganography method.

2. LITERATURE REVIEW

In [03], The Authors measured the quality factor of JPEG images by maintaining quantization tables and performed some permutations along with this scheme to transmit a hidden file. Authors in [03] combined cryptography with steganography by first encrypting a message using Vernam cipher and then embedding it with an image using LSB technique with shifting. Sudha.s [01] implemented neural networks to identify best locations in the host image to embed the secret data. Dr.J.Srinivasan superimposed dynamic cryptography with stegno analysis [04]. The LSB of the picture element is modified with the MSB of it and pixel selection is done using pseudo random number.

3. PROPOSED METHODOLOGY

Among various methods of Cryptography and Steganography we have used one of the Image Steganography method. This section presents a step-by-step solution to the Image stegnography problem described above. The encryption algorithm at the Sender's end and decryption algorithm at the Receiver's end are detailed below.

3.1 Image Stegnography in MANET's:

Image Steganography uses digital image as cover object to hide the information as it contains huge amount of redundant bits [9]. Images are divides into a matrix of pixels and each pixel is represented by bit pattern. Generally images are represented by 24bit or 8bit pixel either in the form of a binary file where each pixel represents three colors Red, Green and Blue (RGB) for color image or as a gray scale image [9]. In image steganography information is hidden within an image with a minor modification in the image pixels. In the specific domain of digital image various image formats exist for different applications such as JPEG (Joint Photographic Experts Group), GIF (Graphical Interchange Format), BMP etc. [3].
In this paper, we have used a .jpeg file as a cover medium. The original text is first encrypted using the well-known RSA cryptography algorithm. The generated cipher text is hidden behind the .jpeg image file for secure transmission of the data to the receiver. The encrypted text is appended at the end of the image file and finally the stegno file is exposed through an RMI architecture for different Client-Server actions.

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 04, April 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

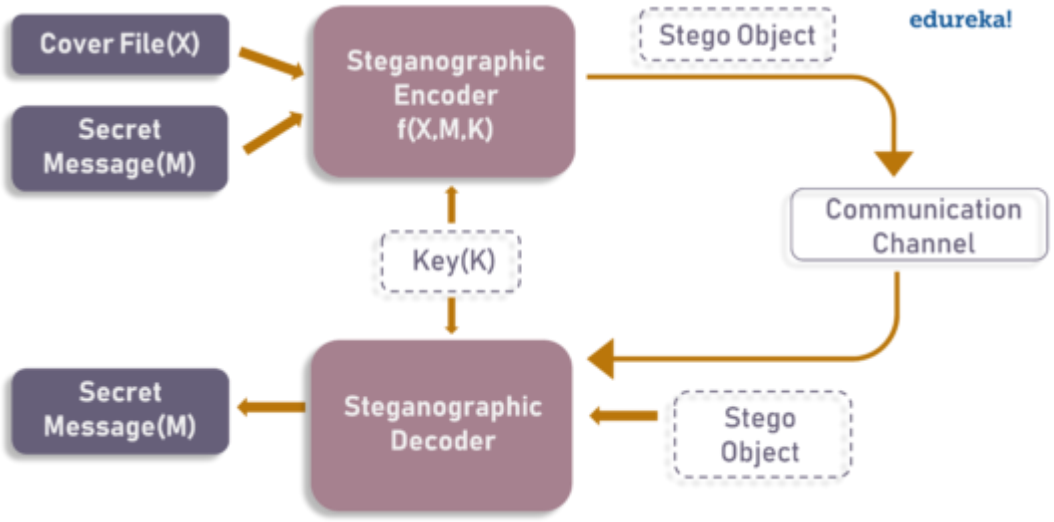

Fig 1.Image stegnography

3.1.1 PROPOSED ALGORITHM

Encryption Algorithm (Sender's end):

Step 1: Select the text file where the original message has been written.
Step 2: Encrypt the content of the text file using the RSA algorithm with the public key of the receiver.
Step 3: Select an appropriate cover image (.jpeg format).
Step 4: Read the header and footer of the selected image in an array buffer.
Step 5: Add the encrypted data at the end of image footer.
Step 6: Sender and receiver are connected to the network.
Step 7: Sender provides the receiver's IP address and then send the Stego-image if the IP address is valid.

