Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 3, September 2019, pp.1405-1411
Available online at: http://pen.ius.edu.ba

PDA: A private domains approach for improved msb steganography image

Sura I. Mohammed Ali[1], Maryam Ghazi Ali[2], Lateef Abd Zaid Qudr[3]

[1,2] Department of mathematics & computer application, Collage of science /Al-Muthanna University
[3] Department of Computer Technology Engineering, Al Safwa University College, 56001 Karbala

Article Info

Received, 2019

Keyword:

Steganography,
Cover image,
Stego-image,
Most Significant Bit (MSB),
Peak Signal-to-Noise Rate
(PSNR).

ABSTRACT

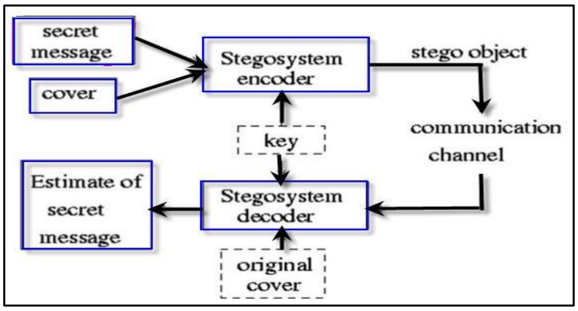
Steganography is one of the secure techniques of protecting data inside a cover object. Images are the most popular cover objects for Steganography. It provides secret message between users. The current paper presents an enhanced Most Significant Bit (MSB) technique. In this paper, a Private Domains Approach (PDA) is proposed; each domain consists of RGB of a pixel of cover image. Bit No.5 is applied to store the secret information in light of the bit that achieved highest steganography rate and the less probability of error rate.Consequently, this technique is allowing an improved version of MSB technique based on Mean-Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR). The experimental results show that our schemes perform well in terms of image quality. Generally; MSB technique produced the best stego-image quality in this paper.

Corresponding Author:

Sura I.Mohammed Ali
Department of mathematics & computer application,
Collage of science
Al-Muthanna University, Iraq.
Email: suraibraheem@mu.edu.iq

1. Introduction

Term of steganography is the method and technology of hiding data in approaches that prohibit revelation [3]. The secret text in cryptography is transformed into ciphertext, while the secret text in steganography stays the identical, but it is hidden in another layout of data. The intention of steganography is to avoid drawing suspicion to the existence of a hidden message. Steganography performs the central role in secret message communication [4]. A steganography framework comprises of three parts, classify as [1] secret data that will secure is pure text. Lid file in which data that hidden is: image, audio or video file, finally stego is merging of concept of secret data and lid file. The data is hidden by change undesirable bits in any types of cover files. The primary model of steganography is shown in Fig 1.



.

Fig 1. Basic Steganography Model [12]

Primary model of steganography includes of two algorithms, for both embedding, and extraction message [1]. The process of hiding includes the original file (cover) to secure stream data, is hidden, secret data, and password is a *key* for stego process. The original file and the secret data are called the *stego* object. The process of extraction is as a rule a simple process, it is an opposite of the stego process, where the secret data reveals ultimately. The approach of steganography image is one of the exceedingly accepted data hiding. A superior data-hiding technique need to be protecting from statistical and visible detection with providing secret message [2].

In this paper used image file as a cover to stego the secret information. The fewest difference of in the stego-image that used to hide huge data is considered the defiance of using steganography in images, and this information must have like features that located of the cover image. The term of Mean Squared Error (MSE) and the Peak Signal-to-Noise Ratio (PSNR) is used for Measure of image distortion between the original image and the stego image of hiding [13]. The decrease of MSE value and the higher of PSNR value will achieve better fineness of the image [3]. This paper is organized as: Section II displays approaches of image steganography. Section III provides popular approaches of steganography. Section IV describes the PDA approach. The experimental results of using PDA approach & discussion are shown in section V. Section VI present the conclusions of the paper.

2. Background and related work

There have been (more than two, but not a lot of) researches in embedding information inside an image using steganography way of doing things. Different ways of doing things have been presented in the domain of LSB stenographic ways of doing things. Each presented way of doing things has its advantage and disadvantage in of hiding signal to noise ratio (SNR) [17, 18]. In [5] compared different image steganography ways of doing things. The goals were to characterize the needed things of a good steganography set of computer instructions and to decide/figure out steganography ways of doing things that are good for various applications, some judging requirements for imperceptibility of a set of computer instructions were proposed. In [6] comparative study has been done between LSB and MSB technique and use gray-scale stego-image. LSB shows no distortion of the original image. Overall execution of LSB was better than of MSB.

