International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229151

Secure Data Transfer Through Internet Using Image Steganography

Nikita Sudhakar Jamgade, Kishor Peshwani

Jhulelal Institute of Technology, Department of Computer Science and Engineering MTECH KH No. 68 and 72 Village Lonara off, Nagpur, Maharashtra, India

ABSTRACT

Article Info
Volume 9, Issue 1
Page Number : 185-188
Publication Issue :
January-February-2022
Article History
Accepted : 08 Feb 2022
Published: 17 Feb 2022

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 data 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 Steganographic algorithm implementing both Cryptography and Steganography. This algorithm imposed a cipher text within a cover image to conceal the existence of the cipher text and the stego-image is transferred from sender to intended receiver by invoking a distributed connection among them to achieve the data authenticity.

Keywords : Cryptography, Steganography, RSA, RMI Architecture, Distributed connection, JPEG image

I. INTRODUCTION

As a part of information security "Steganography" is a wellknown concept, litera lly which signifies the meaning "covered writing". Steganography imposes the secret informa t ion within acover object termed as stego-medium to escape detection and to retain the original information with minimum distortion. This stego- medium appears like a non-secret file in the network and manages to avoid drawing the attention towards itself as a content of security. Secret-information + cover-medium = stegomedium (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]. Both cryptography and steganography provide data confidentiality and authenticity. 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 steganography ensures the secrecy of message and the structure of message does not alter [7].

Steganography may use in conjunction with cryptography by concealing the existence of the ciphered text so that the information is more secure [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 internet [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. Video Steganography embedded the message within the video files. Due to its large size video Steganography is eligible to hide large amount of data. 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.

II. METHODS

Among various methods of Cryptography and Steganography we have used RSA algorithm and Image Steganography method.

Rivest et al. invented RSA [1] algorithm and it is widely used public key cryptography algorithm having two algebraic structures: a public key R = Zn

+ X and a private group G = Z(∅(n))*X. In RSA algorithm two prime numbers (p and q) are taken initially and their products are used to generate the public key and private key. Public key consists of a value n and e, called modulus and public exponent respectively. Private key termed as d is called private exponent. The public key and private key generation of RSA algorithm is as follows:

Step 1: Choose two large, random prime number p and q, such that p ≠ q.

Step 2: Compute modulus n as n = p×q.

Step 3: Compute the Euler's totient for n as Ø(n) = (p-1)×(q-1).

Step 4: Select the public exponent e, where 1 < e < Ø(n) and e is a co-prime of Ø(n).

Step 5: Calculate the private exponent d as d = e1modØ(n).

The encryption operation in RSA for message P is done by the exponentiation to the eth power modulo

N: C = Pe modn (2)

Decryption of ciphered text C is the exponentiat ion to the dth power modulo n:

P = Cd modn (3) Explanation with example:

1. Choose two prime numbers, p = 61 and q=53
2. Compute Modulus n= pq, where n = 61*53 = 3233
3. Compute Euler's totient Ø(n) = (p-1)×(q-1), Ø(n) = 3120
4. Choose e co-prime to Ø(n) where 1< e < Ø(n), e = 17
5. Compute d = e-1modØ(n), d = 17- 1mod(3120) = 2753

Let the message to encrypt P = 123, we calculate C = 12317 mod(3233) = 855 and to decrypt C = 855, we calculate P = 8552753mod(3233) = 123

III. PROPOSED ALGORITHM

This section presents a step-by-step solutio n to the problem described above. The encryption algorithm at the Sender's end and decryption algorithm at the Receiver's end are detailed below.

Encryption Algorithm (Sender's end): Step 1: Select the text file where the origina l message has been written.

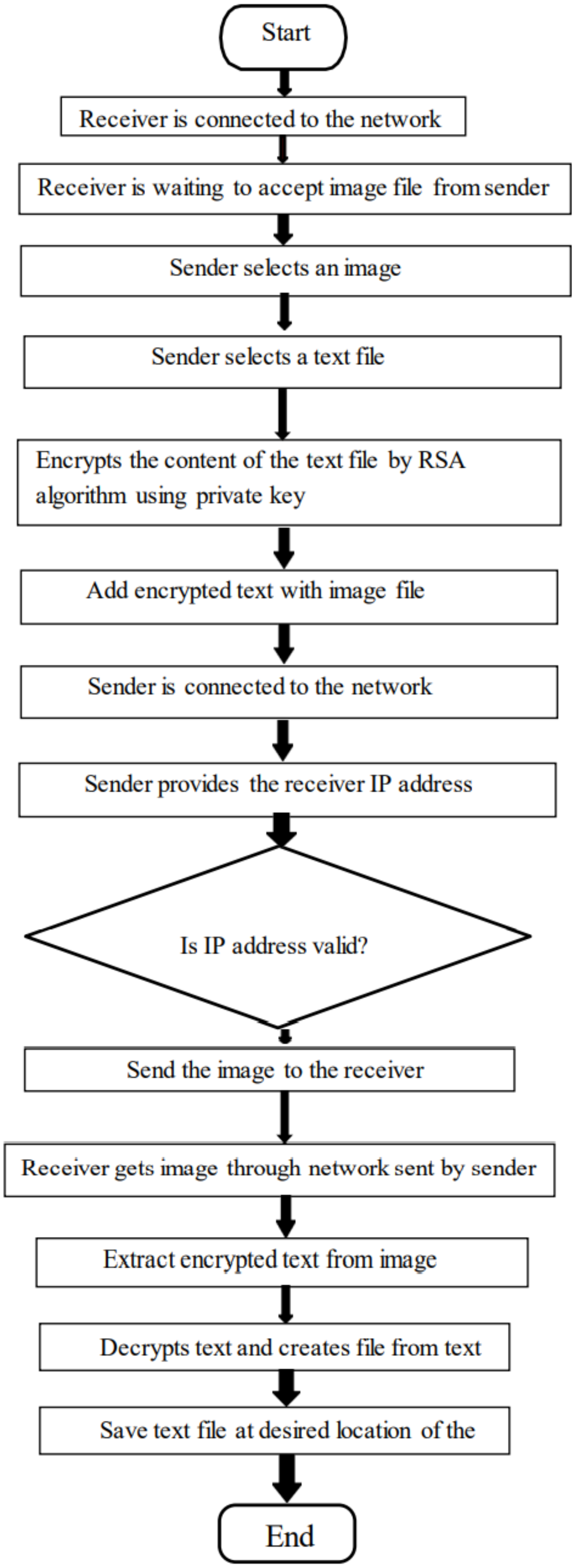
Step 2: Encrypt the content of the text file using the RSA algorithm with the public key of the receiver.

