An Approach of Data Security for Data Transmission through Images using Cryptography

Payel Majumder, Supravat Mondal and Bijoy Kumar Mandal

Abstract

Todays, there is a more important network security in term of information transmission or any data storage. Since data security representation of data is gaining importance, data in the form of images are used to exchange and convey information between entities.

As the use of digital techniques for storing and transmitting of data through the images are increasing very fast and also it becomes more important issue for protecting the confidentiality, integrity and authenticity of images. There are various techniques which are discovered to encrypt the images to make them more secure. The primary goal of this paper is data hiding for security. There, we try to propose a method to provide authentication of users and ensure integrity, accuracy and safety of information. Hence, an image-based data transmission needs more effort during information encryption and decryption for data security.

Keyword: Data Hiding, Cypher Text, Cryptology, Stenography, Dynamic Key

I. Introduction

The The cryptography methodology used for encryption of plain text [1, 2] and steganography for data hiding though image [3] are commonly used well and mainly, these techniques are applied to generate the cipher or cover their existence respectively [4]. The steganography technique is methodology and science of communicating in an approach that hides the existence of the communication [5]. The Steganography hides the message so it cannot be seen; Cryptography encrypts a information so it cannot be understood to unauthorized users [6, 7]. Although both methods generate a double security for information transmission, a study is made to combine both cryptography [8] and Steganography methods into one system for improved concealment and security.

The origin of the word cryptology lies in ancient Greek. The word cryptology is made up of two components: “kryptos”, which means hidden and “logos” mean word [9]. Cryptology is as old as writing itself, and has been used for thousands of years to safeguard military and diplomatic communications. Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process [10]. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources [11, 12]. So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker. The main aim of the modern cryptography can be seen as: user authentication, data authentication (data integrity and data origin authentication), non-repudiation of origin, and data confidentiality. In the following section we will elaborate more on these services. Subsequently we will explain how these services can be realized using cryptographic primitives [13, 14].

In this research area we can study the techniques for decoding cipher original information and detecting the hiding information in image are called cryptanalysis and steganalysis [15, 16]. The previous denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of expose the covert messages. The aim of this paper is to describe a method for integrating together cryptography [17, 18] and steganography through some media such as image only. The technique of steganography is usable to all text information that contains redundancy. People often transmit digital pictures over email and other Internet communication, and color image is one of the most common ideas for sending secret information. Moreover, steganography systems for the color image seem more interesting because the systems operate in a transform space and are not affected by visual attacks stenography is a special case of data hiding [19]. The main goal of steganography is to escape detection of secret message. Steganography uses in different form generally digital form of steganography are used for communication over the internet. In this paper digital form of steganography is used that is hiding a message inside an image

II. METHODOLOGY

The In this system, the sender needs to use Steganography and cryptography concept. So this system will get more secure from attack. We propose a double encrypted key generation algorithm, which generates dynamic and complex keys and avoids key sharing issues like transmission noise and brute force attack. Here we get the unique character set from the user, which appreciates the security of key by having a dynamic nature. We are going to dynamically map the divided sub-parts with the sub-parts of image then the encryption will done on each of the parts for making it more secure. The block diagram of sender and receiver is shown in Figure 1 and Figure 2. A. Steps involved in the proposed system at the sender side is as follows

A. Steps involved in the proposed system at the sender side is as follows

Step 1: Get the unique character set from user

Step 2: Form the alphabetical tire like structure with the unique character set.

Step 3: Chose an image in the public web site.

Step 4: Divide the plain text into number of words (say n) present in that plain text.

Step 5: Divide the image into sub-parts, where the number of sub-parts >=n(say m)

Step 6: Dynamically mapping of sub-parts of plain text with sub parts of image.

Step 7: Then the generated key is given as input to the cryptographic algorithm for encryption with each sub-parts of plain text to obtain cipher text. (Number of cipher text =m).

Step 8: Then send all the cipher text using the concept of stenography.

B. Steps involved in the proposed system at the receiver side is as follows

Step 1: Get the shared unique character set from sender.

Step 2: Form the alphabetical tire like structure with the unique character set.

