Security of Image Processing Over a Network

Sachin Shankar Bangar

Master of Computer Application

YMT College of Management

Kharghar, Navi Mumbai

Sachin11.bangar@gmail.com

---***---

Abstract-*Using image steganography security can be provided to any image which has to be sent over the network or transferred using any electronic mode. There is a message and an image that has to be sent. The image is divided into 'n' no of parts.The first step is process of converting the actual message into ciphertext using the Advanced Encryption Standard (AES) 256 bit algorithm. In the second Step is the cipher text is embedded into first part of the image. Third step is encryption performed on ench part of the image. These individual parts are combined and create single encrypted image. This final encrypted image is sent to the receiver. At the receivers end decryption of the encrypted image is performed. The first step is dividing the encrypted image into the 'n' no of parts. The second step is decryption performed on each part of the image. Thired step is taking the first part of the decrypted image and decrypt the embedded cipher text. Then marge or combine the all the decrypted parts and create the single output image.*

Key words:
Cryptography, Image steganography, Image security

1. INTRODUCTION

In today's world of growing technology security is of atmost concern. With the increase in cyber crime, providing only network security is not sufficient. Security provided to images like blue print of company projects, secret images of concern to the army or of company's interest, using image steganography is beneficial. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. This makes it difficult for the trespasers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly difficult for the intruder to detect and decode the document. There is no limitation on the image format that can be used right from bmp to a giff image can be used. It can be grey scale or coloured images. The size of the message needs to be of only 140 characters.

2. LITERATURE SURVEY

Current picture of the world says that everything that can be thought off can be done with the help of the internet. Right from shopping for clothes to buying a house. The transactions are all done using personal information, credit card numbers etc. With the amount of internet users hiking up day by day, everything that is transmitted over the internet is under threat by some malicious mischief of another person. In order to provide security to the data that is being send across the system network security is not enough. With the growing technology the hackers have also kept themselves updated with technology and ways to hack it.

In order to provide security the only way would be not letting the hackers know about the presence of important information in your transaction.

Many techniques have been developed to do the image security. Some of them are below listed:

A. Steganography
B. Water Marking Technique
C. Visual Cryptography
D. Without sharing Keys Techniques

2.1 Steganography

The steganography word comes from the Greek word Steganos, which is used to cover or secret and a graphy, is used for writing or drawing. Therefore, steganography is, literally, covered writing. The main idea for covering the information or steganography is used for secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [7]. During the transmission process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital videos, images, sound files, and other files of computer that contain perceptually important information can be used as "covers" or carriers to hide secret messages. After embedding a message into the cover-image, a so-called "stego image" is obtained.

In [6] Security, Capacity and robustness are three different aspects which are affecting steganography and its usefulness. Capacity is used to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper‘s inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information. The concept of the mosaic images [8] was created perfectly and it has been widely used. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in [6]. In the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics.

2.2Water Marking Technique

Water Marking is also one of the technique used to hide the digital image, Digital watermarking is a process of embedding (hiding) marks which are typically invisible and that can be extracted only by owner‘s of the authentication. This is the technology which is used [5] in with the image that cannot be misused by any other unauthorized miss users. This technology allows anyone to do without any distortion and keeping much better quality of stegno-image, also in a secured and reliable manner guaranteeing efficient and retrievals of secret file. Digital watermarking finds wide application in security, authentication, copyright protection and all walks of internet applications. There has been effective growth in developing techniques to discourage the unauthorized duplication of applications and data. The watermarking technique is one, which is feasible and design to protect the applications and data related. The term‘ cover‘ is used to describe the original message in which it will hide our secret message, data file or image file. Invisible watermarking and visible water-marking are the two important types of the above said technology. The main objective of this package is to reduce the unauthorized duplication of applications and data, provide copyright protections, security, and authentication, to all walks of internet applications [4].

2.3 Visual Cryptography

Visual Cryptography is used to hide information in images; a special encryption technique in such a way that encrypted image can be decrypted by the human eyes, if the correct key image is used [8]. The technique was proposed by Naor and Shamir in 1994. It is uses two transparent images. One image contains image contains the secret information and the other random pixels. It is not possible to get the secret information from any one of the images. Both layers and transparent images are required to get the actual information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet [1].

2.4 Without sharing Keys Techniques

The author [10] at is securing image for transmission without sharing his encrypted key, but it needs two transmission for a single image transmission, In [10] the image is encrypted with private key and is sent without sharing key to the receiver, after receiving the encrypted image receiver again encrypted the image by its own keys, and send it to the first sender, first sender removed the first encrypted key and again send to opponent, The opponent already had it‘s keys then with this key the image is finally decrypted. Thus different person applying different-different techniques for securing his information.

