International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

A Survey on Enhancement of Text Security Using Steganography and Cryptographic Techniques

Priya Jain[1], Somesh Kumar[2], Raj Kumar Goel[2]
[1]M. Tech Student, [2]Assistant Professor
Department of Computer Science Engineering,
Noida Institute of Engineering & Technology, Greater Noida, Uttar Pradesh, India

ABSTRACT

Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for securing data transfer. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. Many different carrier file format scan be used but digital images are the most popular because of their frequency on the internet. The digital images are the most popular because of their frequency on the Web among all different carrier file formats. Image steganography, achieves the secrecy by embedding data into cover image and generating a stego-image. There are many types of steganography techniques each have their advantages and disadvantages. This paper discussed a technique used on the advanced LSB (least significant bit) and RSA algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

Keywords: *Stegnography, Cryptography, LSB*

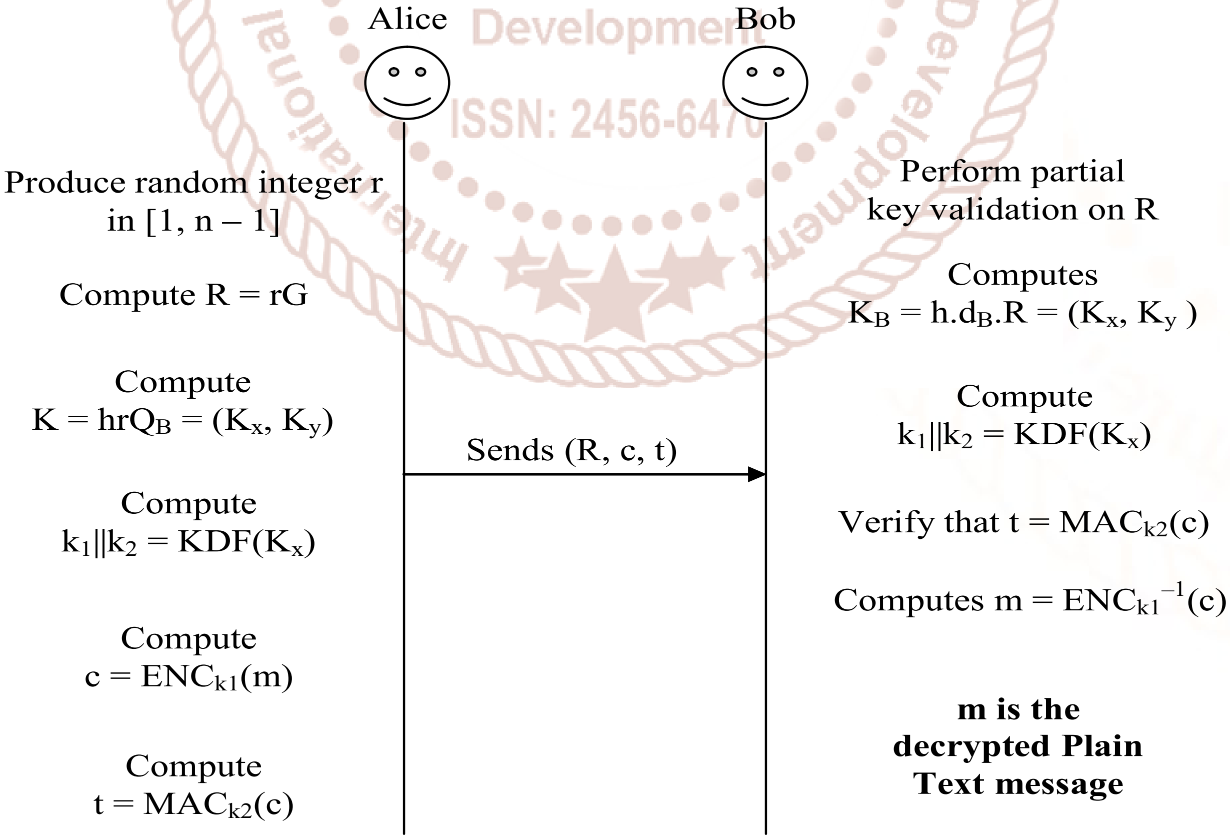
I. INTRODUCTION

The growing use of Internet among public masses and availability of public and private digital data and its sharing has driven industry professionals and researchers to pay a particular attention to information security. Internet users frequently need to store, send, or receive private information and this private information needs to be protected against unauthorized access and attacks. Presently, three main methods of information security being used: watermarking, cryptography and steganography. In watermarking, data are hidden to convey some information about the cover medium such as ownership and copyright. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people. Steganography techniques are based on hiding the existence of information by embedding the secret message in another cover medium. While all three are information security techniques cryptography and steganography are having wide application as watermarking is limited to having information particularly about the cover medium. With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets. Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers Cryptography systems can be broadly classified into symmetric-key systems and public key systems. The symmetric key system uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. The public- key systems that use a different key for encryption as one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receivers public key. The receiver then decrypts this message using his private key. In this paper describes all the techniques and proposed works based on cryptography and steganography.