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.


Start
Receiver is connected to the network
Receiver is waiting to accept image file from sender
Sender selects an image
Sender selects a text file
Encrypts the content of the text file by RSA algorithm using private key
Add encrypted text with image file
Sender is connected to the network
Sender provides the receiver IP address
Is IP address valid?
Send the image to the receiver
Receiver gets image through network sent by sender
Extract encrypted text from image
Decrypts text and creates file from text
Save text file at desired location of the
End

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 Stego-image.

Step 2: Extract the encrypted message from the end of the stegoimage by reading the 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

IV. CONCLUSION

At this age of civilization exchanging data for communication through the network is an integral part of every organization and every sector of society. Our proposed algorithm is to secure this communication with a secure communication system by creating a distributed connection. This algorithm imposed an encrypted text which has been encrypted by using the RSA algorithm within a JPEG image and then the image file is send over the network i.e. we combining the concept of Cryptography and Steganography to make an illusion to the hacker that the sender sends an unsuspicious media file to the receiver. As an image file appear in the network as an innocent media file so it does not attract the hacker as a content of security. In this algorithm Cryptography makes the data secure as a cipher text and Steganography makes this cipher text disguise so that no one other than the intended receiver can know the existence of the cipher text within the image file. Here we have embedded the encrypted text at the footer of the chosen JPEG image file. In future our work will be focused on to embed the text within the image pixel and we will work to eradicate the problem of lossy compression related to the JPEG image and extend our work on other image formats like .BMP, GIF etc.

V. REFERENCES

[1]. Behrouz A. Forouzan, "Cryptography and Network Security", McGraw Hil , 2007.

[2]. Herbert Schidlt, “Java the Complete Reference”, 8th Edition, McGraw Hill, 2011.

[3]. N.F. Johnson and S. Jajodia, “Explor ing Steganography: Seeing the Unseen”, Computer, Vol. 31, No. 2, pp.26-34, 1998.

[4]. S. Song, J. Zhang, X. Liao, J. Du and Q.Wen, “A Novel Secure Communication Protocol Combining Steganography and Cryptography”, Procedia Engineering, Vol. 15, pp. 2767-2772, 2011.

[5]. A.J. Raphael and V. Sundaram, “Cryptography and Steganography-A Survey”, Internatio nal Journal of Computer Technology and Applicatio ns, Vol. 2, No. 3, pp. 626-630, 2016.

[6]. S.A. Laskar and K. Hemachandran, “An Analysis of Steganography and Steganalysis Techniques”,Assam University Journal of Science and Technology, Vol. 9, No. 2, pp. 83-103, 2012.

[7]. F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn,“Information Hiding-A Survey”, Proceedings Of International Conference on Protection of Multimedia, pp. 1062-1078, 1999.

[8]. Y.S. Huang, Y.P. Huang, K.N. Huang and M.S. Young, “The Assessment System of Human Visual Spectral Sensitivity Curve by Frequency Modulated Light”, Proceedings of IEEE International Conference On Engineering in Medicine and Biology, pp. 263-265, 2005.

[9]. T. Morkel, J.H.P. Eloff and M.S. Oliver, “An Overview of Image Steganography”, Proceedings of 5th Annual Conference on Information Security, pp. 111-116, 2005.

[10]. T. Handel and M. Sandford, “Hiding Data in the OSI Network Model”, Proceedings of 1st International Workshop on Information Hiding, pp. 1-7, 1996

Cite this article as :

Nikita Sudhakar Jamgade, Kishor Peshwani, "Secure Data Transfer Through Internet Using Image Steganography", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 1, pp. 185-188, January-February 2022. Available at doi : https://doi.org/10.32628/IJSRSET229151
Journal URL : https://ijsrset.com/IJSRSET229151