International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

An Improved Image Steganography Technique based on LSB

Chetan G. Tappe[1], Anil V. Deorankar[2]

[1]P.G. Student, Department of Computer Engineering, Govt. College of Engineering, Amravati, India[1]
[2]Associate Professor, Department of Information Technology, Govt. College of Engineering, Amravati, India[2]

Abstract **-** The propose paper introduces of secure communication in social demand like Facebook, twitter ,networking site etc. purpose of secure data like text, image, video, audio. Steganography is different type of data hiding technique for robustness , high capacity ,security ,embedded data , visibility ,PSNR, payload capacity ,term of steganography in this paper novel of image steganography is an established method for hiding data from an Unauthorized access of original image data cover for target image .then using encryption key for add embedded data they must be extract data using encryption key for separated data final got in original image. a novel image steganography technique based on most significant bits (MSB) of image pixels is proposed. Improvements in signal to noise ratio. Usually, the hackers focus on LSB bits for secret data extraction but the recommended technique utilizes the MSB bits that make it more secure from unauthorized access.

Keyword- Steganography, LSB, Stego image, embedded data. Cover image.

1. INTRODUCTIONS

In cryptography secret text is converted into cypher text, while in steganography the secret text remains the same but it is embedded in another format of data. Today, in the presence of powerful communication systems, protecting the secret information from the hackers is a challenging task. Steganography hide the existence of information and protects secret information from unauthorized access. A stenographic system consists of three components, namely: Plain text, Cover file, and Stego file. Secret information to be protected is known as plain text. Cover file can be text, image, audio or video in which data is embedded. Stego file is the output of the stenographic system that contains the hidden information. The proposed research work introduces an innovative technique in steganography to maintain the quality of the cover image and also increase the security. The work is based on the color image steganography in spatial domain with maximum data capacity. Using this method the perceptible quality degradation will be minimized and security will be enhanced. In this proposed method the embedding of the secret information is done on a 16 bit color image by using a secure hash function. Similarly, we can extract the secret information from the stego-image. By this technique we can embed 0, 1, 2 or 3 bits of the secret information starting from the least significant bit position of the cover image.

Important issue and steganography offer a very reliable solution for such problems. Steganography is an art and science of embedding secret message into cover medium. In steganography, secret message is embedded in an appropriate carrier object that may be image, video, sound or other file to be transmitted over internet and embedding is parameterized by a key that makes difficult to even detect the presence of data and further to find a key to access it. Once cover object is embedded, it is known as stego object. Steganography had been in use from historical times. Simmon stated that steganography also commonly known as 'Prison's Problem' because in earlier times prisoners used it in prisons for communication purposes. Most basic method of steganography is to utilize the redundant information available in digital medium. There is an increasing interest in using images as cover media for stenographic communication and detection of covert communications that utilize images has become an important issue.

An RGB channel based image steganography technique is proposed. In this method, a bit of hidden information is inserted within 3rd to 8th bit position of either blue component or green component or red component of a pixel. A hash function and a secret key are used to select the data embedding position inside the color byte. In this method, only a single bit can be inserted into a color byte by changing two LSBs of both the blue and green components. Even if data is not inserted into a pixel, both LSBs of blue and green components are changed. The payload capacity as well as the PSNR is lower because two lower significant bits are changed when secret data is inserted.

2. LITERATURE REVIEW

An LSB image steganography technique is presented. In [1], an LSB array based technique is proposed, in which all the bits of LSB's are taken for data hiding. In this technique, encrypted message block is mapped to the LSB array, where maximum matching is found. In [2], an image steganography technique based on adaptive LSB substitution is proposed. The presented technique calculates the number of k-bits (bits to be hidden) by taking into account the edges, brightness and texture masking of the cover image. The experimental result of this technique shows that the value of k is high at non-sensitive image region and it is low at sensitive image regions. Advantage of adaptive based technique is that it can embed high capcity of data, but dataset for experiments is limited; there is not a single image which has many edges with noise region. A combination of stego-key pattern bits and secret bits is used to modify the LSB of cover image pixels [3]. A combination of M×N block with random key value is used as a pattern. The embedding procedure modifies 2nd LSB bit of the cover image pixel if the pattern matches with the secret data bits. This technique is complex in terms of security but lacks in payload capacity.

The majority of today's steganography systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern Steganography uses the opportunity of hiding information into digital multimedia and also at the net-work packet level Another adaptive LSB technique named pixel value difference (PVD) is presented in PVD technique uses [4] a simple relationship of pixel difference between two consecutive pixels of cover image to estimate the size of the hidden data bits. This relationship determines adaptive k-bits to be hidden in cover image. The experimental results of PVD technique show that it can produce high quality stego images with a decent amount of pay load capacity and high impeccability. However, the PVD technique is complex and computationally cost in-effective as it has to calculate pixel value difference for every consecutive pixel pair of the cover image. Multi-Pixel Differencing (MPD) technique [5] in contrast to PVD uses four pixels to calculate sum of difference value of a four pixel block. It uses the simple LSB embedding method when the difference is low and uses MPD when it is high. MPD is a simple and computationally efficient technique if the dataset is small otherwise it's a complex way of data hiding. Another PVD technique that takes into account 3 pixels for difference calculation is presented in The number of k-bits are estimated using three pixels near the target pixel.