Step 3: Chose the same non-volatile image in the public web site.

Step 4: repeat steps from 4 to 7 as in sender side.

Step 5: Then the generated key is given as input to the cryptographic algorithm for decryption to obtain the plain text from cipher text.

Step 6: Receive all the cipher text and mapping table send by sender.

Step 7: Then the generated key is given as input to the cryptographic algorithm for decryption to obtain the plain text from cipher text and store each sub-parts in memory.

Step 8: Then extract the text from each image and store it in an array.

Step 9: With the help of mapping table arrange each sub-parts of the plain text.

III. ARCHITECTURE

In figure 1, there is shown the architecture of sender process and in figure 2, receiver side

Figure 1: Architecture of data process for sender side to send the information.

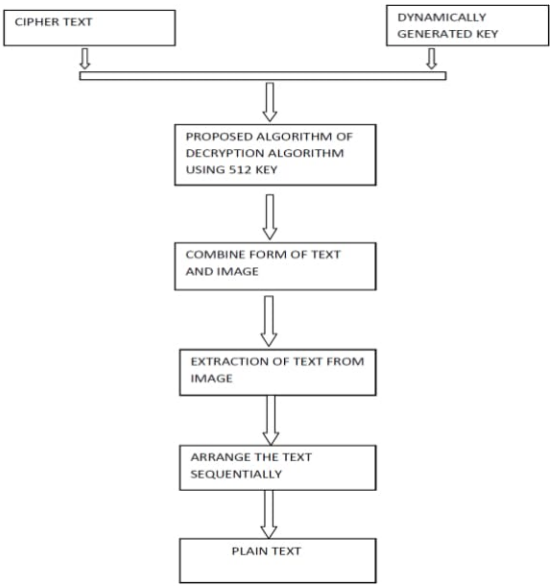

Figure 2: Architecture of data process for receiver side to retrieve the original information

IV. CONCLUSION

In this paper, we propose a methodology for hiding original data as cipher text in images and transmit the encoded image. Using the proposed methodology, we can hide larger capacity of information by stenography and cryptography without loss of imperceptibility. Thus the proposed methodology provides a more secure and convenient technique for secure data trans-mission among devices as compared to the other algorithm.

REFERENCES

[1] Bhattacharyya, S.; Khan, A.; Nandi, A.; Dasmalakar, A.; Roy, S.; Sanyal, G.; , "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.36-41, 11-14 Dec. 2011.

[2] B. Schneier, "Applied cryptography", second edition, NY: John Wiley & Sons, Inc., 1996

[3] J.G. Proakis, D.G. Manolakis, "Introduction to Digital Signal Processing", MacMillan Publishing Company, 1988

[4] Yambem Jina Chanu, Kh. Manglem Singh ,Themrichon Tuithung, " Image Steganography and Steganalysis: A Survey," International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012 ,pp.1-11

[5] L. Scripcariu, S. Ciornei, "Improving the Encryption Algorithms Using Multidimensional Data Structures", Proceedings of the Third European Conference on the Use of Modern Information and Communication Technologies, ECUMICT 2008, Gent (Belgium), pp. 375 – 384, Mar. 2008.

[6] Hawi, T.A.; Qutayri, M.A.; Barada, H.; , "Steganalysis attacks on stego-images using stego-signatures and statistical image properties," TENCON 2004. 2004 IEEE Region 10 Conference , Vol. 2, 21-24 Nov. 2004.

[7] http://phys.org/news/2011-08-world-toughest-encryption-scheme-vulnerable.html

[8] www.tutorialpoints.com

[9] B.D. Hahn, D.T. Valentine, "Essential MATLAB for Engineers and Scientists, 4e", Academic Press, 2010

Authors Details:

Payel Majumder
NSHM Knowledge Campus Durgapur
e-mail:payel.majumdar@nshm.com

Supravat Mondal
NSHM Knowledge Campus Durgapur
e-mail:supravat.mondal@nshm.com

Bijoy Kumar Mondal
NSHM Knowledge Campus Durgapur
e-mail:bijoy.mondal@nshm.com