Applications of the proposed system are:

1. Banking
2. Consultancies
3. Detective agencies
4. Defence forces

3. EXISTING SYSTEMS

Various systems are available for information hiding in an image, but they have some drawbacks i.e., they either do not encrypt the message or use a very weak algorithm in order to perform cryptography. They use the same key for encryption and decryption making it easy for the intruder to get access of the information.In some other cases the technique used may not be very efficient that is, the original image and the resulting image will be easily distinguishable by naked human eyes. For example DES algorithm, an encryption algorithm, and used keys of smaller sizes (64 bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the image smooth and more realistic.

4. PROPOSED SYSTEM

The proposed system is divided into stpes for better understanding. Before going to any process on the image first we divide the image into using some command or algorithm we will divide the image in to J*J parts i.e.

(2*2, 4*4) parts. Each parts of the image will be treated as a single image.

Figure 1 Original Image

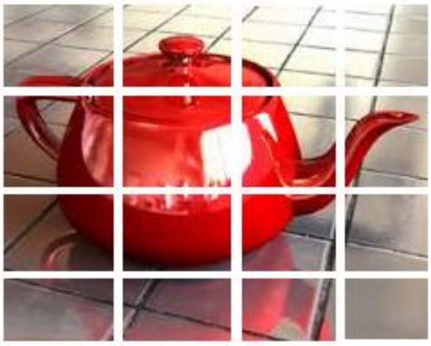

Figure 2 Splited Images (4 * 4)

4.1 Sender Side,

4.1.1 Step 1st -

The message which sent through image is encrypted using AES 256 bit algorithm. The steps involved in performing AES are as follows [2]

AES has three approved key length: 128 bits, 192 bits, and 256 bits. This algorithm starts with a random number, in which the key and data is encrypted, which are then scrambled though four rounds of mathematical processes. The key that is used to encrypt the message must also be used to decrypt it as shown in the figure 3

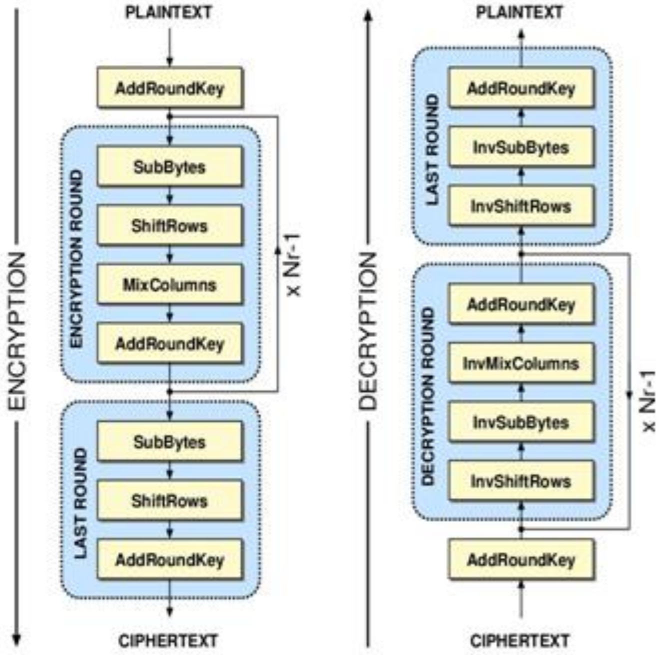

Figure 3 AES Algorithm [3]

High-level description of the algorithm [3]

- **KeyExpansions** - round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
- **InitialRound**
  1. AddRoundKey - each byte of the state is combined with a block of the round key using bitwise xor.
- **Rounds**
  1. SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
  2. ShiftRows - a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
  3. MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  4. AddRoundKey
- **Final Round (no MixColumns)**
  1. SubBytes
  2. ShiftRows
  3. AddRoundKey.

These algorithms essentially take basic data and change it into a ciphertext.

4.1.2 Step 2nd -

In this phase the encrypted message is embedded on to the first part of the image. Figure 4 shows the diagrammatic description.

