ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (119-125), Month: October - December 2015, Available at: www.researchpublish.com

Analysis of Various Methods in Image Steganography

[1]N.Suganya Nachiyar, [2]Mr.Y.R.Packia Das

[1]Dept of ECE, IInd M.E(C.S) PET Engineering College, Vallioor

[2]M.E, MISTE, Associate Professor, Department of ECE, PET Engineering College, Vallioor

***Abstract:* In this project, an improvement in the plain LSB based image steganography is proposed and implemented. The paper proposes the bit inversion technique to improve the stego image quality. Two schemes of the bit inversion techniques are analysed and implemented. In these techniques, Least significant bits of some pixels of host image are inverted if they appear with a particular pattern of some bits of the pixels. In this way, less number of pixels is modified in comparison to plain LSB method. So peak signal to noise ratio of stego image is improved. For correct de-steganography, the bit patterns for which LSBs were inverted needs to be stored within the stego image somewhere. The proposed bit inversion techniques produce very good improvement to LSB steganography. This steganography technique should be combined with other methods for further improvement in image steganography.**

***Keywords:* Image Steganography, LSB inversion, Peak signal to noise ratio, mean square error.**

I. INTRODUCTION

Steganography is a data hiding technique which conceals the existence of data in the medium. It is in this sense, differs from cryptography, which encrypts the data and transmit it without concealing the existence of data. Steganography provides secret text or images to prevent them from attackers. Image steganography embed the message in a cover image and changes its properties. Steganography provides secret communication so that intended hacker or attacker unable to detect the presence of message. Steganography, derived from Greek, literally means "covered writing." It includes a huge array of secret communications methods like microdots, character arrangement, digital signatures, covert channels, and spread spectrum[1].The basic concept is that it has a cover object that is used to cover the original message image, a host object that is the message or main image which is to be transmitted and the steganography algorithm to carry out the required object. The output is an image called stego-image which has the message image inside it, hidden. This stego image is then sent to the receiver where the receiver retrieves the message image by applying the de-steganography.The advantages of Least-Significant-Bit steganographic data embedding are that it is simple to understand, easy to implement, and it produces stego-image that is same as that of cover image and its visual infidelity cannot be judged by naked eyes. Several steganography methods based on LSB have been proposed and implemented[2][3][4][5].

A good technique of image steganography aims at three aspects. First one is capacity that is the maximum data that can be stored inside cover image. Second one is the imperceptibility that means the visual quality of stego-image after data hiding and the last is robustness[6] . The LSB based technique is good at imperceptibility but hidden data capacity is low because only one bit per pixel is used for data hiding. Several staganalytic methods have been developed to detect the hidden message from the original image which is used in communication.

Several staganalytic methods have been developed to detect the hidden message from the image in communication. One of the earliest methods is chi-square test [7], which performs statistical analysis to identify the message. By reducing the sizeof message, detection risk in this attack can also be reduced. In [8], authors have proposed technique known as RS staganalysis which can estimate message size efficiently when the message is embedded randomly.

In [9], a powerful staganalysis method is proposed, called SPA, which uses sample pair analysis to detect the message length. In this paper, have two LSB based steganography schemes which are more secure than plain LSB method. Staganalysis is performed on the plain LSB stago-image to clarify the bit patterns of second and third LSBs that co-occur with LSB. Based on this analysis, LSB of those pixels may be inverted with a specific bit pattern, which improves the PSNR of stago-image and also makes the task of staganalysis difficult.

