Enhanced Security of Data using Image Steganography and AES Encryption Technique

Sandeep Panghal
Computer Science Department
IMS Engineering College
Ghaziabad, U.P, India

Sachin Kumar
Computer Science Department
IMS Engineering College
Ghaziabad, U.P, India

Naveen Kumar
Computer Science Department
IMS Engineering College
Ghaziabad, U.P, India

ABSTRACT

Today Security of data is of foremost importance in today's world. Security has become one of the most important factor in communication and information technology. For this purpose steganography is used. Steganography is the art of hiding secret or sensitive information into digital media like images so as to have secure communication. In this paper we present and discuss LSB (Least Significant Bit) based image steganography and AES encryption algorithm so as to provide an extra layer of security.

Keywords

LSB, Steganography, AES, DES, Encryption

1. INTRODUCTION

Steganography is the art of hiding secret or sensitive information into digital media like images so as to have secure communication [3]. In steganography we hide our secret information in some cover image such that one cannot track the message. The original Image is called cover image and the image in which message is embedded is called Stego Image [7]. Steganography can also be done with Text, video, audio and protocol steganography.

There is a difference between cryptography and steganography. Cryptography helps us to keep message content in secret form while steganography helps to keep the existence of the message as a secret. If cryptography is forbidden to use then in that case steganography is very useful.

Today there are many applications of steganography. It is used in defense organizations so that data can be safely circulated, it is used in smart identity cards where the information of the person is secretly stored in the image of the person itself. Some other applications are medical imaging, online voting system Etc.

COVER IMAGE: This image is used to hold the secret information.

STEGO IMAGE: Image holding the embedded message.

SECRET MESSAGE: This is the secret information which is to be embedded with the cover image.

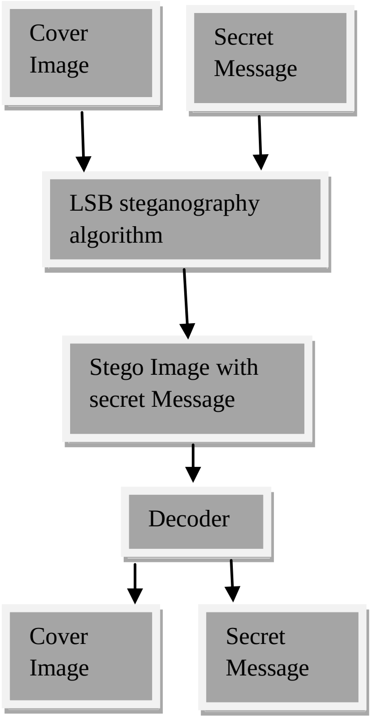


Fig. 1: LSB Image steganography Process [7].

The LSB is the least significant bit in the pixel value of the image. It works by replacing the least significant bit of some randomly selected pixels in the cover image.

2. LITERATURE REVIEW

Bin li,Junhui he et. Al discusses the main aspects of information hiding are steganography and steganalysis. Steganography is the art of hiding secret or sensitive information into digital media like images so as to have secure communication. Steganalysis is the art of detecting the presence of steganography. This paper discusses the fundamental concepts of steganography, the progress of methods of steganography for images in spatial representation. The summarization of methods of steganography is discussed. [3].

Security of data has become foremost concern now. *Satwinder and Varinder Kaur* proposes a Dual Security model for hiding Sensitive information with the help of LSB based steganography and AES encryption Technique. The proposed model is to hide the sensitive information behind some cover image using LSB based Steganography and then encrypt the image using AES algorithm [7].

Kanika Anand and Er.Rekha Sharma compares the LSB and MSB based steganography with one another according to the MSE (Mean square error) and PSNR (Peak signal to noise ratio) values. LSB works by replacing the least significant bit of the pixel value of the cover image (in most of the cases 8th bit is replaced). In MSB most significant bit of the pixel value is changed in the cover image. Techniques are discussed in detail in this paper. In this paper the results show that LSB Based Steganography is better than MSB based steganography on the basis of MSE and PSNR values [5].

Mr . Vikas Tyagi, Mr. Atul kumar discusses the LSB based steganography and a new encryption algorithm. The proposed model is to first convert the data into encrypted form using the proposed encryption algorithm and then patch the data in the cover image using LSB based Steganography. Steganography can also be done with Text, video, audio and protocol steganography [6].

Douglas selent discusses the detailed concept of AES in this paper. AES is a standard used for encryption of data. AES is a symmetric-key algorithm which means that same key is used for both decryption and encryption of data. AES is block cipher which uses block sizes of 128, 168, 192, 224 and 256 bits. The paper also discusses about announcing of AES and some drawbacks of triple DES (3DES) and DES. AES uses Exclusive –OR operation and substitution and permutation operations, rows and column shifting [1].

