IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

Secure Approach To Data Transmission Using Steganography and RSA Technique Through TCP/IP Header

Basant Sah[1*] , V .K Jha[2]

[1]BIT Mesra(CSE), Ranchi, India
[2]BIT Mesra(CSE), Ranchi, India

Available online at: www.ijcseonline.org

Accepted: 22/Sept/2018, Published: 30/Sept/2018

Abstract- This is the time of web, in which whole world is associated with one another, thus significance of security builds step by step. To protect the data from unauthorized user, it is the new challenge for us so that we developed a very simple technique to transfer the data from one party to other by secure channel. As we know that Steganography is a digital technique for hiding information in some form of media, such as image, audio or video. Steganography has advanced routine with regards to hide information in bigger document so that others can't associate the nearness with a shrouded message. In this paper, we outline a framework, which utilizes highlights of both cryptography and in addition steganography, where TCP/IP header is utilized as a steganographic transporter to hide encrypted data. [1] Steganography is a valuable apparatus that permits secretive transmission of data over the correspondences channel. [2] In this paper we have use the MKA algorithm [4] to embed the data inside the image so that capacity of data will be large.

Keywords: LSB,Steganography, Cryptography, Encryption, TCP/IP Header, Fragmentation, MKA algorithm.

1. INTRODUCTION

Always imparted through the Internet are streams of data created from numerous assorted applications, for example, web based business exchanges, sound and video spilling or web based visiting. The security of such information correspondence, which is required and indispensable for some applications these days, has been a noteworthy concern and progressing subject of concentrate given that the Internet is by configuration open and open in nature. Many techniques have been proposed for providing a secure transmission of data. Hence, in order to provide a better security, we propose a data hiding technique called steganography (MKA algorithm) [4]] along with the cryptography technique. Steganography is the workmanship and study of concealing information into various bearer documents such as text, audio, images, video, etc. In cryptography, the secret message that we send may be easily detectable by the attacker.[6] but in steganography, the secret message is not easily detectable. The persons other than the sender and receiver are not able to view the secret message. The secret message that sender transfers over the network, can be encrypted and hidden into TCP/IP header using Stego object. The Stego object is an encrypted message embedded into carrier file. This paper is organized in four sections like Introduction, Basic of Steganography, proposed work, and conclusion

2. STEGANOGRAPHY OVER A COVERT CHANNEL

Secret channel is a correspondence channel through which data transmits by damaging security standards. The correspondence through clandestine channel is non-evident way. TCP/IP Header can fill in as a transporter for a steganography through incognito channel. [1] As the steganography is data hiding technique, sender embeds the encrypted data by using carrier file.[3-5] At the encoder process encryption algorithm is applied over secret file then it embeds with carrier file, it generates stego object that hides into unused fields of TCP/IP header, which implies covert channel. The carrier files may be text, image, audio or video. In our system, we are using images as carrier. Digital images are very useful and secure carrier for hiding the secret massage. Image is a collection of color pixels. In standard, 24 bit bitmap we have three color components per pixel:
Red, Green and Blue. Each component is 8 bit and have 28 i.e. 256 values. In 3 megapixel image you can hide 9 megabits of information using this technique, which is equivalent of 256 pages of book. If we only change the lowest bits of each pixel, then the numeric values can only change by a small percentage. We can only alter the original pixel color value by ±7. Stego object traverses over a communication channel.[8] Stego object is divided into packets. These packets are hidden in TCP or IP header's unused fields. Many fields from the TCP or IP header are not used for certain situations.

3. PROPOSED WORK

In this paper we are focusing on Identification field of the IP header to hide secret encrypted data. Identification field is used only when fragmentation occurs. At the receiver end, to reassemble the packets, identification field tells the right order for that. If fragmentation is not occurred, then identification field will always be unused, so that we can use this 16 bit field to hide secret encrypted message. To avoid fragmentation, we use MTU. Maximum transfer unit decides limit for packet size for transmission over network. Sender and receiver, both should have awareness of MTU unit. [9] For the encryption and decryption we use RSA technique to encrypt the data so that it will be more secure. Before sending the data first of all preprocess the data t.e replace the white space, tab, non printable character from the file so that its size will decrease and payload capacity will increase [20].RSA is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations.[11] Only the particular use knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

RSA Approach

1. Choose two particular prime numbers p and q.
For security purposes, the whole number's p and q ought to be picked aimlessly, and ought to be of comparative piece length. Prime whole numbers can be proficiently discovered utilizing a primality test.
2. Compute $n = pq$.
n is utilized as the modulus for both people in general and private keys. Its length, typically communicated in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient work.
4. Choose a whole number e with the end goal that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are co prime.
e is discharged as the general population key example.

e having a short piece length and little Hamming weight results in more effective encryption – most normally 216 + 1 = 65,537. Be that as it may, significantly littler estimations of e, (for example, 3) have been appeared to be less secure in some settings. [5]

5. Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the multiplicative reverse of e (modulo φ (n)).
This is all the more obviously expressed as: understand for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
This is regularly registered utilizing the expanded Euclidean calculation. Utilizing the pseudo code in the Modular numbers area, inputs an and n compare to e and φ(n), individually.