II. BLOCK DIAGRAM

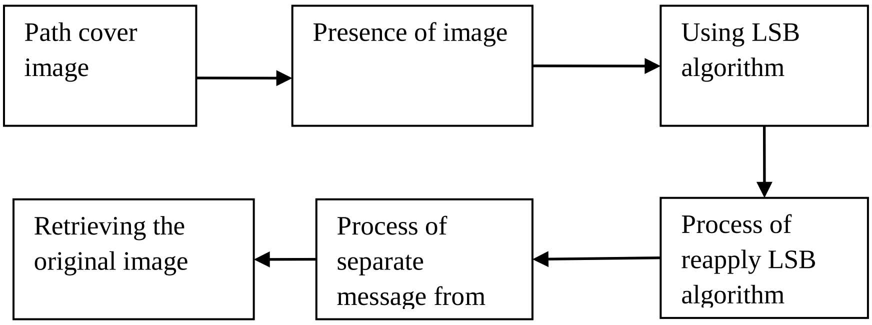
Path cover image
Presence of image
Using LSB algorithm
Process of reapply LSB algorithm
Process of separate message from
Retrieving the original image

Fig.1 Block diagram for the steganography techniques

The block diagram consists of the input image. At first the input image is to be embedded by the LSB algorithm.The original image is embedded into the cover image by using least significant bit inversion method. The image values are first converted into ASCII format and go for the embedding process.The process of apply the LSB algorithm for each bit at the sender side which produce the stego image. The stego image is transmitted to receiver, which provides the secret message from the stego image. Finally retrieving the original image by using steganographic techniques.

III. STEGANOGRAPHY METHODS

A. Steganography using LSB:

The JPEG image is the most fashionable file format in relation to digital images. However, up to the present time, there implys to have been very few data hiding techniques taking the JPEG image into account. In this method, propose a high capacity data hiding technique based on JPEG. The recommended method employs a capacity table to estimate the number of bits that can be masked in each DCT component so that significant distortions in the stego-image can be avoided.

The capacity table is borrowed from the JPEG default quantization table and the Human Visual System (HVS). Then, the adaptive least-significant bit substitution technique is employed to process each quantized DCT coefficient. The proposed data hiding method permits to restrict the level of embedding capacity by using a capacity factor. According to the experimental results, a new scheme can be achieved high embedding capacity of around 20% of the squeezed image size with little noticeable degradation of image quality.In this new method, do not embed the secret data in the high-frequency components in order not to expand the size of the stego-image.

Besides, the LSB number in each DCT coefficient used for data hiding depends on the characteristics of the image according to HVS; as a result, the embedding capacity of the JPEG compressed image can be raised while avoiding significant stego-image distortion. Meanwhile, the capacity formulas for the DC and AC components should be different due to the discrepancy between them. The below table shows the values of quality factor, capacity factor and PSNR value. If increase the value of Q and reducing the capacity factor, which produce the PSNR value in decreasing mannar.

TABLE 1: PERFORMANCE MEASURES

Q factor	Capacity factor	PSNR
5	0.5	41.75
15	0.2	39.38

B. Data hiding using SPA:

This paper introduces a new, principle approach for detecting LSB steganography in digital signals such as image, text and audio. It is shown the length of hidden message embedded in the least significant bits of signal samples which can be estimated with relatively very high precision. The new steganographic approach is based on some statistical measures of sample pairs that are relatively high sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the steganographic approach, bounds on estimation errors are developed. Furthermore, the vulnerability of the new approach is to detect the possible attacks and counter measures are suggested.

In this method, present a new robust steganographic technique for detection of LSB embedding in digital signals. This method is based on a finite state machine whose states are selected from the multisets of sample pairs, called trace multisets.In this section, to motivate the approach of steganalysis, let us select the effects of LSB embedding on some chosen sets of sample pairs and assuming that the digital signal is represented by the succession of samples s1, s2, · · · , sN are the index represents the location of a sample in a discrete waveform), a sample pair means a two-tuple (si, sj), $1 \leq i, j \leq N$. This method use sample pairs rather than individual samples as the basic unit in steganalysis to use higher order statistics such as sample correlation. Let P be a set of sample pairs drawn from a digitized continuous signal.If the message bits are scattered randomly among the least significant bits of all signal samples and then the use of spatially adjacent sample pairs are made the estimate of p more robust. But this choice of P opens a door for possible attacks on the detection method. An adversary can try to fool the detection method by avoiding hiding message bits at locations where some of adjacent sample pairs have close values. For instance, if the adversary does not embed in adjacent sample pairs that differ by less than 3 in value, then he makes $\rho(\pi, D0) = 0$, $\pi \in \{01, 10, 11\}$. Probability of wrong decision: missing rate when $p > 0$, and false alarm rate when $p = 0$, with the decision threshold set at p^ > 0.018.

