ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Survey: A Hybrid Approach to Secure Transmitted Message by Combining Steganography and Asymmetric Cryptography

[1]Pooja Singh, [2]Hardik Upadhyay, [3]Mitesh Thakor, [4]Krunal Suthar

[1]M. Tech Student, Department of Computer Engineering, MEC, Basna, India

[3]Assistant Professor, Department of Computer Engineering, MEC, Basna, India

[2]Assistant Professor, Department of Computer Engineering, GPERI, Mahesana, India

[4]Assistant Professor, Department of Computer Engineering, SPCE, Visnagar, India

ABSTRACT: Steganography is a technique allows a user to securely hide messages in a cover media and to extract hidden message from the same media. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. There is a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. We would propose the combined concept of Cryptography and steganography with the use ECC(Elliptic Curve Cryptography).This is the hybrid approach to hide the data in encrypted form. The main focus of research is to encrypt the data with Asymmetric Cryptography and apply the steganography technique to hide encrypted data. Existing hybrid approach which uses RSA with steganography is suffering from big performance hit. Proposed approach would expected to achieve batter result mainly in terms of performance as compare to existing schemes**.**

KEYWORDS*:* Steganography, Cryptography, Asymmetric encryption, Elliptic curve cryptography

I. INTRODUCTION

Information technology is continually changing, discoveries are made every other day. In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data: via e-mails, chats, etc. The data transition is made very simple, fast and accurate. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorised users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate.

In order to improve the security features in data transfers, many techniques have been developed like: Cryptography, Steganography, etc. While Cryptography is a method to conceal information by encrypting it to "cipher texts" and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

"Steganography" and "Cryptography" are closely related constructs. The hidden or embedded image, audio or a video files act as carriers to send the private messages to the destination without any security breach. Steganography techniques can be implemented on various file formats such as audio (".mp3", ".wmv.", etc.), video (".mpeg", „.dat", etc.) and images (".jpeg", ".bmp", etc.). However, the images are the most preferred file format for this technique. At present, there are a lot of algorithms that help in executing the Steganography Techniques. The aim of this paper is to describe a method for using together cryptography and steganography through some media such as image, audio, video, etc.

The rest of the paper is organized as follows. Section II gives details about related work. Section III Describe detailed comparative study about various available schemes followed by conclusion in Section IV. Last section contains list of references used.

II. SURVEY ON VARIOUS SECURITY PROPOSALS OF DATA BY ENCRYPTION AND EMBEDDED METHOD

Various researchers give different schemes and views for data security by using hybrid approach of steganogarphy and cryptography.

Authors at [1] presented a method that can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications. In the case of a secret message being transferred the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred.

This multimedia data can be transferred in the normal way. Video files and image streams can also be used to transmit data. In case of image streams part of message can be sent in each image. This will increase the security of the system, however the time consumption will increase in this case. The researchers of[2] proposed the scheme based on two levels of data encryption . This technique combines the features of both cryptography and steganography which will provide a higher level of security. It is better than either of the technique used separately. The length of the plain text is also encrypted and sent which provides greater advantage for receiver in order to check the correctness of the decrypted data. Two levels of data encryption provide increased strength. In transferring secret message, two keys are used: One for the purpose of data encryption. Second key is obtained from the matrix based on the property derived out of the image itself. This method is also proved to be secure.

III. COMPARATIVE STUDY

The table-I shows above gives detailed comparison about the various schemes proposed by a researcher. The table gives the description about the basic technique used with the benefits that researcher gets as well as the limitations found in schemes.

Criteria Group →	Encryption/Staganography oriented measures						Others	
Individual Criteria → Providers ↓	Encryption (Data in rest)	Encryption (Data in transition)	Hash based tech. used ?	Authentication ?	Flexible security options	Key exchange required ?	Algo/Flowchart shown ?	Experimental setup ?
[3]	✓	✗	✗	✗	✗	✓	✗	✓
[4]	✓✓	✗	✓	✗	✗	✗	✓✓	✗
[5]	✓✓	✗	✗	✗	✗	✓	✓✓	✓
[6]	✓	✗	✗	✗	✗	✓	✓	✓
[7]	✓✓	✓	✗	✓	✗	✓✓	✗	✓✓
[8]	✓✓	✓✓	✗	✗	✗	✓✓	✗	✓✓
[9]	✓	✓	✗	✗	✗	✗	✓	✓

Table I: Comparative study

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

IV. CONCLUSION

In this paper, we studied various research proposals on data security, using steganography and cryptography to increase the security level of the data while transmitting data over network. We also made a comparative table which can be used by layman to have handy information about the proposals. Some of the proposals are based on public key encryption and some adopt private key techniques. We believe that data security is an area packed of challenges and of vital significance, and many research problems are yet to be identified.

REFERENCES

[1] Piyush Marwaha, Paresh Marwaha "Visual Cryptographic Steganography in images" *IEEE* 2010.
[2] S Usha, G A Sathish Kumar, K boopathybagan "A Secure Triple Level Encryption Method Using Cryptography and Steganography" *IEEE* 2011.
[3] Amal Khalifa "Scientific LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography" *IEEE*, 2014 pg:106-108
[4] Anil Kumar , Rohini Sharma "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" ,*International Journal of Advanced Research in Computer Science and Software Engineering* , Volume 3, Issue 7, July 2013
[5]Vivek Jain, Lokesh Kumar, Madhu Mohan Sharma, Mohan Sadiq, Kashitiz Rastogi, "PUBLIC-KEY STEGANOGRAPHY BASED ON MODIFIED LSB METHOD", *Journal of Global Research in Computer Science*, Volume 3, No. 4, April 2012
[6] Domenico Bloisi and Luca Iocchi, IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY, *http://www.dis.uniroma1.it /~bloisi/steganography/isc.pdf*
[7] Ajit Singh ,Swati Malik , Securing Data by Using Cryptography with Steganography, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, Issue 5, May 2013
[8] Joyshree Nath, Ashoke Nath" Advanced Steganography Algorithm using Encrypted Secret Message" *International journal of Advance Computer Science and applications*, Vol. 2, No. 3, March 2011.
[9] Shaikh Ammarah P.,Vikas Kaul, S K Narayankhedkar Security Enhancement for Data Transmission using Elliptic Curve Diffie-Hellman Key Exchange" *International Journal of applied information syaystems(IJAIS)*-2014.