6. d is kept as the private key example.
Concurring above produced key encode the message and transmit through the safe channel.

3.1 Structure of TCP header:

Structure of TCP header is appeared in Fig 3.1(Appendix A), we can utilize insignificant fields in particular arrangement number and choice fields.

3.1.1 Sequence number*:*

It is 32 bit field. Which is use to distinguish the present position of information byte in the portion. Succession Information and Acknowledge
Number is arbitrarily created number in view of: nearby host, neighborhood port, remote host, and remote port.

3.1.2 Options:

Keeping in mind the end goal to give extra usefulness a few discretionary parameter may utilized between a Tcp sender and recipient. The most widely recognized choice is the greatest section measure alternative. This choice gives the sender ,greatest section measure the beneficiary willing to acknowledge.

3.2 Structure of IP header:

Structure of IP header is as shown Fig 3.2, irrelevant fields used in IP header are given as follows:

3.2.1 Type of service:

It is 8 bit field. The type service in IP header is potential for using as steganographic carrier, because many networks never use them.

3.2.2 Identification field:

It is 16 bit field. When fragmentation of message occur the value of identification field is copied into all fragments. The identification number helps the destination in reassembling the fragments of the datagram.

3.2.3 Flags:

It is 3 bit field which gives information about Reserved, Do not fragment bit and more fragment bit.

3.2.4 Fragmentation offset:

This bit is 13 bit field. When the fragmentation of message occurs this field specifies the offset, or position in the overall message, where the data in this fragment goes.

3.2.5 Option:

Alternatives are not required for each datagram to be sent. They are utilized for organize testing and troubleshooting reason.

Algorithm:

Step 1 : First of all read the data character by from the file, after preprocessing the data .
Step 2 : Generate the public and private key using RSA approach.
Step 3 : Encrypt the data and put these data in TCP Header where bit is unused and send.
Step 4 : Decrypt the data .
For details see the flowchart in given flowchart in appendix B.

4. CONCLUSION

In this work we explored the steganography techniques as well as MKA algorithm [4] to hide high amount of data inside the image then after encrypt the data using RSA approach. TCP/IP header is used as a carrier for transmission of the secret information or data. The TCP/IP suite along with the covert medium further enhances the security of the system since attackers are more concerned over the "http". The proposed method will stay away from illicit transmission of mystery correspondence on the web and will give a superior secure framework if there should be an occurrence of Authentication. Just idea based examined here definite usage will be later, this is my innovative idea not practically implemented right now I will later do it.

References

[1] R.M. Goudar, Prashant N. Patil, Aniket G.. "*Secure Data Transmission by using Steganography*" ISSN 2224- per) ISSN 2224-896X Vol 2, No.1, 2012

[2] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn,"*Information hiding- Survey*", IEEE, (7):1062- 1078, 1999.

[3] G. J. Simmons, "*The Prisoner's problem and the subliminal channel in Advances in Cryptology*", Proc.crypto '83:55–67, 1983.

[4] . H.B.Kekre, Archana Athawale, and Pallavi N.Halarnkar ," *Increased Capacity of Information Hiding in LSB's Method for Text and Image*" World Academy of Science, Engineering and Technology Vol:2 2008-05-22.

[5] Udit Budddia and Deepak Kundur, "*Digital video steganalysis exploiting collusion Sensitivity*",IEEE, 1(4):502- 516, 2006.

[6] Furuta, T,.Noda, H., Niimi, M., Kawaguchi E,"*Bit-plane decomposition steganography using wavelet compressed video*", Joint Conference of the Fourth International Conference, 2(5): 970 - 974, 2003.

[7] V.Karthekayani and kammalakan, "*Conversion grayscale image to color image with and without texture synthesis*", International journal of computer science and network security, 7(4):11-16, 2007.

[8] Eiji Kawaguchi and Richard O. Eason, "*Principle and applications of BPCS- Steganography*", Proc. SPIE ,3528: 464-473 , 1999.

[9] Nameer N. EL-Emam, "*Hiding a Large Amount of Data with High Security Using Steganography Algorithm*" Jordan Journal of Science publications, 3 (4): 223-232, 2007.

