High Security of Data Using Steganography with Hybrid Algorithm

Madhugeeta Verma[1], **Poonam Dhamal**[2]

[1]Savitribai Phule pune University, GH Raisoni College of Engineering and Management, Pune, India

[2]GH Raisoni college of Engineering and Management , Savitribai Phule pune University, Pune, India

Abstract: ***With the modern technology in communication, there need some security on computer network. This security is one of the significant problem in tha data communication. Steganography is the art of hiding the message such that its presence cannot be detected. Message or encrypted message is hidden in the other carrier object before passing it through the network. In the existing system, for hiding the data only one technique is used i.e. steganography with X-box. In this paper, we will use 4 X-box technique which will hide 3 secret bit in each pixel of 24 or 32 bit cover image with hybrid algorithm i.e. AES and SHA-512. This will improve the security and PSNR value.***

Keywords: Steganography; 2 X-Box technique; LSB; network security; AES; SHA-512;

1. Introduction

Steganography word is originated from Greek words steganos (covered) and Graphy (writing) which literally means cover writing[1]. It does not alter the message but hide it in another cover object like text, image, audio, video and network. It is the advance version of cryptography where messages are only scrambled so that it could not be understood by unauthorized person.

Steganography is different from watermarking. Watermarking is used to verify the identity and authenticity of the owner of a digital image[3]. The information are embedded into the digital image or signals. For example if a famous celebrity watermark his picture then if somebody want to copy that picture then that watermark is also copied. This watermarking can be visible as well as invisible. It is used for copyright protection,source tracing, etc, where as steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy.

Information hiding using steganography

Now days, security of information has become a fundamental issue. Steganography is a technique of hiding information in digital media. It is a Greek word, stego means “covered” and graphia means “writing” i.e. covered writing. It embed the message in digital media before passing it to network, so its existence become invisible. This confidentiality and data integrity are required to protect against the unauthorized access. Some terminologies of steganography are [1]

Cover-Image: The image which is used as a carrier for hidden message.

- **Message**: Actual information which is used to hide into images. Message could be a plain text,cipher text, image, etc.
- **Stego-Image**: After embedding message into cover image is known as stego-image.
- **Stego-Key**: A key is used for embedding or extracting the messages from cover-images and stego-images.

Steganographic measures are

- **High Capacity**: Maximum size of data that can be embedded.
- **Perceptual Transparency**: Quality of image that degrades.
- **Robustness**: After embedding, data should not be changed if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- **Temper Resistance**: Alteration of message after embedding.
- **Computation Complexity**: Total expense for embedding and extraction of message

Image steganography can be divided into 2 domain: Spatial and Transform domain. A picture in the spatial domain can be described as a collection of pixel values. Transform domain is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [6].

2. Literature Survey

The early instance of steganography is mentioned in Herodotos’s Histories[2] which clearly shows that the message are not encrypted but only hidden inside other object.

Background

Shaving a slave’s head: First, In this, the head of the slave had been shaved and then tattooed which was a kind of message. Then they wait for the hair to grow back. Once this happened, slave go to the recipient where his head is again shaved and finally recipient received their messages.

Modifying ancient tablets: Here the old wooden writing tablets were used to hide the messages. Sender write the message on the wood tablet which was covered by wax. So during the transit, no one understood that ther is any message.

Invisible ink: During the world war II, invisible ink were used to write the messages which was normally invisible but got visible when they got warmed.

In [4], Author has used a technique based on LSB for image steganography using x-box mapping. Author has used four X-Box which are responsible for embedding secret data. It give a high security without knowing the mapping rule no one can extract the message. X-boxes are 2*2 matrix where 0-15 values are stored. Firstly cipher image is converted into binary value. Then there is division of binary value into 4 parts of 2 bit each(b1, b2, b3, b4). Now get the new mapping values of b1, b2, b3 and b4 from the x-box and lastly those mapped values are stored in the 4 least significant bit of cover image. So finally we will get the stegoimage.

In [7], Namrata S. Malge1, Alaknanda S. Patil have used 2 X-box rather then 4 x-box. This enhances the security of secret message.