TABLE 2: PERFORMANCE MEASURES

	P=0	P=5	P=10	P=20
$\tau = 0$	0.1379	0	0	0
$\tau = 1$	0.1379	0.0069	0	0

C. Encryption using LSB insertion:

A new steganography method for data hiding is proposed. This approach selects the Least Significant Bits (LSB) insertion to embed the data within encrypted image data. The binary representation of the hidden message is used to overwrite the LSB of each byte within the encrypted image in random mannar. The experimental results shows the correlation and entropy values of the stego image before the insertion which are similar to the values of correlation and entropy after the insertion Since the correlation and entropy did not changed, the method offers a very good concealment for data in the encrypted image, and decrease the chance of the encrypted image being detected. The hidden data will be used to enable the receiver to reestablish the same secret transformation table after extracting it and hence the original image can be retransmitted by the inverse of the transformation and encryption processes.

Fig: (a) Baboon **Fig: (b) Lena**

TABLE 3: PERFORMANCE MEASURES

Encrypted images	**Correlation**	**Entropy**
Lena	0.0566	5.2261
Baboon	0.0032	5.5415
Barbara	0.0018	5.5417

This method consists of high image quality and system security. The disadvantages of this method is produce a bit insertion position. The above figures are baboon and lena these are the encrypted image, which produce the value of correlation and entropy values. The values of correlation and entropy are mentioned in table 3.

D. Adaptive LSB Substituition:

Many existing steganography techniques hide more secret data into edged areas than smooth areas in the host image, which will not differentiate textures from edges and produce serious degradation in actual edge areas. To avoid abrupt changes in image edge areas, as well as to obtain the better quality of the stego-image, a novel image data hiding technique by adaptive Least Significant Bits substitution is analysed in this paper. The scheme exploits the brightness, edges, and texture masking of the cover image to estimate the number k of LSBs for data hiding. Pixels in the noise non-sensitive regions are obscured by a k-bit LSB substitution with a lager value of k than the pixels in noise sensitive regions.

To establish that the adaptive number k of LSBs remains constant after pixel modification, the LSBs number is calculated by the higher order bits rather than all the bits of the image pixel value. The theoretical analysis and experiment results show that the suggested method achieves higher embedding capacity and better stego image quality compared with some existing LSB methods.

Fig : (c) F16 **Fig: (d) Tiffany**

TABLE 4: PERFORMANCE MEASURES

Image	**Bit rate**	**Capacity**	**PSNR**
Lenna	5.2634	1379767	22.69
F16	4.4940	1178068	28.45
Tiffany	3.7809	991137	33.65
Peppers	1.000	262144	51.14

The above figure shows the F16 and Peppers, which are used as the input image. After applying adaptive LSB steganography algorithm, this produce the values of bit rate , capacity and PSNR. Each image the PSNR values are different, these are mentioned in table 4. If increasing the values of capacity which increasing the values of PSNR value.

The disadvantage of this method is, it uses the lossy watermark scheme, which makes the error in the image.

E. Data Hiding using GEP:

Steganography method is defined as the art and science of writing hidden in such a way that the sender and the intended receiver only knows that there is a hidden message to be present. One of the most important techniques of steganography uses the Least Significant Bit which hide the secret message in the host image. It is based on swapping the LSBs of the host-image with the secret message bits which produce a stego-image. This scheme consists mainly of two phases: In the first phase, propose a hybrid data hiding technique incorporates LSB technique with a key permutation method. While in the second phase, propose a new scheme for detecting the optimal key-permutation by using gene expression programming (GEP). Where, GEP is a evolutionary algorithm for data analysis and it use the combined advantages of genetic algorithms (GA) and genetic programming (GP).