Today cryptography plays an important role in security of the information systems. *Ritu pahal* in this paper efficiently implements AES. AES is implemented for 200 bit using 5*5 state matrix and AES 128 bit is also implemented for 200 bit using 5*5 state matrix .The proposed work is then compared with the 128 ,192, 256 bit AES. Only the mix column transformation is changed in this process. The results show that the proposed algorithm is 50% slower from AES-128, 40% from AES-192, and 25% from AES-256 [4].

3. LSB BASED STEGANOGRAPHY

LSB works by replacing the least significant bit of the Pixel value of the cover image (in most of the cases 8th bit is replaced).

Example: Consider a 3- pixel grid in a 24- bit image:

00110011 01100011 01101111

01101110 01101100 00110100

01101101 01100101 01101011

Suppose we want to hide a character ‘y’ in the image.

The ASCII code of ‘y’ is 121 whose binary value is 01111001.

Now pixels after embedding the message in the image are as shown [3]:

0011001**0** 01100011 01101111

0110111**1** 0110110**1** 00110100

0110110**0** 01100101 01101011

8 bits were to be embedded in the image however only 4 bits were changed. Thus on an average only half of the bits are changed in the embedding process. In LSB process we use BMP (bitmap) images because they are lossless compression images. In lossless compression size of file is reduced but it does not affect the quality of file. The original data in the file is restored when the file is uncompressed [7].

The pseudo code for LSB is given by:

Embedding the text inside the image:

1. Calculate the Pixels of the image.
2. Make a loop through the pixels.
3. In each pass get the red, green and blue value of pixels.
4. Make the LSB of each RGB pixel to zero.
5. Get the character to be hidden in binary form and hide the 8-bit binary code in the lsb of pixels.
6. Repeat the process until all the characters of the image are hidden inside the image.

Extracting the embed message from the image:

1. Calculate the pixels of the image.
2. Loop through the pixels of the Image until one find the 8 consecutive zero.
3. Pick LSB from each pixel element and then convert it into the character.

In LSB when we flip the value of the LSB the value is only affected by 1 [6].

3.1 Comparison with MSB (Most significant Bit)

In MSB most significant bit of the pixel value is changed in the cover image. Thus the change In MSB is 1*27 i.e. the value is affected by 128 which is a significant effect on the image.

4. ADVANCED ENCRYPTION STANDARD

AES was introduced to replace DES in commercial applications. Advanced Encryption Standard was announced by National Institute of Standards and Technology (NIST) on November 26, 2001 [2]. AES is a symmetric-key algorithm which means that same key is used for both decryption and encryption of data.

AES is also called RIJNDAEL which was named after the name of its inventors John Daemen and Vincent Rijmen. AES is block cipher which uses block sizes of 128, 168, 192, 224 and 256 bits [1]. The key sizes used in AES are 128,192 and 256 bits. There are some differences between AES and DES. DES uses a feistel structure in which the block is divided into two halves before it goes through the steps of encryption whereas in DES , each round consist of a series of functions which are byte substitution, permutation, arithmetic operator over a finite field and X-OR operation with key. AES is faster than 3DES and DES. The basic structure of AES is shown below [7].

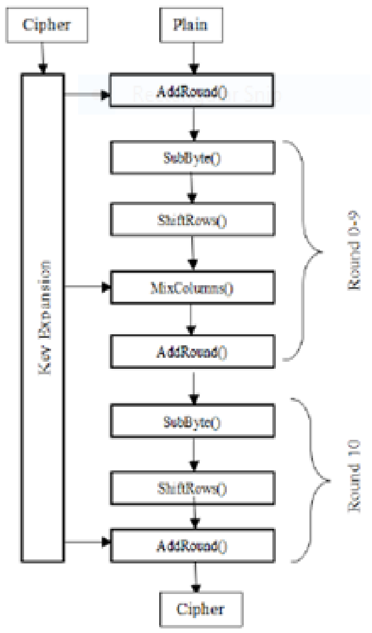
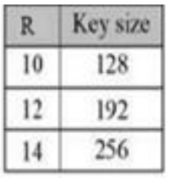


Fig 2: [7] Basic Structure of 128 bit AES algorithm

Unlike DES the number of rounds in AES depends on the length of the Key used and thus the number of rounds are variable. 10 rounds are used for 128 bit key, 12 rounds for 192 bit key and 14 rounds for 256 bit key are used. Each of the rounds uses a different 128 bit key which is calculated from the original key.



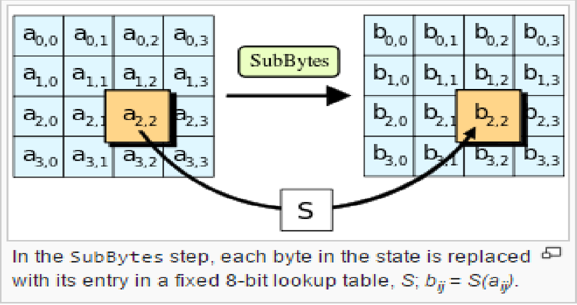
R	Key size
10	128
12	192
14	256

Fig 3: Relationship between No. of Rounds (R) and Cipher Key Size.

