INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

Ultimate Data Security Using LSB and Chaos Algorithm

P.Divyapriyadarshini[1], K.Prashanthini[2], S. Aravindsrinivasan[3]

[1] PG Scholar, Department Of ECE, SNS College of Technology, Coimbatore,India
[2] PG Scholar, Department Of ECE, SNS College of Technology, Coimbatore,India
[3]UG Scholar, Department of IT, Adithya Institute of Technology, Coimbatore,India

Abstract- *The information is an important for security concern while the data is to be transmitted in internet as it is prone to malicious attacks. To increase the security of the data, it is hidden inside an image. This technique is called steganography. While even the images are prone to attack, it is to be encrypted. A method of combining the steganography using LSB algorithm with a private key encryption of the message and image encryption using chaos algorithm is proposed. This apart from increasing the security of the data also provides a fast and efficient way of providing security. Steganography sometimes is used when encryption is not allowed. More commonly, steganography is used to supplement encryption. Information is hiding in encrypted file by using steganography, while deciphered hidden message is not visible.*

Keywords-*Cryptography, Steganography, LSB Algorithm.*

1. INTRODUCTION

The existing mechanisms involve the encryption of the image separately and information hide, the steganography is done separately. The prevailing methods thus are separate and it increases the chance for the intruders to track down the data. The method proposed here combines the process of steganography and image encryption into a single process so as to increase the security of the image as well as the message hidden in it with much effective and efficient algorithm. The aim of the project is to secure the information that is being transmitted in the internet for very confidential purposes. The hyper security is provided to a message and the image information by using the concepts of steganography and image encryption and combining it together to achieve the duel security for the content. The proposed method clears the security problem by increasing the information security using two highly efficient methods of steganography and image encryption with fast algorithm such as the LSB and chaos algorithm for the two processes. The steps are combined to produce the encrypted image which is not only an image but the one that has hidden data in it. Three public keys are used here which are only known to the sender and the receiver which also increases the data security further to another level. This project thus brings a high security image which can be transmitted in the internet without attracting much nuisance from the hackers. The algorithms used are fast so that the image can be encrypted and decrypted sooner which increases the possibility to transfer large number of information at a much sooner rate than the prevailing methods. A typical architecture of existing chaos-based image cryptosystem is composed of alternative permutation and diffusion stages multi-dimensional chaotic map is usually employed for image pixel permutation in the spatial domain while a one dimensional chaotic map is used for diffusion purpose.

The paper is organized as follows. Section II gives about overview of cryptography and stenography. In the section III it is briefly discussed about LSB algorithm in stenography .finally in the section IV the summary of the work is provided.

2. OVERVIEW OF CRYPT-OGRAPHY AND STEGANOGRAPHY

In cryptography a message is to be transmitted in a hostile channel, the message can be encrypted to maintain privacy. The plaintext is original message; the encrypted message is called the cipher text. The transformation form plaintext to cipher text is called encryption, and the inverse transformation cipher text is referred to as decryption. The encryption and decryption processes using a secret key, with the secret key it can perform a decryption operation. In encryption algorithm has set of all possible keys called key space. For both encryption and decryption use the same key is refers as Secret-key, or symmetric algorithms. On the other side, different keys are used for both encryption and decryption algorithms is refers as public-key, or asymmetric key. The encryption key is easily derived from the decryption key, but it should be computationally infeasible to obtain the decryption key from the encryption key. the message is encrypted using public encryption key and by using decryption key can be decrypted. Public-key encryption algorithms eliminate the need of a secure channel for key exchange. However, they are much slower than secret-key algorithms when a large amount of data needs to be encrypted. they are mostly used only to exchange the key used in secret key algorithms.

2.1. Symmetric Key Cryptography

Single key encryption was only algorithm used before public key encryption called Symmetric encryption.in this process both sender and receiver use same key. Key should have some secret with both sender and receiver and also provide same maintain in private.

