Survey on Image Steganography Techniques

Nishant Pattani[1], Kishan Patel [2], Nirmal Patel[3], Kashyap Pandya[4] and Amruta Patel[5]

[1]Nishant Pattani (Student of M.sc.(IT)), Department of Computer Science & Technology,Uka Tarsadia University, Bardoli,Gujarat,India
[1]pattani.nishant@gmail.com
[2]Kishan Patel (Student of M.sc.(IT)), Department of Computer Science & Technology,Uka Tarsadia University, Bardoli,Gujarat,India
[2]mscit.kp031@gmail.com
[3]Kashyap Pandya (Student of M.sc.(IT)), Department of Computer Science & Technology,Uka Tarsadia University, Bardoli,Gujarat,India
[3]kashyappandya55@gmail.com
[4]Nirmal Patel (Student of M.sc.(IT)), Department of Computer Science & Technology,Uka Tarsadia University, Bardoli,Gujarat,India
[4]nirmalpatel3679@gmail.com
[5]Amruta Patel (Student of M.sc.(IT)), Department of Computer Science & Technology,Uka Tarsadia University, Bardoli,Gujarat,India
[5]amrutapatelmscit@gmail.com

ABSTRACT

Image Steganography is very useful technique in Information Security Domain. Image Steganography is used to hiding data inside image. In this study we analyze how image steganography is done and where it is used. This is very useful technique when we transmit very sensitive information. There is also comparison of different steganography methods and overview of it. We have found some problems of using Image Steganography with Encryption algorithms.

Keywords — LSB, TTIE, HIEA, PSNR.

1. INTRODUCTION

Now a days Information security becomes most important factor in everywhere. Image steganography refers to hiding data inside image. In Image Steganography data is stored inside image in such a way that data is not visible to any other person without processing image.

Advantage of Image Steganography instead of using simply encrypted text is that message is hidden inside image and quality of image is not so much affected. So Quality of image is not so much affected so chances of attacks possible on secret message become less.

Image Steganography is mostly used in modern printers. HP and Xerox brand laser printers uses Image Steganography. This printer adds tiny yellow dots to each page. The dots are not easily visible and contain encoded printer serial numbers as well as date and time stamps.

Russian foreign intelligence service uses custom image steganography software for hiding encrypted information inside images for communication with “illegal agents”.

Image Steganography adds extra layer to security of information by hiding encrypted secret message in image and not affecting quality of image.

2. RELATED WORK

2.1. Literature Review

In Information Security Data is first encrypted using a key and after that data is send over network. So that without knowing

key attacker is unable to do with data is that is encrypted and transmitted over network.

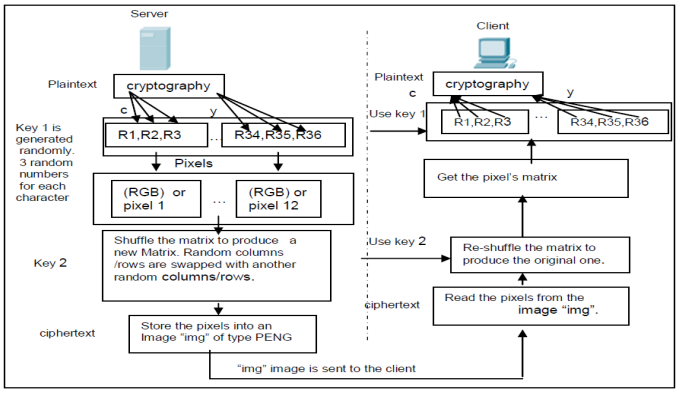

Figure 1 Text-to-Image-Encryption (TTIE) algorithm [6]

In Figure 1 First plaintext is translated to encrypted text and after key 2 is used to shuffle the matrix to generate new matrix for image. After shuffling matrix that matrix is stored in image of type png.

At the receiver side first step is to read pixel from image. After reading pixel from image, matrix is again is re-shuffled to generate original one. Now key 1 is used to get plaintext from cipher text.

In [2] paper Steganography algorithm, secret key, image processing, data retrieval is used. With this algorithm, plain text is converted into text file and compressed and compressed file is converted into binary form and binary form of message is hidden in last two bit of each pixel. Stego images are tested using PSNR value. If PSNR of stego image is High than stego image has more quality.

In [2] paper new system called Steganography Imaging System (SIS) is developed. Using SIS some experiments are done on the images of type bmp to check how much distortion is there in proposed algorithm.

Based on PSNR value evaluation of this algorithm is done. And formula for Peak Signal to Noise Ratio is as follows:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

Figure 2: PSNR Formula [2]

Where MSE is as follows:

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - S(x,y))^2$$

Figure 3: Formula of MSE [2]

Where S is stego image, C is Cover image, MN is size of image and (x, y) is pixel value of image.

In [7] Enhanced least significant bit method information is stored inside image but only in blue component part of each pixel to decrease distortion of image while storing of information inside image so that imperceptibility of Enhanced LSB will be low compared to simple LSB.

First information is translated into encrypted information using cryptography. In cryptography algorithm key and plain text message is translated into array of length of ascii character. After that text message is appended according to length of key. Then encrypted information is hidden inside image using pixel processing.