In [7], a new approach for secure exchange of secret data among ends in a communication sitting is supplied; a secret key is the cover image. Each set content of 8 bits, then comparison with pixels of the cover image. The position of that pixel is transmitted if correspond with binary code of pixel. Securely splits between the two ends of communication of cover image.

RS Steganalysis in [8] based on the least significant bit plane to embedding secret massage, separating the image into disjoint groups of n adjacent pixels (x_1, ..., x_n) and an function that assigns areal number to order sets of pixels. The counts of the sets permit the estimation of a number embedding rate. Images that exclude steganography regularly have a characteristic percentage equal to 3%, while images including hidden data for the most part have a number hiding rates which reflects the amount of hidden data. In [19], bit complementation based way of doing things is indicated for hiding the information in images, using 4 bits for hide from bit 2 to bit 5 or its complement of cover image in each pixel and replace it with secret information bits. Steganography is depending on a decision of corresponding with the bits from bit 2 to bit 5 or its complement. In [16], a new method has been submitted; nine bits of message can be hidden in one pixel. Image color is comprises of three channels Red, Green, and Blue pixels in each pixel conations three bits of message hidden. One byte is used to represent character of forma ASCII value. The process of embedding is done by least significant bit (LSB) method. In this method, changes done two bit of each pixel. The change is only on the even columns of pixels that achieve higher security

3. Approaches of Steganography

There are public approaches for text embedding in images. These approaches are LSB insertion and MSB insertion. Insertion process of secret message is done in Least Significant Bit (LSB) or Most Significant Bit (MSB) of the image pixels. Then the stego image created is having a message which is hidden to human eye. Become of difference in the original image and stego image non-existent. The secret message is embed by using an algorithm and using reverse algorithm to extract secret message from stego image. Pixel's RGB of image color is represented with $\mathbf{b_i}$ where **b** is a bit, $\mathbf{i} \in \mathbf{[1,\dots, 8]}$ from low to high in case of LSB approach and from high to low in case of MSB approach **,** $\forall \mathbf{b_i} \in \mathbf{B}$ where **B** is a byte as shown in Fig 2.

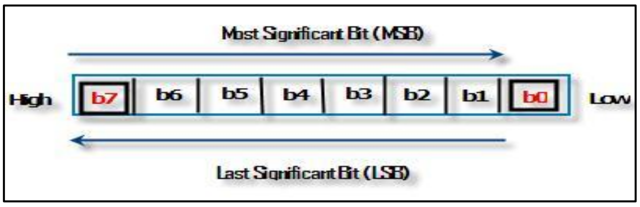


Fig 2. MSB and LSB information hiding algorithms

in literatures [10][11] is given MSB approach, embedding data in the Most Significant Bit (MSB) approach will affected very slight of the color value of pixels, so the most significant bit approach can be selected for information hiding. "1" or "0"value is covered up in image's pixels, the pixel should be prepared by renumbered it so the distinctive pixel value acquires a similar type of color in the palette [9].

A new approach is provided, which hide data in most significant bit approach. One of most significant bits that accomplished less rate error is provided in this paper.

4. Proposed Approach

In this paper, a Private Domains Approach (PDA) technique is presented; PDA is based on the MSB approach, which hides data in most significant bit of the image. Each domain consists of RGB of a pixel of cover image. Once we got the domains we needed randomly, then we can perform the process of hidden. The Private Domains are available at random based on image size. See Fig 3 that shows process of embedding.