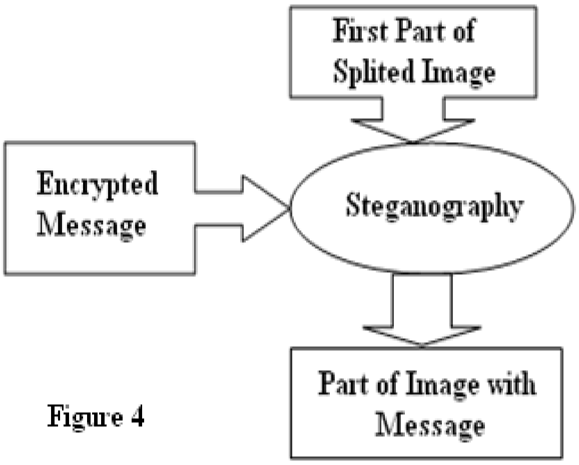

Figure 4

4.1.3 Step 3rd -

Using the Image encryption algorithm, we will encrypt each part of the image. Figure 5 shows the splited encrypted images. Also marge the all images and create one single image. Figure 6 shows the marged encrypted images. This marged encrypted file sends through the network tennel.

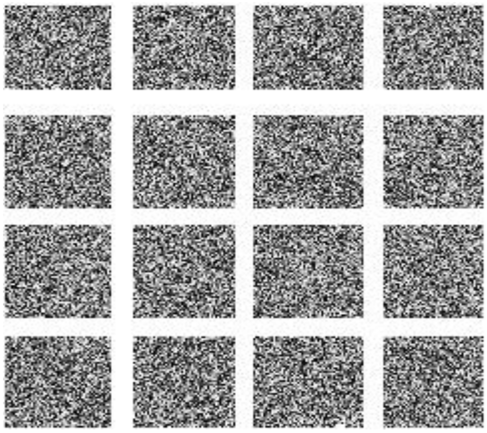

Figure 5 Splited Encrypted Images

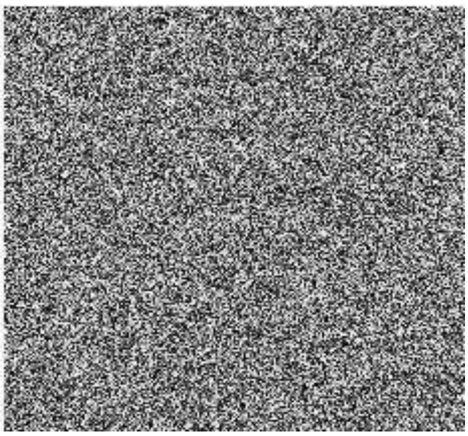

Figure 6 Marged Encrypted Images

4.2 Receiver Side,

4.2.1 Step 4th -

Here we will receive the encrypted image from source side. First we divide the encrypted image into the J*J parts using same command or algorithm which used for spliting the image before encryption. Each parts of the encrypted image will be treated as a single image which shows in figure 5.

4.2.2 Step 5th -

Decrypt the all the part of the encrypted image using the same image encryption algorithm which used to encrypt the image.

4.2.3 Step 6th -

Take the first part of the decryptd image and decrypt the cipher text using the AES 256 bit algorithm. Figure 7 shows the original image after decryption.

Figure 1 Original Image

5. CONCLUSIONS

This paper has presented for data and image encryption using AES 256 bit algorithm for cryptography, image steganography and image security.

As the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the intruder to get access of all the parts. Also intruder can not access the encrypted chiper text from part of the image.

Thus we have increased the security of an image for transmission over a network up to n times or we can increase 2n number of times instead of one in a single information transmission, more number of splitted blocks means more secure information.

REFERENCES

1. Visual Cryptography Moni Naor and Adi Shamir EUROCRYPT -1994
2. "Proposed System for data hiding using Cryptography and Steganography" -Dipti Kapoor Sarmah1,Neha Bajpai2,Department of Computer Engineering, Maharashtra Academy of Engineering,Pune,INDIA
3. Ahmad Salameh Abusukhon, "Block Cipher Encryption For Text-To-Image Algorithm" ,International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3,2013, pp. 50 - 59, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375
4. Battiato, G. M. farinella, and G. Gallo, Digital mosaic framework: An overview, Eurograph.– Computer Graph.Forum,Vol.26, no. 4, pp. 794 – 812, Dec.2007.
5. John Blesswin, Rema, Jenifer Josel 978-1-4244-9799-71111$26.00 ©20 11 IEEE, in Proc. Eurographics, Saarbrucken, Germany, Sep. 2002, pp. 341-348.
6. Silver and M. Hawley, "Photo mosaics". New York: Henry Holt, 1997.
7. E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.
8. Abdul Razzaque and Narendra Thakur International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181

BIBLOGRAPHY

1. 'AES 256 bit algorithm' - https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
2. 'Water Marking Technique' - https://engineering.purdue.edu/~ace/water2/sampleimages.html