Encryption Process

First of all, we take our data and copy the data into the 4x4 Matrix. This is called **state matrix**. In the initial round each byte of the state matrix is X-OR with each byte of the corresponding key for first round. Each round comprise of four sub processes:-

SubByte( ) – We put each byte into a S-Box (Substitution box) which maps the byte into a different byte. The result is a output matrix with four columns and four rows [2].

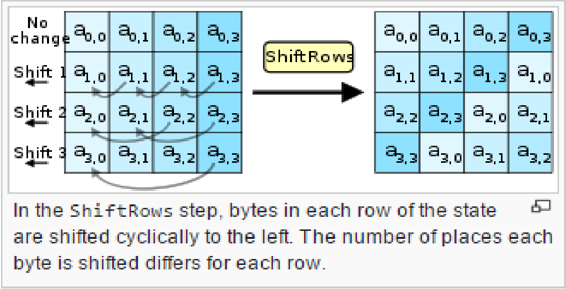

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

Fig 4: [8] Substitution round in AES.

ShiftRows( ) – In this step we shift the rows to the left.

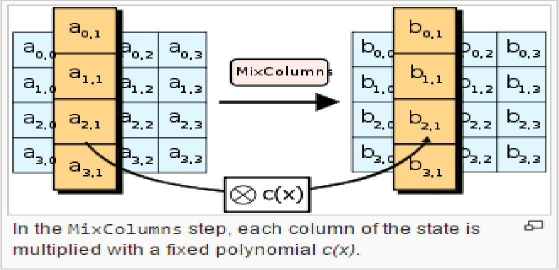
First row is not shifted. Second, third and fourth row are shifted by one byte, two byte and three byte respectively. Rows are wrapped to the other side [4].


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

Fig 5: [8] Shift Rows round in AES

MixColumns() - Each column of 4 bytes is transformed using the special mathematical function. The input to the function is the four bytes of one column and output is the four new bytes which replaces the four input bytes [4].


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\otimes c(x)$

In the MixColumns step, each column of the state is multiplied with a fixed polynomial $c(x)$.

Fig 6: [8] Column Mixing Round in AES.

AddRoundkey(): At the end of each round, the next round key is applied with an X-OR. In the final round we skip the Mix columns step since it slows down the process.

The process of decryption is the inverse of encryption process.

Today AES is used because DES was inherently weak.56- bit key is used in DES which means there are 2^{56} combination which is easy to crack in case of Brute Force attack. Alternatives to DES like TripleDES (3DES) are available but 3DES is very slow.

Table 1. Comparison between AES and DES

PARAMETERS	AES	DES
Developed in Year	2000	1977
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher
Key Length	128,192,256 bit key	56 bit key
Possible keys combination	2^{128},2^{192},2^{256}	2^{56}
Block size	128,192 or 256 bit key	64 bit
Security	Secure	Not Secure, inadequate

5. FUTURE WORK

The proposed work in this paper uses a steganography technique called image steganography. The data is embedded into the stego image. The main purpose of the project is to provide security. The cover media helps to embed the data. In future we can use different carriers and different keys for encryption and decryption of data which will provide greater security. We can also embed the audio in the carrier media.

6. CONCLUSION

In this paper we presented LSB based Image Steganography. LSB based image Steganography is a good method of embedding sensitive information behind some cover media. LSB based steganography in combination with AES will provide a good security model for hiding data. AES is preferred over DES due to its simplicity and its speed.

7. ACKNOWLEDGMENTS

We are grateful to our Department of **Computer Science & Technology** for their support and providing us an opportunity to review on such an interesting topic. While reading and searching about this topic we learnt about various important and interesting facts.

8. REFERENCES

[1] "Advanced Encryption Standard", Douglas Selent, Rivier Academic Journal, Volume 6, Number 2, Fall 2010.

[2] "Announcing The Advanced Encryption Standard (Aes)" Federal Information Processing Standards Publication 197. US NIST. November 26, 2001. Retrieved October 2, 2012.

[3] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi. A survey on Image steganography and steganalysis, Volume 2, Number 2, April 2011.

[4] "Efficient Implementation of AES", Ritu Pahal, Vikas Kumar, Volume 3, Issue 7, July 2013 ISSN: 2277 128X IJARCSSE.

[5] Kanika Anand, Er. Rekha Sharma, Comparison of LSB and MSB Based Image Steganography, Ijarssce, Volume 4, Issue 8, August 2014.

[6] Mr . Vikas Tyagi, Mr. Atul kumar, Image Steganography Using Least Significant Bit With Cryptography, Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012.

[7] Satwinder Singh and Varinder Kaur Attri .Dual Layer Security of data using LSB Image Steganography Method and AES Encryption , ISSN: 2231-2307, Volume-2, Issue-3, July 2015.

[8] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[9] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1(1), 70-75.

[10] Al-Ataby, A., & Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transform. changes, 4, 6