ISSN : 2231-0711

Data Hiding Scheme in Spatial Domain

Shanthakumari.R [1] Malliga.S[2] And Dheepika.S [3]

[1]Department of Information Technology,Kongu Engineering College,Perundura,,India.
[3]Department of Information Technology, Kongu Engineering College,Perundurai,India.
[2] Department of Computer Science and Engineering,Kongu Engineering College,Perundurai,India.

Abstract: **Steganography is the practice of concealing messages or information within other non-secret text or data in a way that only the sender and intended recipient identifies the existence of the message. Technically in simple words, steganography means hiding one piece of data within another. In the existing system, such as in Least Significant Bit(LSB) only 4 bits can be embedded in every 4 pixels and in some systems in addition to the message bits, extra bits are to be embedded for providing security. In the proposed Least Significant Bit Inversion(LSBI) algorithm 6 bits of data is embedded in every 4 pixels. Use of grey code standard to hide the secret data inside the cover medium forms a layer of security. The proposed system is evaluated using the quality metrics like Mean Squared Error and Structural Similarity Index.**

Keywords: Image Processing, Steganography, Data Hiding, Grey Code Standard and LSBI.

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. In simple words “steganography means hiding one piece of data within another”. The word steganography is of Greek origin and means “concealed writing” from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". Steganography hides the fact that the communication does not exist. The main objectives of the Steganographic algorithms are to provide confidentiality, data integrity and authentication. The purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceal the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used. It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively.

Yang et al [1] proposed pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. This method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality. This method is complex due to adaptive k generation for substitution of LSB.

Jung et al [2] proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding.

Channalli et al [3] uses common pattern bits (stego-key) to hide data. The LSB’s of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. The disadvantage of this technique is that has low hidden capacity because single secret bit requires a block of (MxN) pixels.

Zhang et al [4] proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

Jain et al [5] proposed a method by which the image pixel values are divided into ranges and based on the range stego-key is generated. The private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of this method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitations of this method are for integrity purpose extra bits of signature are to be hided with hidden message and if the fixed number of bits that has to be embedded in LSB is more than 3 bits then the distortion may occur in the image.

Rajkumar et al [6] proposed a new method for insertion of message in an image. The last two bits of pixel value are used for insertion and retrieval of message. If the last two bits of pixel value are 00 or 10 , the bit 0 of the secret message can be embedded directly, otherwise by adding /subtracting 1 at that pixel value we can insert 0. Similarly 1 is inserted if last two bits are 01 or 11. Message is embedded at pseudo random locations for security reasons. The message is retrieved similarly based on the pixel values of the last two bits. The limitation of this method is that 2 bits of the cover media is considered and only one bit of secret information is embedded.

Vikas Tyagi et al [7], proposed the method of hiding data in the LSB position. This method is chosen because the intensity of image is only changed by 1 or 0 after hiding the information and there won't be much distortion in the image. The drawback of this approach is that an intruder can easily identify the secret data.

Shanmuga Priya et al [8], proposed a method where data is embedded in pair of pixels. The LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information.

From the above survey papers it has been clear that the embedding capacity is low in the existing systems, if more data is embedded the image quality degrades and it also makes the attacker to easily identify the secret data and some systems are more complex to design. The rest of the paper is organized as follows. In section 2, the proposed scheme is discussed. Experimental results is described in section 3, section 4 concludes the paper.

II. Proposed Scheme

In the existing system, such as in LSB only 4 bits can be embedded in every 4 pixels and in some systems in addition to the message bits, extra bits are to be embedded for providing security. In certain existing methods if more data is embedded it results in the distortion of the original image. Thus the problems that were faced in the existing systems are the embedding capacity, security and distortion of image. In proposed system, a novel steganographic method based on Least Significant Bit Inversion algorithm is used for embedding secret data in to the digital images in order to improve the embedding capacity, to minimize the distortion between cover and stego image and to provide security to the secret data. Fig. 1 shows the overall block diagram of the proposed system. This work consist of two phases.

- Embedding Phase
- Extraction Phase

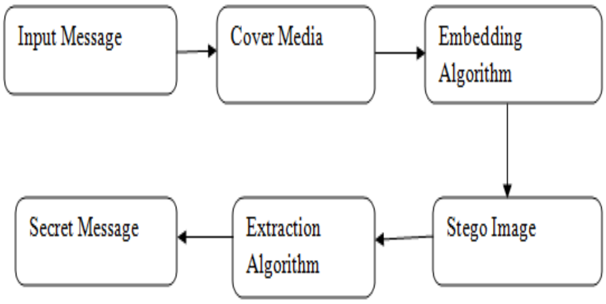


Fig. 1 Model of the proposed system

The details of data embedding and data extraction algorithms are as follows.