In [8], author has encrypted the secret data using AES (Advance Encryption Standard) and embed it in skin region of image. Skin tone detection is performed on input image using HSV (Hue, saturation, value) color space.Also embedding is performed using frequency domain approach-DWT (Discrete Wavelet Transform). DWT applies on entire image. DWT splits component into numerous frequency bands called subbands known as: LL – Horizontally and vertically low pass;LH – Horizontally low pass and vertically high pass; HL - Horizontally high pass and vertically low pass; HH - Horizontally and vertically high pass. Secret data is hidden in one of the high frequency sub-band of DWT by tracing the skin pixel in that sub-band. The skin detection algorithm will produce a black and white image. The value of black pixel is 0 and white pixel is 1 which can be considered as skin.

In [9], author has first encrypted the message using DES, AES and RSA along with steganographic algorithm. Then using the decryption algorithm, the receiver can extract the message. And lastly their performance have been compared. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. Also RSA consume more encryption time and buffer . It is observed that decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

In [10], author has used 2 different data hiding technique that is cryptography and steganography. In this process, first message is encrypted with transposing cipher method and then the encrypted message is embedded inside the image using LSB insertion method. The combination of 2 will enhance the security.

Example of LSB Technique

In the image steganography, LSB is the most common and simple technique. In this the least significant bit of some or all of the bytes of cover image is converted into bit of secret image[4]. For example a grid of 3 pixel of a 24 bit image

00100100 01111000 11001011
10101101 01110011 10111001
00111100 01101001 00011011

When the number 128 whose binary value is 10000000 is embedded into least significant bits of cover image, then the result will be

0010010**1** 01111000 1100101**0**
1010110**0** 0111001**0** 1011100**0**
00111100 0110100**0** 00011011

Only 8 byte of the grid have been used and 6 underlined bits needed to be changed. Since there are 256 possible intensities of colour, so if we change some least significant bit, then there will be only small change which can't be detected by human eyes. But there is a drawback, if we use consecutive bytes of image then it will be easy to retrieve it. So a more secure way is to use a key which will specify which pixel is having the secret data.

3. Existing System

This paper gives an approach for Image Steganography to increase the level of security for data transfer over the internet. Here a 24-bit RGB image is chosen as a cover image which hides the secret message inside red, green and blue color pixel values. Four X-Box have been used which contains sixteen different values (0-15). The values stored in the X-Boxes are mapped with the LSBs of the cover image. This mapping provides security to the secret message which makes it difficult for the intruders to extract the hidden information. A Peak Signal-to-Noise Ratio is calculated which measure the quality of images used. Larger PSNR value means lower distortion and hence a good quality of image.. The future work includes the improvement to the method in terms of complexity and selecting the pixel values[12].

4. Proposed System

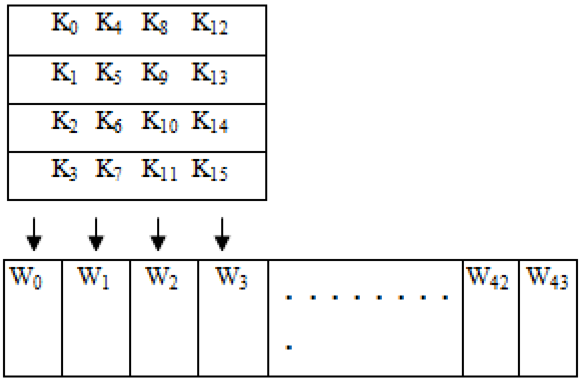
In the proposed system, first there is encryption of secret message using AES (Advance Encryption Standard) algorithm. This algorithm is used because it consumes least encryption and decryption time and buffer usage compared to DES and RSA[9]. Now we have encrypted message. At the same time we will also produce message digest or hash value of original message using SHA-512 algorithm which is send along with stego-image.

AES (Advance Encrytion Standard)

AES is based on 128 bit blocks with 128 bit keys. Since 128 bits gives a key range of 2^{128} . The input to the algorithm are the key and the plain text. Encryption consists of 10 rounds of processing for 128-bit keys[11]. Each round of processing consist of one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption. Now 128-bit block is converted into 4 × 4 matrix of bytes.

Byte0	Byte4	Byte8	Byte12
Byte1	Byte5	Byte9	Byte13
Byte2	Byte6	Byte10	Byte14
Byte3	Byte7	Byte11	Byte15

First four byte will occupy first column, second four byte will occupy second column and so on. The 4×4 matrix of bytes is referred to as the state array in AES. AES also use the term word. A word consists of four bytes, that is 32 bits. Therefore, each column of the state array is a word. Each round of processing works on the input state array and produces an output state array. since, same steps are used in encryption and decryption but the order in which the steps are carried out is different. Now the four column words of the key matrix are expanded into a schedule of 44 words.



