ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

An Enhanced Least Significant Bit Steganography Technique

Mohit

Abstract - ***Message transmission through internet as medium, is becoming increasingly popular. Hence issues like information security are becoming more relevant than earlier. This necessitates for a secure communication method to transmit messages via internet. Steganography is the science of communicating secret data in several multimedia carriers like audio, text, video or image. A modified technique to enhance the security of secret information over the network is presented in this paper. In this technique, we generate stegno-key with the help of slave image. Proposed technique provides multi-level secured message transmission. Experimental results show that the proposed technique is robust and maintains image quality.***

Index Terms – Steganography, Least-significant-bit (LSB) substitution, XORing pixel bits, master-slave image.

I. INTRODUCTION

Data is being transmitted with the use of network today. But transmission through network is subjected to various issues like data unauthorized data access. Now, steganography introduced by Greek Historian Herodotus is available to tackle these issues.Steganography helps to transmit data secretly to authorized receiver only. Cryptography, water marking and finger printing are techniques similar to steganography[1].

Steganography is basically composed of following two words: Stegano and Graphy. The word “Stegano” is a Greek work “Steganos” which actually means “Covered” whereas “Graphy”is a Greek word “Graptos” means “Writing”. In all, steganography means “covered writing” which signifies the motive to cover or hide whatever written.

Mohit, Student, Computer Science and Engineering Department, Guru Jambheshwar University Of Science & Technology, Hisar, Haryana, India (u9mohitgoyal@gmail.com)

Steganography is an important technique because it does not allow the attacker to identify if there is any message. This technique basically emphasis on hiding rather than protecting information. Data in which secret data is hidden is called carrier object or cover-object whereas data which is hidden is called stego-object[2].

This technique can be applied on various multimedia like image, audio, video and text.

Text Steganography: In this technique, basics of text are used to hide data based on format based and random method such as capital letter, tabs and spaces[3].

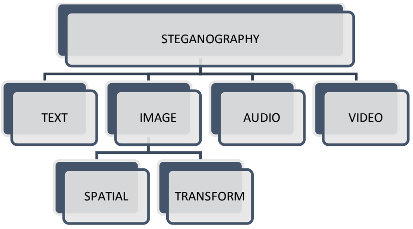

Fig.1. Classification of Steganographic techniques[4].

Image Steganography: Image intensity and pixels are used as covered object in which text as stego object is used. Some commonly used carrier object in image steganography are GIFF, JPEG and BMP etc.In this technique, pixel values and intensities are changed based upon stego values in such a way that changes in covered objects remains approximately unnoticeable[2].

Audio Steganography: In this technique, audio in various formats like .WAV, .MIDI, .AVI, .MPEG as covered object is used. This technique is very popular due to high popularity of voice over IP (VOIP). Various methods are applied in audio based upon its characteristics like low bit coding, phase coding and spread spectrum[2].

Video Steganography: Video, basically combination of pictures in particular sequence is used as covered object in various formats like .MP4, .MPEG, .AVI etc. In this technique, discrete cosine transform (DCT) alters pixel value of image which is impossible to interpret by human eye due to negligible change in the picture[3].

The effectiveness of a steganography technique can be evaluated by comparing stego-image with the cover-Image based upon some factors as follow[2], [3]:

Robustness: This property ensures that converted image will remain intact after transformation independent of type of transformation used.

Imperceptibility: The imperceptibility means invisibility which actually means here is that whatever the algorithm is used should remain unidentified. This property signifies the strength of technique by which covered object and stego-object are similar.

Payload Capacity: This actually refers to the amount of object that can be hidden in cover-object. Large amount of stego-object data that can be hidden signify high payload capacity.

PSNR (Peak Signal to Noise Ratio): This Ratio signify the quality difference between original image and stego-image and defined as the ratio between the maximum available power of a signal and the power of noise that affects the fidelity. The higher the value of PSNR, the higher the quality of conversion.

MSE (Mean Square Error): MSE is calculated by adding up the squared differences of all the pixels and dividing by the total pixel count. The smaller the value of MSE, the better the technique.

II. IMAGE STEGANOGRAPHIC TECHNIQUE

Image steganography techniques can be categorized as follows:

Spatial domain technique (LSB)

Least significant bit (LSB) in this technique we use pixel values of image for embedding the message into the image. We use last bit of n no. of pixels for embedding the n-length message. Since it hides the message in the LSBs of the pixel values, negligible distortion, imperceptible for the necked eyes[2], [5].

Advantages

There is less change for distortion of the original image.

More data can be embedded into an image.

Disadvantages

Less robust, the hidden data can be lost with image manipulation (image compression, crop, resize etc.).

Transform domain technique

In transform domain information is embedded into the image using various algorithms and transformations. In DCT transform pixels are grouped into non-overlapping blocks of pixels and transforming these blocks into DCT coefficients. Tseng and Chang [6]applied DCT for each block of 8×8 pixels[5].