Decryption Algorithm (Receiver's end):

Step 1: Receive the Stegno-image.
Step 2: Extract the encrypted message from the end of the stegnoimage in image footer
Step 3: Generate the private key and decrypt the extracted message and then create a text file.
Step 4: Save the text file at the desired location.

3.1.2 Key Used:

The privacy of any cryptography or steganography algorithm depends on the size of the key used. In the proposed algorithm, we have used the RSA algorithm for encrypting the text data. In RSA, two large random prime numbers are generated and are processed to create the private and public keys. These prime numbers need to be kept secret. The length of the RSA key depends on the number of bits used in the modulus function. In this algorithm, we have used keys of size 2048 bits.

4. CONCLUSION

Stegnography can protect data by hiding it but using it alone may not guarantee total protection. It is possible that by using a stegno encryption technique, enemy detects presence of text message in the image file and then he/she may succeed in extracting information from the picture, which can be disastrous in real life situations. This is same for plain encryption. In this case by seeing the meaningless appearing sequence of bits enemy can detect that some illegal message is being sent and we may land –up in a problematic situation. However, if one uses both the proposed methods, this will lead to 'security in depth'. The message should first be encoded using a strong encryption algorithm and then embedded into a carrier.

REFERENCES:

1. J. Srinivasan , S. Sudha ,Collision Detection in MANET based on Network Coding Technique,International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Volume 3 Issue 1 –NOVEMBER 2013.
2. Srinivasan.J, Mythili.K, Geetha.V , A Review on Routing Protocols in Cloud Computing Architecture **,** International Journal of Applied Engineering Research,Volume 10, Number 17, June-2015.
3. J.Srinivasan, Dr.S.Audithan , STI Protocol Design for Cloud Based Medical Imaging Repositories , International Journal of Applied Engineering Research, Volume 10, Number 17, June-2015.
4. J.Srinivasan, Dr.S.Audithan, STI Protocol Design to Improve the Security over Multi-hop Networks, International Journal of Computer Applications ,Volume 130 – No.11, November2015.
5. J.Srinivasan, Dr.S.Audithan, Secure Authentication Framework Design and Routing Metric (SAF&RM) based Communication in Multi-Hop Wireless Mesh Networks, Indian Journal of Science and Technology**,** *Vol 9(39),DOI:10.17485/ijst/2016/v9i39/96243, October 2016.*
7. J. Srinivasan, S. Audithan , Anonymous Secure Routing Protocol for Multi hop Wireless Mesh Network(ASRP) **,** International Journal of Engineering and Advanced Technology (IJEAT) , Volume-5, Issue-6, August 2016.
8. J. Srinivasan and S. Audithan, Secure and Efficient Multi-hop Routing for Wireless Mesh Networks, **I J C T A**, 9(2) 2016, pp. 911-918.
9. Srinivasan.J, Secure Anonymous Routing Protocol For Wireless Mesh Network, International Journal of Innovations & Advancement in Computer Science IJIACS,Volume 6, Issue 8,August 2017.
10. Srinivasan J.,Sleep Deprivation Attack in MANETS: A Review, IJRECE VOL. 6 ISSUE 2 , APR.-JUNE 2018.
11. Srinivasan J,Security Threats and Attacks of Wireless Network: A Review, ,International Journal of Innovations & Advancement in Computer Science IJIACS,Volume 7, Issue 5,May 2018.
12. Srinivasan.J, BLACK HOLE ATTACK IN MANETS: A REVIEW , JETIR June 2018, Volume 5, Issue 6 .