K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

Before any round-based processing for, the input state array is XORed with the first four words of the key schedule. During decryption, we XOR the ciphertext state array with the last four words of the key schedule. For encryption, each round consists of four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The last step consists of XORing the output of the previous three steps with four words from the key schedule. For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. The third step consists of XORing the output of the previous two steps with four words from the key schedule.

SHA-512 (Secure Hash Algorithm)

The SHA-512 algorithm takes a message of length 2^{128} bits and produces a message digest of size 512 bits The input is divided into blocks of size 1024 bits each.

How SHA-512 works:

Step1. Padding: First step is to add padding to the end of original message such that length of the message become 128 bit less than the exact multiple of 1024.

Step2. Append Length: The length of the message excluding the length of the padding is now calculated and appended to the end of the padding as a 128 bit block. Hence the length of the message is exactly a multiple of 1024 bits.

Step3. Divide the input into 1024- bit blocks: The input message is now divided into block, each of length 1024 bit. These block becomes the input to the message digest processing logic.

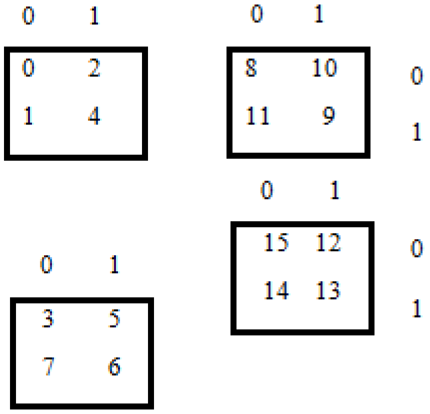
Step4. Initialize chaining variables: Now eight chaining variable a through h are initialized.

Step5. Process blocks: Now the actual algorithm begins.

a) Copy the chaining variable A-H into variable a-h. The combination of a-h, called as abcdefgh will be considered as asingle register for storing temporary intermediate as well as the final results.
b) Now, divide the current 1024-bit block into 16 sub-blocks, each consisting of 64 bits.
c) SHA-512 has 80 rounds. Each round takes the current 1024-bit block, the register abcdefgh and a constant K[t] (where t=0 to 79) as the 3 inputs. It then update the contents of the register abcdefgh using the SHA-512 algorithm steps.

These process makes the message Digest more complex and difficult to break. Now the next part is to hide encrypted message in cover image before sending to the network. For this following steps are as follows:-

Hiding of the image



1. Generation of the X-Box

In the proposed system 4 X-boxes have been used same as in existing system. These X-Boxes are of 2*2 matrix which will store value from 0-15. Value from 0-15 can be stored in any of the X-Box.

2 Division of bits

Suppose we want to embed $(11000101)_2$ in the cover image. So first we will divide the bits into 4 parts of 2 bit each.

11	00	01	01
B1	B2	B3	B4

We will map the value of B1, B2, B3 and B4 from X-Box. Value of B1 is 4. Value of B2 is 3. Value of B3 is 10. Value of B4 is 12.

3 Insertion of mapped value into the cover image

In case of 24 bit color image, each pixel consist of RGV value and each of these color use 8 bit. The intensity of these color is different. Suppose intensity of red, green and blue is 220, 198 and 135 respectively.

So RGB first pixel can be represented as [11011100 11000110 10000111]
Since value of B1, B2, B3 and B4 are 4, 3, 10, 12 respectively. So now first we will hide B1, then B2, then B3 and at last B4.

B1 = 4 →0100

The LSB of red, green and blue of first pixel will get replaced by B1.

Red

1	1	0	1	1	1	0	0

In this there is no need to replace LSB because it is already 0 which is same as first bit of B1.

Green

Replace by 1

1	1	0	0	0	1	1	0

⇩ New value is 199

1	1	0	0	0	1	1	1

Blue

Replace by 0

1	0	0	0	0	1	1	1

⇩ New value is 134

1	0	0	0	0	1	1	0

Similarly we will take LSB of red, green and blue of second pixel. Intensity of RGB of second pixel are 210, 150 and 115 respectively.