III. RELATED WORK

Steganalysis is used to encrypt data to prevent un-authorized attack and reliability of the algorithm is measured by S-tool. Udhayavene et al.[1] compared LSB and DKL on the basis of Mean Square Error, Peak Signal Noise Ratio, Relative Payload and Rate of Embedding and proved DKL to be more efficient. Suitable cover image is used to hide desired text by using DKL technique and extraction algorithm is separately used to retrieve the secret message.

Yang et al. [7] put forward a method that uses the difference of values of consecutive pixels. K-bit LSB is employed at the edge areas with large value while that of small values for smooth area. Pixel difference of nearby values is used to calculate the secret bits that can be embedded. Experimentally it is observed that this method outperforms over existing algorithms but the problem of automatic analysis of cover image still exists.

Baek et al.[8] proposed an intelligent method for cover image that utilized observed relationship between binary and grey code representation and secret data is embedded in the altered image rather than original. The proposed scheme first converts binary values to grey code values and then EX-OR with desired text data.

High PSNR value and histogram almost identical to original values are experimentally observed but N cover image are needed to decode stego image.

A novel steganography technique by Das and Tuithung[5] used Huffman Encoding using two 8 bit grey level image of M×N and P×Q as cover image and secret image respectively. Huffman code is embedded at LSB value of pixels for secret message and size of code itself making stego image a single point information to the receiver. High capacity and good security without compromising the quality of stego image are experimentally observed characteristics of the algorithm.

Gupta et al. [9] introduced an enhanced LSB technique which changes 3 Bits of blue color only rather than 1Bit of each of primary color i.e. Red, Green and Blue. In this way, this algorithm reduce the leap of color values on color scale by 65,793. Enhanced technique is applied on image after applying Pixel filtering over blue component of image.

We summarize our main contributions as follows:

1. We provide three level securitieson the message (using image and xor logic- property).

- Level 1: Encode our text message into binary form.
- Level 2: 2nd level encoding by XORing with slave image pixel bit.
- Level 3: Embed the double-encoded message into master image.

2 Our message uses intrinsically generated key without any external dependence.

IV. PROPOSED METHOD

Our algorithm

Input: n-digit secret message D to be transferred securely, two images (Master (M) & Slave(S)).

Output: n-digit secret message D received securely.

The procedure of embedding the message in master image is explained as follows:-

Encoding phase (at sender's end):-

1. Encrypt D using alphabets and special characters, to generate n-digit encoded text D'.
2. XOR D' with slave image pixel bits S(x,y) to generate D' (i).
3. Hide D' (i) in master image M using LSB technique.

Decoding phase (at receiver's end):-

4. Extract $D'(i)$ from master image M using LSB.
5. XOR $D'(i)$ with slave $S(x, y)$ to get D'.
6. Decode D' to obtain D.

Following are the detailed steps of our proposed approach:-

1. Key generation algorithm:-

1. Generate random 62-length alpha-numeric sequence s (26 a-z, 26 A-Z, 10 zero-nine).
2. Encrypt D with key s, $(s[i] \rightarrow D'[i]\ \forall i \in [1, n])$.
3. Encode D' [i] into binary form using function dec2bin () to generate D' with size $= i \times 8$.
4. Let Sbe the slave image of size p × q, where p is the no rows and q is no of Columns, of S.
5. Convert s pixels into binary form with same function dec2bin ().
6. XOR binary bits of S and D':-

```
For $i = 1$ to size
$D'[i] = XOR(S[i, 1], D'[i]);$
End
```

2 Hide message into image:-

1. Prepend message length to D'.
2. Find the block size in image for embedding the message on LSB of image:-

Block size = ceiling (image size/message size).

3. Embed message on LSB of image pixel on first bit of contiguous blocks.
4. Decoding steps are analogous to the encoding steps discussed above.

V. EXPERIMENTAL RESULTS

The steps followed in our approach are shown in figure 2. Security is provided sequentially three times, first while encrypting the message, second while XORing encrypted message bits with slave image bits and third while embedding the stegno-bits into master bit-blocks. Our approach differs from LSB (figure 3) and Enhanced LSB [9](figure 4).

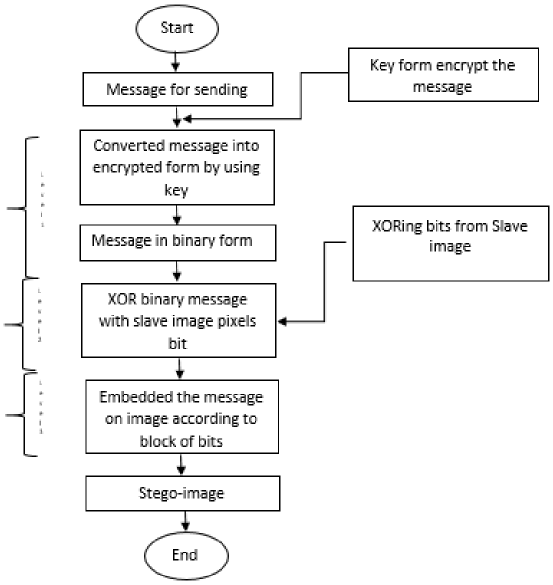
Start
Message for sending
Key form encrypt the message
Converted message into encrypted form by using key
Message in binary form
XORing bits from Slave image
XOR binary message with slave image pixels bit
Embedded the message on image according to block of bits
Stego-image
End

Fig.1 Flow Chart of proposed approach.