In [8] the Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the text messages is decided based on hash function. Hash function finds the position of least significant bit of each RGB pixel's .Then the Hash LSB technique uses the values provided by hash function to hide the data.

In [10] Genetic Algorithm in this technique, it will translate text message into binary type. Then that binary message is encrypted. After that it will convert encrypted message in numeric form. After that it will divide this numeric form by single digits. And it will get deviser, dividend, quotient and reminder. These will be treated as individual file. Now multiple images are as cover to hide these files. It also calculates LSB (Least Significant Bit) of each pixels of each image. This LSB is replaced by the bit of encrypted message one by one.

In [11] K-Matrix is used for encryption by mapping text's bits with the numbers stored in the matrix. In K-Matrix, Four 2 X 2 matrices are being used. Every cell of this K-MATRIX is assigned a random number ranging between 1 to 16. Convert the message ASCII value into binary form. Make the two digit pairs of obtained data starting from left. Mapping of these pairs is done with the number assigned in the corresponding cell of K-MATRIX to obtain another number. New corresponding number will be again converted in binary form.

Now the obtained Bits are being stored behind the LSB of RGB components of pixel of an image.

In [6] paper new permutation technique is introduced based on the combination of image permutation and new encryption algorithm called Hyper Image Encryption Algorithm. In this paper image is converted into permuted image and then converted image is converted using hyper image encryption algorithm.

In [12] paper survey of all steganography techniques, type of attacks that are possible on steganography and application of steganography is written. There are some different types of steganography and different techniques of audio, image and video in spatial and transform domains.

There are image steganography techniques and overview of each technique is explained. And there are some parameters on which we can measure each technique namely imperceptibility, robustness and payload capacity.

We have done literature review of image steganography and we analyze that least significant bit method is better among of all methods.

3. METHODS AND ALGORITHMS

3.1. Methods

1. Least significant bit method(LSB):

   In LSB information is hidden at last bit of each pixel of image so that information is hided and quality of image is not so much affected.

2. Spatial domain technique:

   Spatial domain technique is also known as substitution techniques, are group of techniques that create a covered channel in parts of the cover image in which changes are bit.

3. Transform domain technique:

   Transform domain technique is less exposed to compression, cropping and image processing.

4. Spread spectrum technique:

   Spread spectrum technique in radio communications transmits messages below the noise level for any given frequency. With integration of image steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image.

5. Statistical method:

   Statistical method is used to modify statistical properties of image in addition to preserving them in the embedding process.

6. Distortion techniques:

   In this technique knowledge of original image is required to check differences between original cover image and the distorted cover image to retrieve secret message. Encoder adds a sequence of changes to the cover image.

7. File embedding:

   In this techniquej information is stored in header structure or at the end of file.

8. Pallet embedding:
   In this technique pallet is used to hide secret information. Order of colours in pallet also used to transfer information. Hidden message can be embedded using the differences between two colours.

3.2 Methods Comparison

From [13] all methods used are listed as below and advantage and disadvantage of methods is also written below:

LSB:

Advantages:

- Imperceptibility is high.

- Payload capacity is high.

Disadvantages:

- Robustness is low.

Transform Domain:

Advantages:

- Imperceptibility is high.
- Robustness capacity is high.

Disadvantages:

- Payload capacity is low.

Spread Spectrum:

Advantages:

- Imperceptibility is high.
- Payload capacity is high.

Disadvantages:

- Robustness is Medium.

Statistical Techniques:

Advantages:

- Imperceptibility is Medium.

Disadvantages:

- Payload capacity is low.
- Robustness is low.

File and Pallet Embedding:

Advantages:

- Imperceptibility is high.
- Payload capacity is high.

Disadvantages:

- Robustness is low.

3.3 Algorithm

3.3.1 RSA algorithm and Hash-LSB technique:

RSA algorithm is an encryption algorithm in which two prime numbers are taken initially and then the product of these values is used to create public and private key.

RSA algorithm can be used with HASH-LSB technique to embed cipher text in image.

RSA algorithm steps:

- Select two large strong prime numbers
- Compute Euler's totient value for n:f(n)=(p-1)(q-1)
- Find random number e satisfying 1<e<f (n) and relatively prime to f (n).
- Calculate a number such that d=e-1 mod f (n).
- In Encryption phase: take plain text m satisfying m < n, then the cipher text $c=m^e$ mod n.
- Decryption: The cipher text is decrypted by $m=c^d$ mod n.

In [8] Hash based Least Significant Bit (H-LSB) which position of LSB for hiding the messages is decided based on hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are hidden into these RGB pixels. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be divided into RGB format. Then the Hash LSB technique will uses the values given by hash function to hide message inside image.

3.3.2 Cryptography algorithm

- Change the key and message in to ascii format.
- Pad message according to the length of key.
- Take two arrays flag text and flag key of size of text and key and fill it with zeros.
- Do these processes till the length of key.