2.2. Stengaography

An ordinary message containing with secret message and the extraction at receiver side.in image has secret information is hiding and also large variety of steganography. Applications require invisibility of the secret information; others require a large secret message to be hidden. It gives overview of image steganography. A good steganography meet requirements and apply to other techniques. In modern digital steganography, encrypted data by the usual means and then inserted, using LSB algorithm, into redundant data that is part of a particular file format such as a JPEG image. To make the images more secure encryption was used. The advantage of using LSB encoding technique is hard to detect and the original image is very similar to altered image.

2.2.1 Encryption

The message or information is encoded by using authorized parties and also read is refers as encryption. Encryption doesn't prevent hacking but it reduces encrypted read the data from hackers in scheme and encrypt plaintext by CHAOS algorithm into cipher text is unreadable. In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but respective person. In an encryption algorithm scheme by using the message or information is encrypted into an unreadable cipher text and usually done with the use of a key, message is encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized person is able to decode the cipher text using a decryption algorithm, that usually requires a secret decryption key. it needs a key generation algorithm to continuously produce keys. The single highly considerable reason for using encryption is to preserve confidentiality. And means that only respective receiver can read the message. Basic two types of encryption schemes: Symmetric-key and public-key encryption. The encryption and decryption are same in symmetric-key schemes. Both receiver and sender have to accept secret key before communicate. To publish the encryption key and encoded message in public key schemes. Only receiver can access to decryption key and also compatible of reading the encrypted message.

2.2.2 Decryption

The process data or information encoded into text as such that can able to read.it could be used to explain method of decrypting information with specified keys. In an image containing information or data is hiding by using encryption. From image can extract secret information or data in decryption. To send a message, text, an image in which the text should be embedded, and a key are needed. The encryption is used by key and to decide the information should be hiding in the image. An image or else a short text can be used as a key. To encrypt a message, a source image containing the information and the corresponding key are both required. The result will appear in the text after decrypt.

3. LSB ALGORITHM

LSB layer of image have several layer application provides in encryption and decryption. From last layer starts data writing (8stor LSB layer) significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires. The encryption is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination. The decryption is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden in that LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats, but the problem with the GIF image is whenever the least significant bit is changed the whole color palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect.JPEG, the direct substitution of steganography techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images.

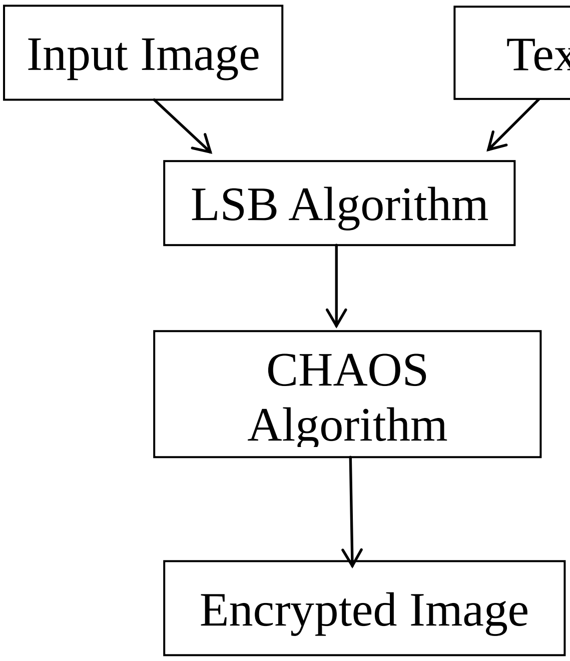

Figure 1: Process Flow

3.1. Input Image

The process starts with a GUI that takes the images of kind JPG, PNG, BMP as input for canvas image within which the message has to be hidden. And then, another GUI prompts asking for the text file that has to be hidden behind the message.