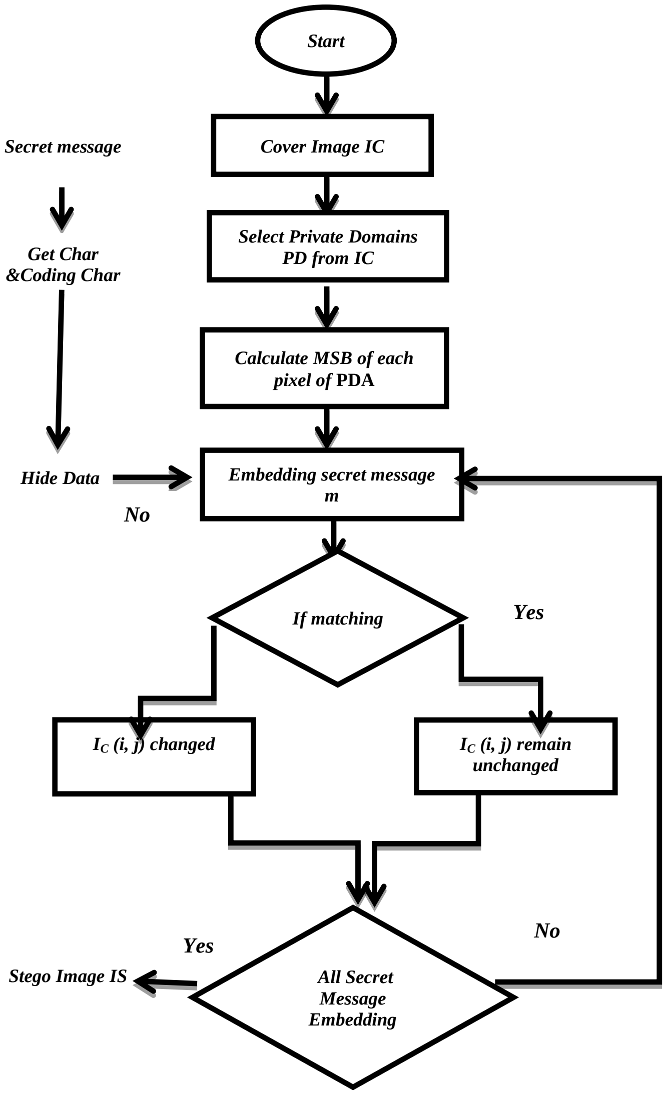

Start
Secret message
Cover Image IC
Get Char &Coding Char
Select Private Domains PD from IC
Calculate MSB of each pixel of PDA
Hide Data
No
Embedding secret message m
If matching
Yes
I_C (i, j) changed
I_C (i, j) remain unchanged
Yes
No
Stego Image IS
All Secret Message Embedding

Fig 3. Proposed Approach

However, a process of embedding is done by taking one of bits of Private Domains Approach (PDA). First, we will hide neither in Bit No. 5 or 6 or 7 or 8; the hiding may be in (Red, Green, or Blue) domain of the pixel and so on to insert the entire secret text. No.Bit has the highest steganography rate and the less probability of error rate is used for hiding secret information bits. According to the presented approach, the inputs of the cover image and the secret message are pre-processing; all bytes in the secret text are represented by its binary layout. After gives each char coding as the data is hidden in most significant bit.

The Algorithm of our approach is as follows:

Algorithm: Message embedding using MSB approach.
Input: Cover Image I_C, PDA, Secret Message M.
Output: Stego Image I_S.

Steps:

```
1: Read the $I_C$ and M that is to be hidden in the $I_C$.
2: Change M to binary, $M \in (0, 1)$.
3: Get each byte of hidden information from M, adjust it Byte hide, then get bits of Byte hide in role.
4: Get PDA of $I_C$
5: Calculate MSB of each pixel of PDA.
6: Replace MSB of PDA with each bit m of M one by one
     Where ($m \subseteq M$), m is the bit to be embedded
7: If MSB of PDA (i, j) is similar to m, $I_C$ (i, j) keep value unchanged.
8: Else: adjust the MSB of PDA (i, j) to m, (PDA (i, j)) subject of MSB of $I_C$ (i, j) of $I_C$, i = row, j = column pixel in the cover image.
9: Repeat step 5 until the whole M has been embedded in $I_C$.
10: Display $I_S$, where $I_S = (I_C + M)$.
```

V. The Performance Evaluation:

A. Experiments are executed with system: 2.27 GHz Intel (R) Core (TM) i3 CPU, 4 GB RAM and operating system windows 7, the coding language is visual basic 0.6 and bmp images that size (24 bit/pixel)
B- In this section, the suggested approach will be performed using private domains approach (PDA). We have managed variety experiments using variety images. ***Peak-Signal-to-Noise Ratio (PSNR)*** is used as performance measurement criteria, which is labelled under the variety image distortion metrics, is exercised on the Original and Stego images. The difference between two images measures by ***Mean-Squared Error (MSE)***. PSNR and MSE are summarized in equations 1, 2.

$$\text{MSE}= \frac{\sum M,N[I_C\,(i,j\,)- I_S\,(i,j\,)]^2}{M*N} \quad \textbf{………. (1)}$$

Where:

M, N= Measurements of the image.
*I_C **(i, j)** =the pixels in the original image(I_C).*
*I_S **(i, j)** =the pixels of the stego image (I_S).*

$$\text{PSNR}= 10log_{10}\frac{R^2}{MSE} \quad \textbf{…………... (2)}$$

Where, for color image R = 255. When MSE value is lower and PSNR value is higher, the better quality of the image is achieved. Several experiments were performed to evaluate our proposed approach. In this section, Table 1 represents the result of our method by using different position bits to be embedded and Private Domains Approach (PDA) as shown in cases 1, 2, 3, and case 4, cover image (Lana).