II. LITERATURE REVIEW:

The word steganography is originally derived from Greek words which mean “Covered Writing”. It is defined as "hiding information within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected" [1]. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [2, 4,5,7]. Basically, the purpose of cryptography and steganography is to provide secret communication. Steganography can be used to cloak hidden messages in image, audio, video and even text files. According to [7], the two most common methods used for hiding information inside a picture, audio and video files are LSB (Least Significant Bit) and Injection. The survey of Johnson [6] appeared in the “Information hiding” book, which limits its distribution compared to a Journal paper which can be more affordable. The classification, herein, of the techniques and that of Johnson are different. Johnson classify steganography techniques into: Substitution systems, transform domain techniques, spread spectrum techniques, statistical methods, distortion techniques, and cover generation methods. Johnson survey neither talks about the history of steganography nor its applications.

Several techniques have been proposed by researchers for securing electronic communication. In the research work of [9], the researchers proposed cryptography and steganography for securing data transfer using images as cover objects for steganography and key for the cryptography. The performance of the proposed ISC (Image-Based Steganography and Cryptography) system was presented and the system was compared with F5 algorithm. Also, [10] proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step, finds the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide.


Alice
Bob
Produce random integer r in [1, n – 1]
Compute R = rG
Compute $K = hrQ_B = (K_x, K_y)$
Compute $k_1||k_2 = KDF(K_x)$
Compute $c = ENC_{k1}(m)$
Compute $t = MAC_{k2}(c)$
Sends (R, c, t)
Perform partial key validation on R
Computes $K_B = h.d_B.R = (K_x, K_y)$
Compute $k_1||k_2 = KDF(K_x)$
Verify that $t = MAC_{k2}(c)$
Computes $m = ENC_{k1}^{-1}(c)$
m is the decrypted Plain Text message

III. CRYPTOGRAPHY

Cryptography is the art and science of achieving security by encoding messages to make them non readable. In this, the structure of message is scrambled to make it meaningless and unintelligible unless the decryption key is available. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of something or someone. Cryptanalysis is the reverse engineering of cryptography. There are several ways of classifying cryptographic algorithms. The three types of algorithms are:

1. **Secret key Cryptography:** Use a single key for both encryption and decryption
2. **Public Key Cryptography:** Use one key for encryption and another for decryption.
3. **Hash Functions:** Use a mathematical transformation to irreversibly "encrypt" information

IV. STEGANOGRAPHY TECHNIQUES

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data.

Spatial domain techniques are classified into following categories:

1. Spatial domain techniques

I. Least significant bit (LSB)
II. Pixel value differencing (PVD)
III. Edges based data embedding method (EBE)
IV. Random pixel embedding method (RPE)
V. Mapping pixel to hidden data method
VI. Labeling or connectivity method
VII. Bit Plane Complexity Segmentation (BPCS)

I. LSB: this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

II. BPCS: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

III. PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3. Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) v)Embedding in coefficient bits.

V. COMBINED CRYPTO STEGANOGRAPHY

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret N message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use

Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.

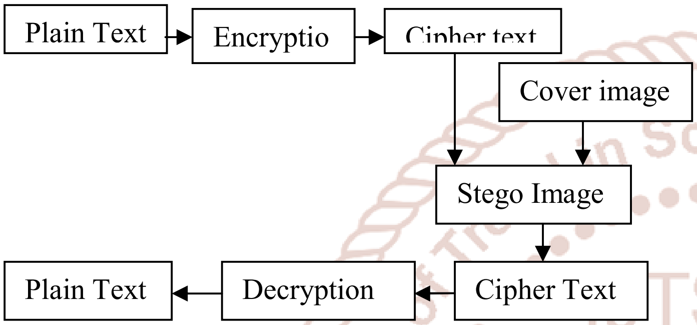


Figure 2: Systematic graphical representation of combined Cryptography and Steganography

In figure 2, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganography technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message

The steganography approaches can be divided into three types [8]:

1. Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

2. Secret Key Steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

3. Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

VI. CONCLUSION

A secured advanced based LSB technique for image steganography has been proposed. An efficient steganography method for embedding secret messages into cover images without producing any major changes has been accomplished through advanced-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been proposed, which makes our technique secure and more efficient than LSB. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message.

REFERENCES

1. R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice "Andre Leier. Cryptography with DNA Binary Strands. Bio Systems, 57:13–22, April 2000. Communications, 16(4), pp. 474-481.

2. Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. International Journal of Computer Applications. 8(9), pp. 7-10.

3. Jasleen Kour, "Steganography Techniques –A Review Paper", International Journal of Emerging Research inn Management &Technology, Volume-3, Issue-5, May 2014, pp 132-135.

4. Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

5. Jie Chen. A DNA-based, bio-molecular cryptography design. In Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on, volume 3, pages III–822-825 vol.3, May 2003.

6. Mark D. G. 2003. Chameleon Image Steganography- Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ghazy/Steg/References/ref13.pdf.

7. N. F. Johnson and S. C. Katzenbeisser, “A survey of steganographic techniques”, in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House,

8. Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.

9. R. J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, IEEE Journal Selected Areas in

10. Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

11. S. B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

12. T. Morkel, J. H. P. Eloff, M. S. Olivier, ”An Overview of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.