[10] K B Raja, C R Chowdary K R Venugopal, "*A Secure Image Steganography using LSB, DCT and Compression Techniques on Images*", IEEE, 170-176, 2005.

[11] Naofumi," *Technique of lossless steganography*", IEICE Transactions on Communications, 90(11):1-4, 2007.

[12] .Nan jiang and wan jiang, "*Random oracle model of information modeling*", World academy of science, 18:1307-6884, 2006

[13] Steganography [tG. Pulcini, \Stegotif,"http://www.geocities.com/SiliconValley/ 9210/gfree. Html, 10/28/2008

[14] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "*Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory*," The International Society for Optical Engineering, Electronic Imaging, San Jose, CA, USA, 2005.

[15] G. Xuan, Y. Q. Shi, D. Zou, J. Gao, C. Yang, Z. Zhabg, P. Chai, W. Chen, C. Chen, "*Steganalysis based on multiple features formed by statistical moments of wavelet characteristic Functions*," IH 2005 LNCS 3727, pp. 262-277, Springer-Verlag Berlin Heidelberg 2005.

[16] H. Noda, J. Spaulding, M. Shirazi, M. Niimi and E. Kawaguchi, "*BPCS Steganography Combined with JPEG2000 Compression*", Proceedings of Pacific Rim Workshop on Digital Steganography , pp. 98-107, 2002.

[17] J. Huang and Y. Shi, "*Adaptive image watermarking scheme based on visual masking*", Elect. Lett., vol. 34, no. 8, pp. 748-750,1998.

[18] A. Piva, M. Barni, F. Bartolini and V. Capellini, "*DCT-Based watermark recovering without restoring to the uncorrupted original image*", in Proc. of IEEE ICIP, pp. 520-523, 1997. 438

[19] Rahul Jain,Naresh kumar ." *Efficient data hiding scheme using lossless data compression and image steganograpgy* ", International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 4 No.08 August 2012

[20] Swami Vivekanand Mahavidhyalaya etl," *Information Security: A Review on Steganography with Cryptography for Secured Data Transaction* ",Int. J. Sc. Res. in Network Security and Communication , ISSN: 2321-3256 , Volume-5, Issue-6, Dec 2017 .

[21] A. Sudha1, A. Basheer Ahamed, " *Img-Protect : Privacy Protection of Images in Online Social Networks Using Watermarking Scheme* ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology , Volume 3 | Issue 7 | ISSN : 2456-3307

Authors' Profiles

Mr.Basant Sah received his MCA degree from IGNOU in 2005 and MTech (CS) from BIT Mesra, Ranchi, Jharkhand (India) in 2008; also qualify the GATE Exam in 2006. He is associated with the BRCM College of engineering & Technology as an assistant Professor in CSE Department. At present, he is research scholar at Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand (India). His research interest includes Information security, algorithm Design, automata theory etc.

Vijay Kumar Jha received his BE in Electronics from SIT Tumkur in the year 1996, M.Sc. Engineering in Electronics from MIT Muzaffarpur in the year 2007 and PhD in Information Technology in the Area of Data Mining from MIT Muzaffarpur, in the year 2011. He is working as an Associate Professor in the Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Ranchi, Jharkhand (India). His research interest includes Data mining, ERP etc.

Appendix A

List of figure

In given figure we demonstrate that the vast majority of header field is unused amid information transmission, we proposed to shroud the information in showed header design.