Data representation is an essential process for implementing GEP according to the nature of the problem. In order to design the chromosomes, a GEP technique called Multigene Families (MGFs) are used which are very useful for finding solutions to combinatorial problems as different items can be organized into MGFs. This kind of genes is obtained when the head length h is zero.The inversion operator is the most efficient specific genetic operators, causing populations to evolve with high efficiency even if used as the source of genetic modification will produce better results than when combined with the others operators.

The inversion operator randomly selects the chromosome, the multigene family to be modified, the inversion points in the MGF and then inverts the sequence between the two selected points. Where, each chromosome can only be modified once by this operator. This experimental results have demonstrated that the proposed method improves the image quality andprovides large message capacity and low computation time as well as increase in the system security.

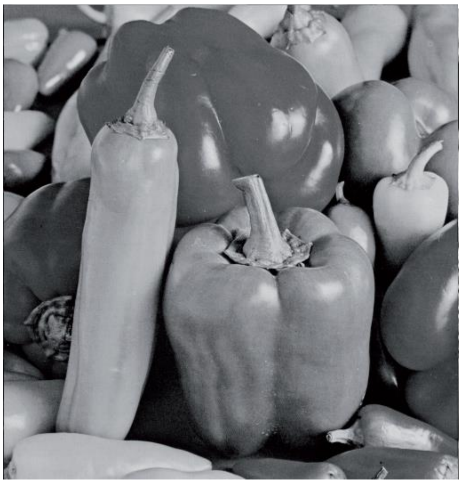

Fig: (e) Peppers

Fig: (f) Barbara

The above figure shows the peppers and Barbara image, which are used as a cover image, This produce PSNR value with the usage of key values. The PSNR values of cipher image, GEP image and LSB are shown in below table 5.The advantages of this method produce larger message capacity, low computation time, high quality and high system security. The disadvantages of this method produce the low PSNR value compare with inverted LSB method.

TABLE 5: PERFORMANCE MEASURES

Cover image	**Cipher**	**GEP**	**LSB**	**Key**
Lena	51.028	51.1742	51.1348	1
Baboon	51.0581	51.1361	51.1180	1
Barbara	51.1174	51.1937	51.1299	1
Pepper	50.994	51.1475	51.1395	1

IV. PERFORMANCE CRITERIA FOR IMAGE STEGANOGRAPHY

SNR:

Signal-to-noise ratio is given by ratio of the power of the signal to the power of noise in the signal. SNR is given in decibels by

$$SNR(db) = 10\ \log_{10} \frac{\sigma_x^2}{\mathrm{MSE}}$$

σ_x^2 → Average squared value of the source image

PSNR:

Peak value of SNR is defined as the ratio of the maximum power of the signal to the power of the corrupted noise signal.

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

Where, the value 255 is the peak in image signal.

MSE:

Mean square error is defined as the measure of average of square of ratio of estimator output to the estimated output. it is also known as the rate of distortion in the retrieved image. Mean square error is given in decibels by

$$MSE(db) = \frac{1}{xy} \sum_{m=0}^{x-1} \sum_{n=0}^{y-1} X(m,n) - Y(m,n)^2$$

X → Matrix data of original image

Y→ Matrix data of degraded image

m→ Index of that row image

n→ Index of that column image

x→ No. of rows of pixel of the image

y→ No. of columns of pixel of the image

V. RESULTS AND DISCUSSION

Analysis of the various survey results discuss with the capacity, PSNR and quality of the Image in the steganographic method for different images. It is proposed to obtain a better quality, capacity and accuracy in the steganography applications. From the survey its clear that the data hiding using inverted least significant method shows better results.

