www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19583-19586

Image Steganography Using LSB Along With IDEA Algorithm

Priyanka Tirkey[1], *Dipika Kudiyam*[2], *Neha Dhruw*[3], *Deepshikha Markam*[4], *Miss Rumi Ghosh*[5]

[1]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
pritirkey25@gmail.com
[2]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
986dpka@gmai.com
[3]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
Dhruw.neha0409@gmail.com
[4]Student 7th sem., Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
shikhamarkam199325@gmail.com
[5]Miss Rumi Ghosh, Assistant professor, Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001
rumighosh.8@gmail.com

Abstract:

Security is one of the most challenging aspects for information exchange in the World Wide Web. So this is an approach to find out the best solution for providing necessary protection to our data against malicious attacks from intruders.

Cryptography and Steganography are the two major techniques that are being used worldwide for enhancing the security of data in secret communication. Steganography is the method through which existence of the original message is kept secret from a third party. In steganography the original message is hidden into the cover medium. Cryptography converts information from its original form (plaintext) easily understood by anyone into an unreadable form (cipher text) that does not express or mean anything. In this paper we are using steganography to hide the message applied together with cryptography so that we can enhance the security of the data. We are using LSB algorithm for steganography along with IDEA algorithm for cryptography.

Keywords: Encryption, Decryption, LSB, IDEA, Steganography, Stego key, Stego image

1. Introduction

1.1 Steganography:

Steganography is the art and science of invisible communication in the sense that it does not specify anything whether any communication is taking place or not. This is accomplished by hiding information in any other form of information, thus hiding the existence of the original information to be transmitted [6]. Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means “cover writing”. Steganography means to conceal messages’ existence in another medium (audio, video, image, communication) [9]. Steganography is different from cryptography in the sense that cryptography focuses only on keeping the contents of a message secret, whereas steganography focuses on keeping the existence of a message secret. We have used image steganography in which the information is hidden exclusively in images. We are using LSB algorithm for image steganography.

Image steganography terminologies are as follows:-

• **Cover-Image:** Original image which is explicitly used as a carrier for hidden information to be transmitted.

• **Message:** Actual information which is used to hide into images. Message could be a plain text or some other image.

• **Stego-Image:** After embedding message into cover image what we get is known as stego-image.

• **Stego-Key:** A key that is used for embedding or extracting the messages from cover-images and stego-images.

1.2 Cryptography:

Cryptography may be defined as a study of methods or techniques that involve security of data to be transmitted across a network. Cryptography involves encoding and decoding of data to prevent it from any alteration, modification or just listening of data by a third party. Cryptography is one of the main techniques that is being used in computer security that converts information from its normal form into an unreadable form [4].

Encryption:

Encryption is the technique that converts any readable format into non-readable format. It takes any plain text and converts it into non-readable format with the use of any algorithm which may or may not use any key(or keys).

Decryption:

Decryption is just the inverse process of encryption. It converts non-readable format into readable form by taking the encrypted text known as cipher text as input and applying the decryption algorithm to it, giving us the original plain text.

Block Diagram:

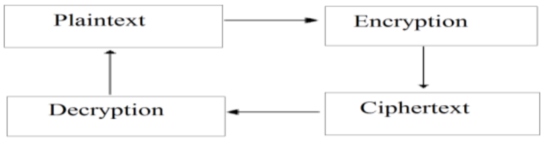

Fig 1: Conventional Encryption-Decryption Method

2. LITERATURE SURVEY

Champakamala .B.S et.al: on their paper state the Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. A new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique [2].

Dr. Rajkumar L Biradar & Ambika Umashetty have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications. It proposes different techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods [3].

Bibhudendra Acharya et.al: On their paper proposed a novel advanced Hill (AdvHill) encryption technique which uses an involutory key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background [4].