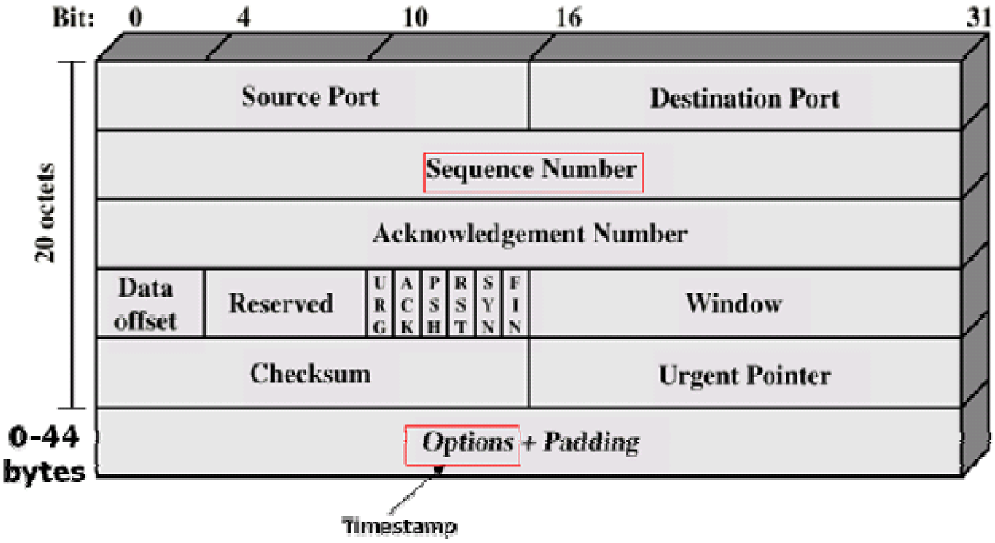

Fig.3.1 TCP header

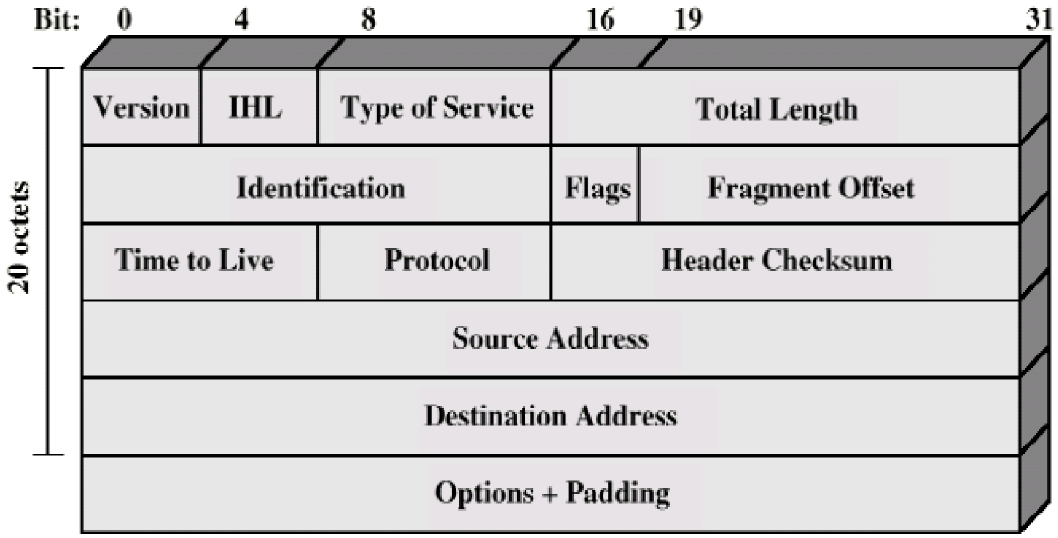

Fig.3.2 IP Header

Appendix B

In proposed technique we have use modify kekre's algorithm [19] to embed the data inside the image and send it using secure channel.To do this following are the flowchart .

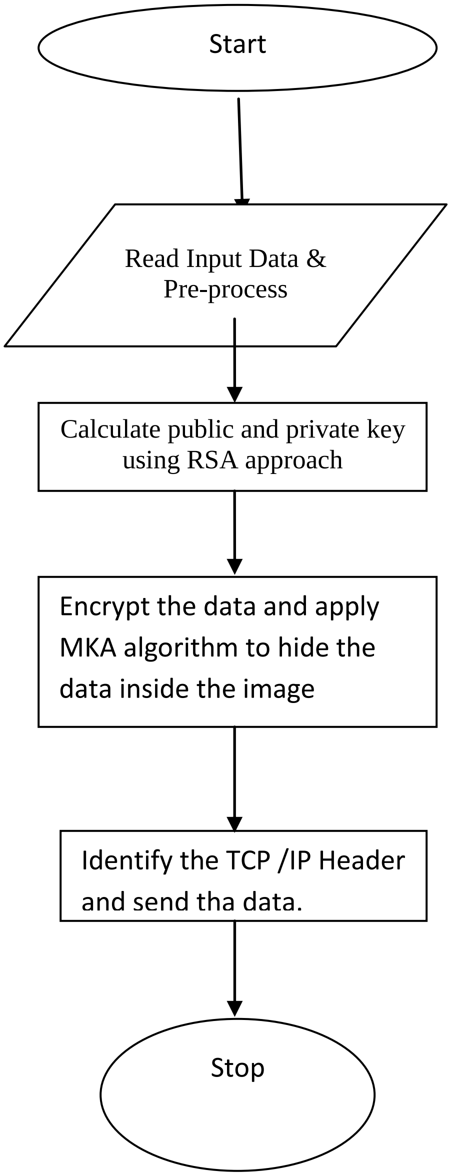
Start
Read Input Data & Pre-process
Calculate public and private key using RSA approach
Encrypt the data and apply MKA algorithm to hide the data inside the image
Identify the TCP /IP Header and send tha data.
Stop

Figure.3