A. *Data Embedding Algorithm*

The original uncompressed image C with MxN pixels is assumed to be be grey level. Each grey level is assumed to be 8 bits. Let (i,j) be the pixel location and let C(i,j) be the associated grey value, where C(i,j) €[0,255] $1 \leq i \leq M$, $1 \leq j \leq N$. The steps in the embedding algorithm are as follows:

```
Input:  Cover image
Output: Stego image
Step 1:  Read the cover image.
Step 2:  The cover image is divided into four 8 bit planes
         and the planes represents the grey code order
         (group 1:00, group2:01, group3:11, group4:10)
Step3:   Read the secret message stored in the file.
Step 4:  The secret message is binary encoded.
Step 5:  The binary values obtained in the above step is
         taken as input to the proposed algorithm.
         Step5.1: The binary values are grouped into 2 bits.
         step5.2: If the total number of bits to be
                  embedded is odd, then bit '0' is inserted at
                  the last otherwise no change is
                  performed.
         Step 5.3: Check to which grey code order the input
                  bits belongs to.
         step5.4: Change the 1st LSB bit of the
                  corresponding group, and the LSB's of
                  the remaining 3 groups are inverted.
         step5.5: If the bits are inserted till the last pixel
                  and the message to be hidden still exists
                  then the above procedure from step 5.3 is
                  followed for the 2nd and 3rd LSB bits.
Step 6:  Stego image is generated.
```

B. *Data Extraction Algorithm*

```
Input:  Stego image
Output: Secret data
Step 1:  Read the stego image.
Step 2:  The stego image is divided into four 8 bit planes
         and the planes represents the grey code order.
Step 3:  Identify the odd pixel and retrieve the 1st LSB
         positions for every four 8 bit plane.
Step 4:  Extract the group values based on the position.
Step 5:  The extracted bits are grouped to 7 bits and the
         corresponding decimal values are evaluated and
         these decimal values represent the ascii value of
         the secret message.
Step 6:  The secret data is extracted by converting the
         acsii to the corresponding characters.
```

C. *Experimental Results*

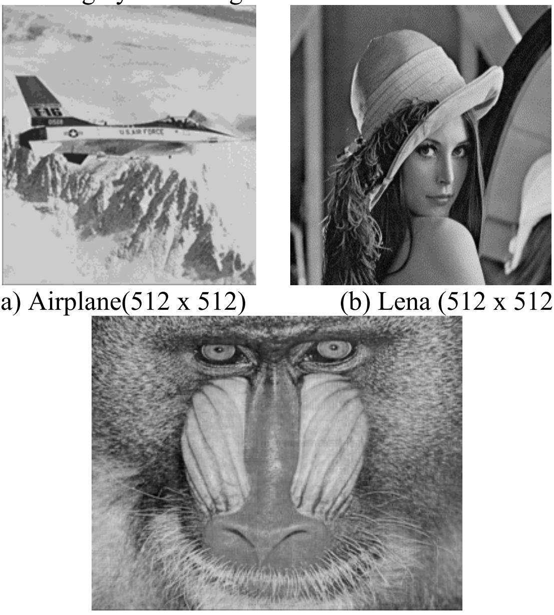
The proposed algorithm has been implemented using MATLAB. The performance of the methods have been evaluated and compared on the basis of following measures:

- Mean Squared Error (MSE)
- Structural Similarity Index(SSIM)

TABLE 1
MSE AND SSIM FOR GRAYSCALE IMAGES

Quality metrics	Capacity	Mean Squared Error	Structural Similarity Index	Root Mean Square Error	Structural Similarity Index	Peak Signal to Noise Ratio
AIRPLANE	393216	1.097652	0.957959	1.047689	0.957959	46.319407
LENA	393216	0.756470	0.976780	0.869753	0.976780	48.130804
BABOON	393216	0.804756	0.996525	0.897082	0.996525	48.130804

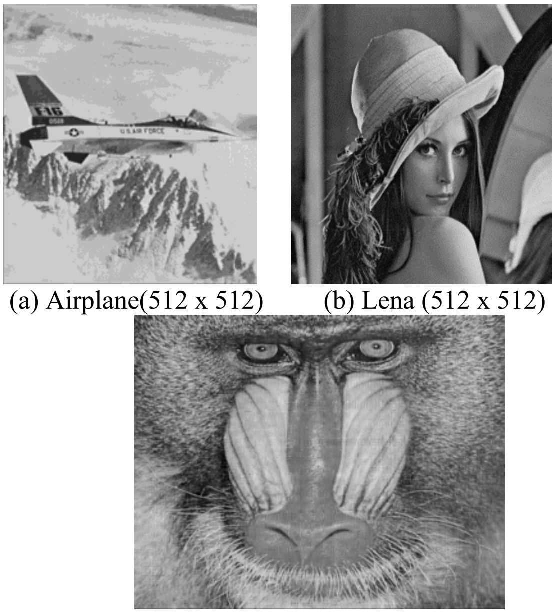
Fig. 2 (a) –(c) shows the original cover(carrier) images for Airplane, Lena, Baboon and Fig. 3 (a) –(c) shows the original stego images. The above measures are calculated for the test images by varying the number of characters embedded. Here the results of MSE and SSIM are shown in Table 1 for grayscale images.