3. METHODOLOGY

The proposed technique is based on two steps- one is embedding and the second is extraction. Compare with some existing technique already discussed in the literature survey proposed technique provides better capacity, security and quality of stego-image. Here we have used a secure hash function. The data hide capacity per byte is also increased here.

A. Encoding Algorithm

The data encoding procedure of the proposed technique. The steps for encoding the secret information in cover image are given as under:

i. Read the secret information bits

ii. Read the cover image

iii. For every pixel of cover Image
   a. Read bit No. 5 and 6
   b. Compute the difference
   c. Compare the difference with secret information bit, If data bit is not equal to the difference then transverse bit No. 5

iv. Write the stego image.

B. Decoding Algorithm

The following steps are required to extract the secret information bits from the stego image.

i. Read the stego image

ii. For every pixel of stego image
   a. Compute the difference between 5th and 6th bits: data bit = difference

iii. write the secret data to file

In above algorithm, after reading every pixel of stego image, we take the difference between 5th and 6th bit. The result of difference will be the value of data bit. The data decoding procedure of the proposed algorithm.

4. EXPERIMENTAL RESULTS ANALYSIS

The results of this research paper are obtained by applying the proposed method on four standard images. All the cover images have the same dimension of 512 × 512, with the same size of 768 KB of 24 bit bit-map. The cover image and the stego-image are column wise. The embedding and extraction operation are done using the *.Net* platform.

Then the statistical measurement like peak signal to noise ratio (PSNR) and mean square error (MSE) are obtained using shown in Table I.

The peak signal to noise ratio is the most important terms with respect to measure the quality of a cover image and its corresponding stego-image. The PSNR is measured using the following equation

$$PSNR = 10\log_{10}\frac{255^2}{MSE}db \quad (1)$$

Where M is peak signal level for a color image and MSE is computed by the equation (2).

$$MSE = \frac{1}{w*h}\sum(c(ij) - s(jk))^2 \quad (2)$$

H and W are the height and width of the frame and C(i, j) and S(i, j) represents the cover image and corresponding stego-image respectively. A high value of PSNR indicates the less distortion in stego-image, hence the discrepancy between cover image and stego-image is more invisible to human eyes. According to the right column. It is clear that there are no such noticeable dissimilarities between the original image and
stego-image.

TABLE I. STATISTICAL MEASUREMENT

Cover Images	Maximum Payload (bits)	Embedded Payload (bits)	PSNR (dB)	MSE
Ankush	885150	784110	44.97	2.07
Chetan	884320	785436	44.88	2.11
Bhagyesh	880513	787392	44.78	2.16
Mayur	881523	784832	45.09	2.01

TABLE II. PROPOSE METHODS

Technique	PSNR	Payload
Proposed	47.50	786432

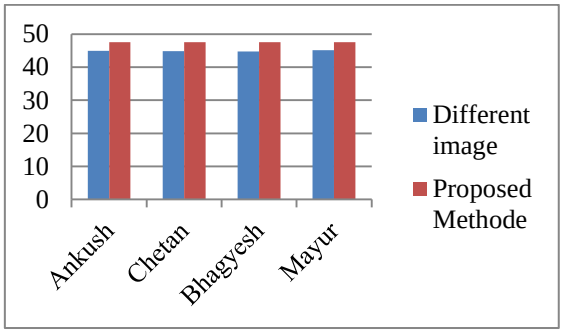

Fig.1 Comparison of PSNR value (dB).

5. CONCLUSION

In this work Steganography provides a reliable solution by hiding the very existence of message and hence used as a security tool. The technical challenge of data hiding is finding redundant bits in carrier signal that cannot be statistical and perceptually attacked Uncompressed file formats (BMP, GIFF, TIFF,JPEG.) based on lossless compression provides high data capacity and are more convenient for data hiding algorithms. Usually, the LSB are targeted in steganography systems, therefore using the MSB makes the system more secure. Furthermore, comparative analysis shows that the proposed technique has greater PSNR that shows the effectiveness of the proposed scheme. Payload capacity of the proposed technique is also comparatively better than the available techniques which can be used to hide more data in a single cover image.

REFERENCES

[1] M. Juneja, and P.S. Sandhu, "Designing of Robust Steganography Technique Based on LSB Insertion and Encryption". Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, pp. 302–305, 2009.

[2] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radio Engineering, vol. 18, pp. 509-516, 2009.

[3] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, vol. 1, 2009.

[4] X. Li, T. Zeng and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in Proc.10th ACM Workshop

on Multimedia and Security, Oxford, U.K, pp. 133–138, 2008.

[5] H. W. Tseng and H. S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Hindawi Publishing Corporation, Journal of Applied Mathematics, vol. 2013, no. 13, pp. 1-8, 2013.

[6] M. Hussain and M. Hussain, "A survey of image steganography techniques," International Journal of Advanced Science and Technology, vol. 54, pp. 113-124, 2013.

[7] P. Thomas, "Literature survey on modern image steganographic techniques," International Journal of Engineering Research and Technology, vol. 2, 2013.