Mohammad Ali Bani Younes & Aman Jantan worked on a steganography method to embed information within an encrypted image data randomly. The approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Experimental results show that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image, and reduces the chance of the encrypted image being detected [5].

T. Morkel et.al, discussed on their paper that there exists a large selection of approaches to hiding information in images with different strong and weak points. Where one technique lacks in payload capacity, the other lacks in robustness. Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he wants to use the algorithm for and if he is willing to compromise on some features to ensure the security of others [6].

Shailender Gupta et.al: used two popular techniques Rivest, Shamir, Adleman (RSA) algorithm and Diffie Hellman algorithm to encrypt the data to show that the use of encryption in Steganalysis does not affect the time complexity if Diffie Hellman algorithm is used instead of RSA algorithm [7].

Jawahar Thakur & Nagesh Kumar on their paper provide a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm on the basis of these parameters: speed, block size, and key size [10].

3. Proposed Methodology

We have used LSB and IDEA algorithm both together for hiding and securing of data. At sender’s side we are first applying IDEA algorithm to the plaintext. Then after we get the cipher text, we are using LSB for hiding the encrypted data. In this way even if an attacker comes to know the existence of secret data he/she must first have to deal with the cover image then comes the encrypted data, Which obviously does not make any sense unless decrypted. So, the proposed technique helps in improving the data security, thus prevents the data from being attacked and tempered.

3.1 LSB Algorithm:

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [2]. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message [1]. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [7].

For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 100, which binary representation is 1100100, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 10101101 01100011)

For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images [8].

3.2 IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM)

The IDEA algorithm is interesting in its own right. At first it may appear that it is a non-invertible hash function instead of a block cipher. Also, it is interesting in that it entirely avoids the use of any lookup tables or S-boxes.

IDEA uses 52 subkeys, each 16bit long. Two are used during each round, and four are used before every round and after the last round. It has total eight rounds.

- IDEA is block cipher similar to DES.
- Takes 64 bit plain text block as input.
- Key is longer and consists of 128 bits.
- IDEA is reversible like DES i.e. same algorithm can be used for encryption as well as decryption.
- IDEA also uses diffusion as well as confusion techniques.

Broad steps in IDEA:

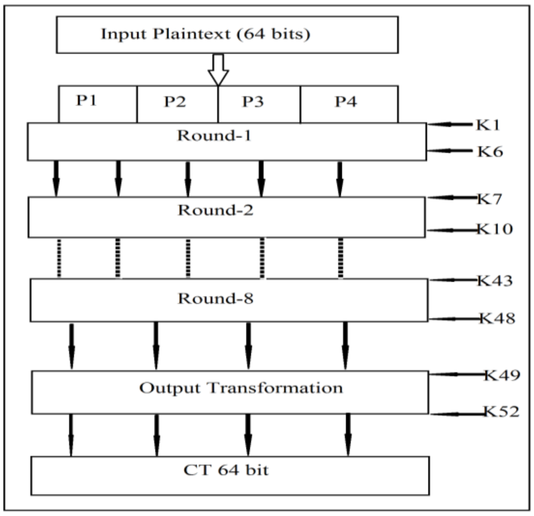

Fig 2: Broad level Steps in IDEA

WORKING:

- 64- bit of input PT block is divided into four parts (each of size 16 bit) say p1 to p4 and taken as input into first round.
- There are 8-such rounds and as we mentioned key consist of 128 bit.