Figure 2: Screen Shot

After these two steps, the key used for steganography encryption is taken as the input. Steganography encryption module deals with the encryption of the text within the canvas image. This starts with converting the text message into its ASCII value string. This step is carried out as to operate on the text values and also to find the length of the message string. A header consisting of the message length is appended with the message. Then the message along with the header is encrypted by performing a bit XOR operation of the ASCII string of the text and the encryption key. Now, the message is converted into a bit stream so as to hide the message in the image. The image which has the color values is converted into uint8 (unsigned 8-bit integer) format for operating and hiding the message bit stream M. In computer, a color image is formed by color values of three color planes namely red, green and blue which forms the 3rd axis of an image that is formed by [x,y] pixels. The red, green and blue colors are represented by the numbers 1, 2 and 3 in mat lab, thus making a pixel to be represented as img(x, y,k) where K is the color plane value. The general idea behind the algorithm is to hide the i^{th} bit of message M in the LSB of (X, Y, K) th bit of the image. The M bits of the message are hidden using the LSB algorithm in the image in RGBBGRRG color order so as to make a secure way of hiding which makes the process of extracting the message from the image by a malicious user a hard process.

The steganographed image is then encrypted using three key values K1, K2 and K3 using chaos algorithm. The three key values which are public keys are predefined both at the sender and the receiver end for both encryption and decryption process. The image encryption is done by performing a bit XOR operation on the pixel value with one of the keys K1 or K2 or K3. And the key is incremented till certain extend for increasing security and complexity. After that the key value is reset and the process is carried out. After the encryption of the whole image, the image is saved with extension.

4. IMAGE DECRYPTION

The decryption process takes the encrypted image as the input and the key which should be the same as the encryption key. The decryption of the image follows the chaos algorithm to get the correct unencrypted image from which the text is extracted. The decrypted image is then sent to steganography decryption process which performs modulo arithmetic. The modulo arithmetic involves the extraction of the last bit of every pixel value of the image which is represented in uint8 format. The first eight bits are extracted to get the header that consists of the message size. With the message size known, modulo arithmetic is again applied to the image in the RGBBGRRG order to get the message bit stream.

5. CONLUSION

In this paper dealt with increasing the security of the text and image data which can be highly prone to attacks while on transmission through the combined effort of steganography and image encryption with much accuracy and encryption. It decreases the possibility of the data being cracked by unknown users who drastically want to steal or reveal information. In future, this project can be modified with much faster and hard to crack algorithms with efficient time and processing to deliver the message and image security to the core.

REFERENCES

[1]P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, pp. 767-769, 1994.

[2] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng., vol. 36,pp.992-998,1997.

[3] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," J. Opt. Soc. Amer.A, vol.15,pp.2629-2638,1997.

[4] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain," Opt. Lett.,vol.25,pp.887-889,2000.

[5] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt., vol. 41, pp. 5462-5470, 2002.

[6] L. G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," Opt. Eng., vol. 35, no. 9, pp. 2459-2463, 1995.

[7] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Amer.A, vol. 16, pp. 1915-1927, 1999.

[8] G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," Opt. Commun., vol. 193, pp. 51-67, 2001.

[9] Y. Frauel,A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Exp., vol. 15, pp. 10253-10265, 2007.

[10] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett.,vol.31,pp.1044-1046,2005.

[11] J. W. Goodman, Introduction to Fourier Optics, 2nd ed. New York, NY, USA: McGraw-Hill, 1995.

[12] J. Fridrich, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Singapore: World Scientific, 1997.

[13] Y. Honglei, W. Guang-shou, W. Ting, L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei, andM. Yuankao, "An image encryption algorithm based on two dimensional Baker map," in Proc. ICICTA, 2009.

[14] I. F. Elashry, O. S. Farag Allah, A.M. Abbas, S. El-Rabaie, and F.E. A. El-Samie, Homomorphic image encryption," J. Electron.Imag., vol. 18, no. 3, pp. 033002-1-033002-14, 2009.

[15]B. Javidi, Ed., Optical and Digital Techniques for Information Security New York, Springer Verlag, 2004.