Red

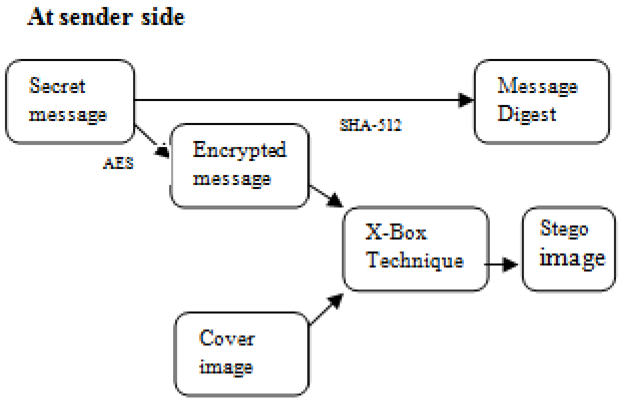
1	1	0	1	0	0	1	0

Here also no need to replace LSB because it is already 0 which is same as fourth bit of B1.

So B1 is embedded in the cover image. Similarly we will embed B2, B3 and B4. The process will continue until all messages get embedded. Finally Stego image will get formed.

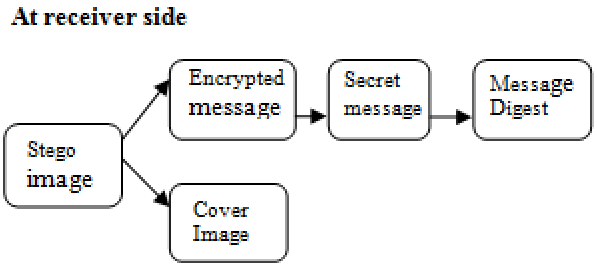
Embedding Algorithm
Input: A text message and a cover image
Output: Stego image
Steps:

1) Encrypt secret message with AES algorithm.
2) Create message digest of secret message.
3) Convert encrypted secret message into binary sequence.
4) Divide 8 bit secret message into 4 parts(B1, B2, B3 and b4) of 2 bit each.
5) Map the value of different parts from X-Box.
6) Insert new values into the LSB of RGB of cover image.
7) Stego image is formed.



Retrieval Algorithm
Input: Stego-image
Output: Secret message
Steps:

1) Convert stego-image into binary format.
2) Now extract LSB of RGB from pixels.
3) Cascade all LSBs in order to get encrypted secret message.
4) Decrypt the encrypted message in order to get original secret message.
5) Create message digest of original message.
6) Compare the message digest which sender has send and the message digest which receiver has created.
7) If both message digest is same, it means there is no modification in secret messa.ge and if it is not same means there is some change.



5. Conclusion

In this paper, we propose a mapping based steganography process with X-Box , AES algorithm for encryption and decryption and SHA-512 for generating message digest. Our approach is better because this will provide triple security. First we encrypt the message, second we hide it in cover image. If anyhow message gets modified, then we will find it by comparing message digests. So this is third security.

References

[1] Mehdi Hussain and Mureed Hussain, “A survey of image steganography techniques,” vol. 54, May 2013.
[2] http://bit599.netai.net/stego_background.htm
[3] Hardikkumar V. Desai, “Steganography, Cryptography, Watermarking: A Comparative Study, Volume 3, No. 12, December 2012.
[4] Mr.Jagadeesha.D.H, Mrs.Manjula.Y, Dr.M.Z.Kurian, “FPGA implementation of X-box mapping for an image steganography technique,” Vol. 2, Issue 6, June 2013.
[5] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, “New

Comparative Study Between DES, 3DES and AES within Nine Factors", journal of computing, volume 2, issue 3, march 2010, issn 2151-9617

[6] N.F. Johnson and S. Katzenbeisser, "A survey of steganographic technique in information hiding technique for steganography in Digital watermarking, Ed. London:Artrch House, (2000), pp. 43-78

[7] Namrata S. Malge1, Alaknanda S. Patil,"*Secure Steganography Approach using 2 Xbox Mapping Technique***",** Vol. 4, Issue 3, March 2015

[8] Manoj gowtham.G.V, Senthur.T, Sivasankaran.M, Vikram.M, "*AES BASED STEGANOGRAPHY*", Volume 2, Issue 1, January 2013

[9] B. Padmavathi, S. Ranjitha Kumari**, "**A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", **Volume 2 Issue 4, April 2013**

[10] Shamim Ahmed Laskar1 and Kattamanchi Hemachandran, "*High Capacity data hiding using LSB Steganography and Encryption*", Vol.4, No.6, December 2012

[11] Avi Kak, "AES: The Advanced Encryption Standard", May 1, 2015; Purdue University

[12] Ekta Dagar, Sunny Dagar, "LSB Based Image steganography using X-Box Mapping, 2014 IEEE