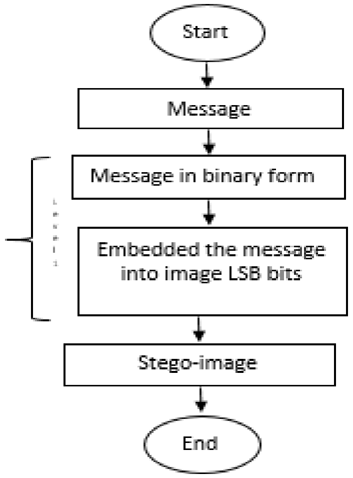

Fig.2 Flow Chart of simple LSB Technique

We implemented the algorithm in MATLAB® 2015b version. Since our method is based on LSB substitution, experiments carried out demonstrate the preservation of image quality.

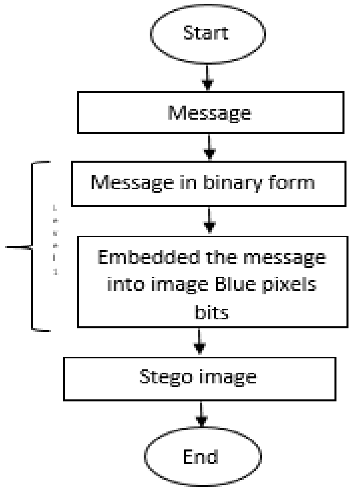

Fig. 3 Flow Chart of Enhanced LSB Technique[9]

Quality difference between cover image and stego-image is measured using PSNR[10] (Peak Signal to Noise Ratio).

$$PSNR = 10 \times \log(\frac{255^2}{MSE})$$

$$MSE = \sum_{x=0}^{N-1} \sum_{y=1}^{N-1} \frac{f(x,y) - g(x,y)^2}{N^2}$$

Functions $f(x,y)$ and $g(x,y)$ refer to intensity values of pixel located at (x,y) of cover and stego image respectively. It is measured in dB. PSNR is inversely proportional to the distortion b/w cover and stego-image. Summary of results obtained after experiment are shown in Table 1:

Table 1 Performance of the proposed approach with random secret message

Name	Type	size	MSE value	PSNR for LSB	PSNR for E-LSB
Lenna	BMP	512×512	1.3733e-04	86.753	87.131
Baboon	PNG	298×298×3	3.33782e-04	82.843	83.174
Boat	PNG	512×512	9.1553e-05	88.514	91.524
Lenna	Jpg	512×512	9.7275e-04	78.250	78.250
Mohit	jpg	399×300×3	0.0021	74.863	77.463
import	Jpg	330×330×3	0.0023	74.435	75.869

VI. CONCLUSION

In this paper, we have presented a new method for image steganography which improves the security of data over the transmission network. Based on adaptive LSB substitution, our method embeds secret message into master image without any perceptible distortion. Since we generated key from slave image, we circumvent any possible errors due to random encryption. The algorithm was applied on BMP images. Using this method, we can fully recover our stego-message. We conclude that the embedding capacity of data depends on master image pixels.

REFERENCES

[1] S. Udhayavene, A. T. Dev, and K. Chandrasekaran, “New Data Hiding Technique in Encrypted Image: DKL Algorithm (Differing Key Length),” *Procedia Computer Science*, vol. 54, pp. 790–798, 2015.

[2] M. Hussain and M. Hussain, “A survey of image steganography techniques," *International Journal of Adavanced Science and Technology*, vol.54, 2013.

[3] J. Kour and D. Verma, “Steganography Techniques–A Review Paper,” *International Journal Of Emerging Research in Management & Technology*, vol.3, issue 5, pp. 2278–9359, 2014.

[4] B. Saha and S. Sharma, “Steganographic Techniques of Data Hiding Using Digital Images (Review Paper),” *Def. Sci. J.*, vol. 62, no. 1, pp. 11–18, 2012.

[5] R. Das and T. Tuithung, “A novel steganography method for image based on Huffman Encoding,” *3rd National Conference onEmerging Trends and Applications in Computer Science (NCETACS),* pp. 14–18,2012.

[6] C.-C. Chang, T.-S. Chen, and L.-Z. Chung, “A steganographic method based upon JPEG and quantization table modification,” *Information Sciences*, vol. 141, no. 1–2, pp. 123–138, 2002.

[7] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems, ”*IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, 2008.

[8] J. Baek, C. Kim, P.S. Fisher, and H. Chao, “(N, 1) secret sharing approach based on steganography with gray digital images, "*IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, pp. 325–329,2010.

[9] S. Gupta, G. Gujral, and N. Aggarwal, “Enhanced least significant bit algorithm for image steganography,”*International Journal of Computational Engineering & Management*, vol. 15, no. 4, pp. 40–42, 2012.

[10] Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” *Electronics Letters*, vol. 44, no. 13, pp. 800–801, 2008.