(a) Airplane(512 x 512) (b) Lena (512 x 512)

(c) Baboon(512 x 512)

Fig. 2 (a) – (c) shows the original cover (carrier) images.



(a) Airplane(512 x 512) (b) Lena (512 x 512)

(c) Baboon (512 x 512)

Fig. 3(a) – (c) shows the stego images

III. PERFORMANCE ANALYSIS

A. Mean Square Error (MSE)

The Mean Squared Error (MSE) is a statistical measure of how far estimates or forecasts are from actual values. It is most often used in time series, but it is applied more where one set is “Original" and the other is a “Stego image”. In simple words MSE indicates average amount of modifications to the image. MSE is calculated by the following equation.

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(X_{j,k} - X_{j,k})^2$$

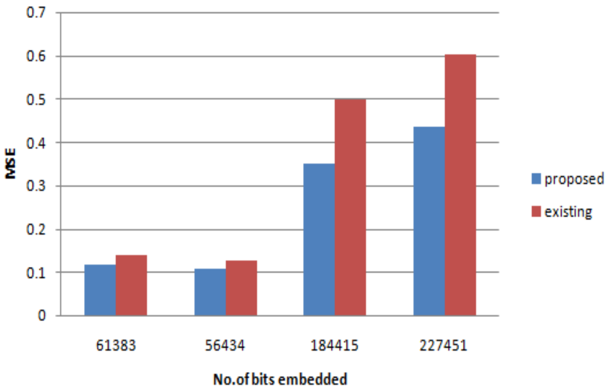


Fig. 4

B.Structural Similarity Index

The Structural Similarity (SSIM) Index is a method for measuring the similarity between two images. The SSIM index measures the image quality based on an initial uncompressed or distortion-free image as reference.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

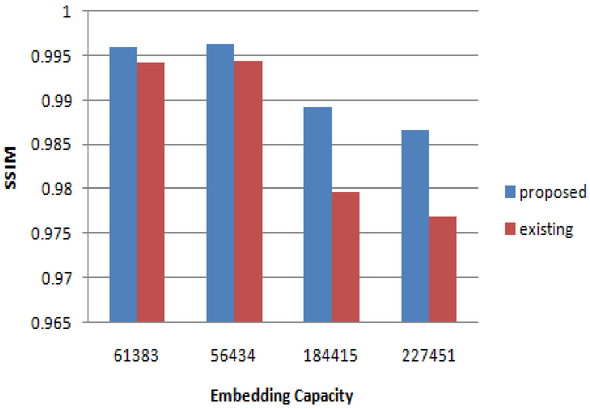


Fig. 5

IV. CONCLUSION

In the proposed LSBI algorithm 6 bits of data is embedded in every 4 pixels. Use of grey code standard to hide the secret data inside the cover medium forms a layer of security. From the results it can be observed that the proposed scheme works better when compared to the existing systems and high embedding capacity is achieved. This scheme can be applied to other covers like audio and video which can be taken as the future work.

REFERENCES

[1] C.H. Yang, C.Y. Weng, S.J. Wang, Member, IEEE and H.M. Sun, (2008) "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.

[2] K.H. Jung, K.J. Ha and K.-Y. Yoo, (2008) ,"Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. International Conference on Convergence and Hybrid Information Technology, ,Vol.2, pp. 355-358.

[3] S. Channalli and A. Jadhav, (2009), "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, Vol. 3, No. 3, pp. 245-269.

[4] H. Zhang, G. Geng and C. Xiong, (2009), "Image Steganography Using Pixel-Value Differencing", Second International Symposium in Electronic Commerce and Security, Vol. 2, pp. 109-112.

[5] Y. K. Jain and R. R. Ahirwal, (2010), "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security, Vol. 4, No. 1, pp 40-49.

[6] Rajkumar Yadav, (2011) , "A Novel Approach For Image Steganography In Spatial Domain Using Last Two Bits of Pixel Values", International Journal of Security, Vol.5, No. 2, pp. 51-61

[7] Vikas Tyagi, Atul kumar (2012), "Image steganography using least significant bit with cryptography", Journal of Global Research in Computer Science Vol. 3, No. 3, pp. 53-55.

[8] S. Shanmuga Priya, K. Mahesh and Dr.K. Kuppusamy,(2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications, Vol. 2, No. 3, pp. 2632-2637.

[9] Xing Tian Wang, Chin Chen Chang, Thai Son Nguyen and Ming-Chu Li, (2013), "Reversible Data Hiding For High Quality Images Exploiting Interpolation and Direction Order Mechanism" digital signal processing, Vol.23, No.2, pp. 569-577.

[10] Shabir A. Parah, Javid A. Sheik, Abdul .M. Hafiz, G.M. Bhat (2013), "Data hiding in scrambled images: A new double layer security data hiding technique", International Journal on Computers and Electrical Engineering, Vol. 40, No.1, pp.70-82.