VI. CONCLUSION

This article describes a survey of different method for improve the quality of the images. Then the different methods performance analysis was carried out. Capacity, PSNR and quality of image were estimated for the different techniques. From the literature analysis It is inferred that the LSB bit inversion schemes enhance the stego-image quality. The enhancement in PSNR is not proportional. The improvement in PSNR may be very high for some image as in the case of Test Pat image and for some other image, it may be small. In the first scheme, for given a message image, a set of cover image can be considered and that cover image is selected for which the improvement is largest. Although the third party could determine if the message bits are embedded using some staganalysis methods, he would have difficulty to recover it because some of the LSBs have been inverted; it will misguide the staganalysis process and make the message recovery difficult. The bit inversion method makes the steganography better by improving its security and image quality.

REFERENCES

[1] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganograpby- survey and analysis of current methods. Signal Processing, 90, 727-752.

[2] Chang, Chin-Chen, and Hsien-Wen Tseng. "Data hiding in images by hybrid LSB substitution." Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on. [EEE, 2009.

[3] Zayed, Hala H. "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution." The 30th lnternational Conference on Artifical Intelligence. 2005.

[4] Nadeem Akhtar, Pragati Johri, Shabbaaz Khan, "Enbancing the Security and Quality of LSB based Image Steganography", [EEE lnternational Conference on Computational lntelligence and Computer Networks (CICN), 27-29 September, 2013, Mathura, lndia

[5] Wang, Ran-Zan, Chi-Fang Lin, and Ja-Chen Lin. "Image hiding by optimal LSB substitution and genetic algorithm." Pattern recognition 34.3 (2001): 671-683.

[6] c. Kessler. (2001). Steganography: Hiding Data within Data. An edited version of this paper with tbe title "Hiding Data in Data". Windows & .NET Magazine.http://www.garykessler.netllibrary.

[7] Fridrich, Jessica, and Miroslav Goljan. "Practical steganalysis of digital images: state of the art." Electronic Imaging 2002. lnternational Society for Optics and Photonics, 2002

[8] Fridricb, J., Goljan, M., Du, R.: Detecting LSB Steganograpby in Color and Gray Images. Magazine of [EEE Multimedia (Special Issue on Security), October-November, pp. 22-28. (2001)

[9] Dumitrescu, S., X. Wu and Z. Wang, Detection of LSB steganography via sample pair analysis, Springer LNCS, voI.2578, pp.355-372, 2003.

[10] C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-bydigit data in images based on modulus function, Pattern Recognition 36 (2003) 2875-2881.

[11] Wu, Nan-I., and Min-Shiang Hwang. "Data Hiding: Current Status and Key Issues." IJ Network Security 4.1 (2007): 1-9.

[12] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.

[13] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan Kaufmann, 2007.

[14] The USC-SIPI Image database http://sipi.usc.eduldatabase/

[15] D. Shapira and A. Daptardar, “Adapting the Knuth Morris Pratt Algorithm for Pattern Matching in Huffman Encoded Texts,” Information Processing and Management, Vol. 42, No. 2, 2006, pp. 429-439. doi:10.1016/j.ipm.2005.02.00

[16] K. D. Sonal, “Study of Various Image Compression Techniques,” Proceedings of COIT, RIMT Institute of Engineering & Technology, Pacific, 2000, pp. 799803

[17] M. F. Talu and I. Turkoglu, “Hybrid Lossless Compression Method for Binary Images,” University of Firat, Elazig, Turkey, 2003

[18] W. Walczak, “Fractal Compression of Medical Images,” Master Thesis, School of Engineering Blekinge Institute of Technology, Sweden.

[19] H. Zha, “Progressive Lossless Image Compression Using Image Decomposition and Context Quantization,” Master Thesis, University of Waterloo, Waterloo.

Author’s Biography:

N.Suganya Nachiyar received the B.E degree in Electronics and communication from Anna University, Chennai, 2012. She is currently doing her M.E in in the PET Engg college.

Y.R.Packia Das received the B.E degree in Electronics and communication from Anna University, Chennai, 2006 and M.E degree from Anna University, Chennai, 2011. His is currently working as an Associate Professor in the PET Engg college, Department of Electronics and Communication, Vallioor. His research areas include digital image processing.