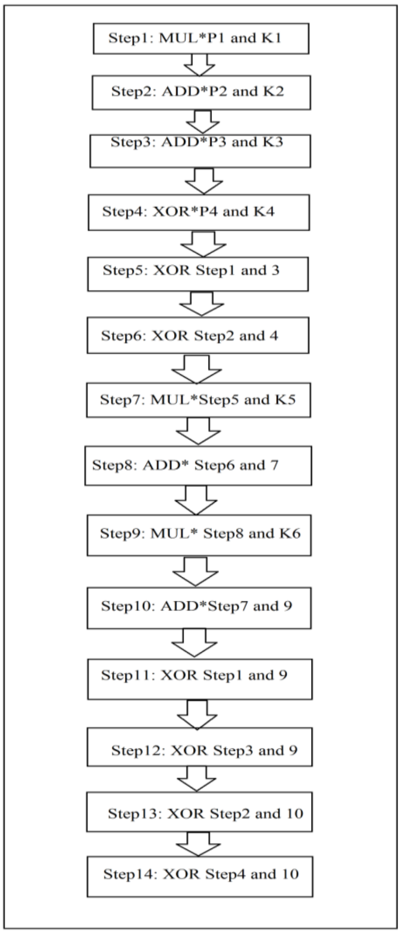

Fig 3: Details of One Round in IDEA

- First 8 subkeys are obtained from original 128 bit key. Then next 8 subkeys are derived by applying 25-bit circular left shift. In this way all 52 subkeys are first obtained.
- Each sub key consists of 16-bit and are applied on four input blocks from p1 to p4.
- Involved eight rounds consist of a series of operations on the 4 input blocks.
- Above specified broad steps perform lots of mathematical action in each step like Multiplication, Addition and XOR operations.
- ADD* MULTIPLY* are not mere addition and multiplication**,** instead they are addition modulo 2^{16} (Addition Modulo: 65536) and multiplication modulo $2^{16}+1$ (Multiplication Modulo: 65537).

DOI: 10.18535/ijecs/v5i12.59

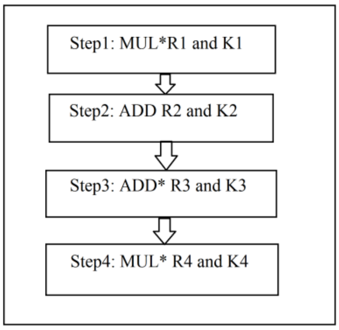

Fig 4: Details of Output Transform in IDEA

4. CONCLUSION

In this paper we have discussed the detailed study of LSB technique for Steganography applied along with Cryptography for better security of data in transit. In LSB the least significant bits of pixel values of the cover image are replaced with the secret data. We have used IDEA algorithm for encryption, a block cipher algorithm, of data before applying steganography. IDEA is a strong encryption algorithm used in commercials products such as PGP and some standards. Since LSB doesn't contain any information there is no loss of information and secret image recovering back become undistorted. This paper mentions an approach through which security of data is improved by using LSB technique and IDEA Algorithm together.

6. REFERENCES

1. "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique" by Kshetrimayum Jenita Devi Under Dr. Sanjay Kumar Jena (Professor) , Department of Computer Science and Engineering , National Institute Of Technology – Rourkela Odisha.

2. "Least Significant Bit Algorithm for Image Steganography" by Champakamala .B.S, Padmini .K, Radhika .D.K Asst Professors, Department of TCE, Don Bosco Institute of Technology, Bangalore, India.

3. Dr. Rajkumar L Biradar, Ambika Umashetty, "A Survey Paper on Steganography Techniques" , IJIRCCE vol. 4, Issue 1, January 2016.

4. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", Int. J. of Recent Trends in Engineering and Technology, Vol. 1, No. 1, Nov 2009.

5. Mohammad Ali Bani Younes and Aman Jantan , "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.

6. "AN OVERVIEW OF IMAGE STEGANOGRAPHY" by T. Morkel , J.H.P. Eloff , M.S. Olivier , Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

7. "Information Hiding Using Least Significant Bit Steganography and Cryptography" by Shailender Gupta, Ankur Goyal and Bharat Bhushan, Department of Electrical & Electronics Engineering, YMCAUST, Faridabad, India. I.J.Modern Education and Computer Science, 2012, 6, 27-34.

8. Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

9. Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. **(1996)**.

10. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", ISSN 2250-2459, Volume 1, Issue 2, December 2011