3.3.3 Hyper Image Encryption Algorithm

- Select an Image which is having at least 256 bits in Size to Be encryption.
- Calculate Binary Value of Image.
- Select First 256 bits form Binary Value and create 16 sub Blocks of 16 bits. This process will repeat till end of file.
- Select Key Value of 256 bits. And create 16 sub blocks of 16 bits.
- Select 64 bits from transformation table. And create 4 blocks of 16 bits.
- Apply Logical operation XOR between first 8 block of selected image and second 8 block of selected key.
- Apply Logical operation XOR between last 4 blocks of selected images and 4 blocks of transformation table.

- Apply Circular Shift Operation on last 4 block of selected key and second last 4 block of selected image.
- Apply logical XOR operation between selected image and key which is output of step 8. Result will store in image block.
- Apply Circular Shift Operation on 4 blocks of Transformation table and second last 4 block of selected key.
- Apply logical XOR operation between transformation table and selected key, which is output of step 10. Result will store in key block.

.

- Combine output of step 6, 7, 9, and 11 in such that it should be produced 256 bits total.
- Output of step 12 will become input for next round.
- Repeat step-1 to step-13, 10 times.
- After 10th round, cipher text will produce of selected image.

3.3.4 Enhanced least significant bit algorithm

- Select a cover image of size M*N as an input.
- The message to be hidden is embedded in Blue component only of an image.
- Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Enhanced Least Significant Bit (ELSB) of every pixel to hide information, leaving most significant bits (MSB).

After that Message is hidden using Bit Replacement method.

3.3.5 K-MATRIX

- K-MATRIX is a 2 X 2 Matrix. This stores 4 different numbers between 1 to 16.
- Select a cover image of size M*N as n input.
- Convert the message ASCII value into binary form.
- Make the two digit pairs of obtained data starting from left.
- Mapping of these pairs is done with the number assigned in the corresponding cell of K-MATRIX to obtain another number.
- New corresponding number will be again converted in binary form.
- Now the obtained Bits are being stored behind the LSB of RGB components of pixel of an image.
- Repeat above step until the whole message is being hidden.

3.3.6 Text-To-Image Encryption (TTIE)

- In this algorithm there are two phase: TTIE phase and ISE(Image Shuffle Encryption) phase.
- In the TTIE phase the plain text is transformed into an image. In this phase plain text is concatenated as string is stored into array of characters.
- For each character in array one pixel of resulting image is generated. Each pixel consists of three integers created randomly before transmission.
- Each integer of three integer values represents one color. The color value is the range from 0 to 255. The result of this phase is matrix.
- In ISE phase matrix is shuffled number of times.
- In shuffle process row and column swapping is done.
- In row swapping two rows are selected randomly and swapped.
- In column swapping tw

4. CONCLUSION

We have done survey of image steganography techniques and learn advantage and disadvantage of all image steganography techniques. From all steganography techniques the Least Significant technique is better because it easy to process using this technique and also using encryption scheme in LSB makes it better but there is also disadvantage of this.

We identify that using traditional encryption algorithm with least significant bit is very time consuming. So we are going to minimize this problem as possible.

5. REFERENCES

[1] http://en.wikipedia.org/wiki/Steganography.Date: 9/12/2014

[2] Rosziati Ibrahim and Teoh Suk Kuan,"Steganography Algorithm to Hide Secret Message inside an Image". David Publishing, February 25, 2011.

[3] Saurabh Singh, Gaurav Agarwal, "Use of image to secure text message with the help of LSB replacement", International Journal of Applied Engineering Research, Dindigul Volume 1 2010.

[4] Vikas Tyagi, "Data Hiding in Image using least significant bit with cryptography", International Journal of Advance Research in Computer Science and Software Engineering, Volume 2,4th April 2012.

[5] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm", International Journal of Computer Technology and Electronics Engineering, Volume 1.

[6] Ahmad Abusukhon, Mohamad Talib, Issa Ottoum, Secure Network Communication Based on Text-to-Image Encryption, International Journal of Cyber-Security and Digital Forensics, 2012.

[7] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography.", International Journal of Cyber-Security and Digital Forensics 4,Volume 15, July 2012.

[8] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique". International Journal of Computational Science & Software Engineering, Volume 3, 2013.

[9] Rahul Joshi, Lokesh Gagnani, Salony Pandey, "Image Steganography with LSB", International Journal of Advance Research in Computational Engineering & Technology, Volume 2, 1 January 2013.

[10] Chital R. Gaidhani, Vedashree M.Deshpande and Vrushali N.Bora, "Image Steganography for Message Hiding Using Genetic Algorithm", 30 March 2014.

[11] Komal Singh Arora and Geetanjali Gandhi, "Enhanced Steganography using K-MATRIX", International Journal of Computer Sciences and Engineering, Volume-2, 30 June 2014.

[12] Chandra Prakash Shukla, Mr. Ramneet S Chadha," A Survey of Steganography Technique, Attacks and Applications", International Journal of Advance Research in Computer Science and Software Engineering, 2 February 2014.

[13] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. AI-Qershi, "Image Steganography Techniques: An Overview."

[14] http://en.wikipedia.org/wiki/Information_security.Date: 9/12/2014

[15] http://simple.wikipedia.org/wiki/**RSA_(algorithm)**.Date: 9/12/2014