Table 1. An Example of the Proposed Algorithm Procedure

Cover Image	**PDA**	**m(bit to be embedded)**	steganography rate
Lena	Case1	**Bit 5**	**55%**
	Case2	**Bit 6**	**28%**
	Case3	**Bit 7**	**10%**
	Case4	**Bit 8**	**5%**

by depending on these rates we figure out that whenever we moving from bit to bit which has higher position for hiding in it, the steganography rate will decrease, because if we moving from bit to bit which has higher position the chance of error rate will became bigger, therefore the bit 5 has the highest steganography rate because it has the least position comparing to (bit 6, bit 7, bit 8).

We display Lena and Baboon images of stego-image for the experimental result with size 512×512×3 and 512×512×3 respectively, as show in Fig 4.

Fig 4. Original image

A stream of random bits is used as input of secret message. Fig. 5 displays the resultant stego images after applying suggested algorithm for the implementation.

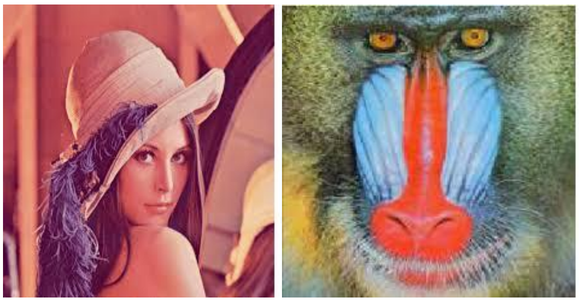


Figure 5. Stego image

In order to estimate the performance of the suggested approach, stego-images from the MSB and the proposed private domains approach were compared using MSE, PSNR. The result is tabulated in table I.

According to the experimental results, it is found that the proposed approach is supposed an effective Stenographic method in order to it satisfies the Stenographic system goals with high quality and PSNR value. A comparative study has been done among our approach with state of the art methods [14], that is used to store the secret bits based on the variation of bit No. 5 and 6 of cover image and [15] that hides the secret bits into the scaled up pixels by using stream data, it is found that our results are better. Table II is displaying the comparison of proposed approach for Baboon color image.

Table 2. PSNR and MSE for PDA

Cover Image	Proposed approach(PDA)	
	PSNR	**MSE**
Lena	**59.77155**	**6.85**
Baboon	**60.29828**	**0**

Table 4: Comparison of MSB Lena Color Image

Technique	PSNR
[14]	**44.6583**
[15]	**52.3438**
PDA	**59.77155**

The results approaching in Table 4 indicate that the proposed approach performed well in comparison with [14] and [15] techniques in terms of PSNR.

5. Conclusion

The proposed PDA an image stenographic approach based on MSB is presented. The approach uses all pixels' bits of MSB of the cover image and select **Bit. No5** has the highest steganography rate and the less probability of error rate for embedding. The proposed procedure is simple and easy to implement and depending on the domain values that are available random in the image.

To evaluate the proposed Stenographic approach, a comparative study has been done among our proposed approach. After comparative analysis appears the effectiveness of the proposed planner provides high PSNR.

References

[1] Z. Khan, M. Shah, M. Naeem, T. Mahmood, S.N.A. Khan, N. Amin, D. Shahzad, “Threshold based Steganography: A Novel Technique for Improved Payload and SNR”, International Arab Journal of Information Technology, vol. 13, No. 4, pp.380-386, 2016.

[2] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,”IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar.2006.

[3] O.Akinola, Adebanke A.Olatidoye," ON THE IMAGE QUALITY AND ENCODING TIMES OF LSB, MSB AND COMBINED LSB-MSB STEGANOGRAPHY ALGORITHMS USING DIGITAL IMAGES ", International Journal of Computer Science & Information Technology (IJCSIT) , Vol 7, No 4. , pp.79-91, August 2015.

[4] I. Al Barazanchi and H. R. Abdulshaheed, “Adaptive Illumination Normalization Framework based on Decrease Light Effect for Face Recognition,” *Jour Adv Res. Dyn. Control Syst.*, vol. 11, no. 01, pp. 1741–1747, 2019. [5] Kanzariya Nitin K. and Nimavat Ashish V. ,"Comparison of Various Images Steganography Techniques", International Journal of Computer Science and Management Research, Vol. 2, Issue 1, 2013.

[5] Rohit Garg and Tarun Gulati ,"Comparison of Lsb & Msb Based Steganography in Gray-Scale Images", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 8,2012.

[6] M. Islam, M. Shah, Z. Khan, T. Mahmood, M.J. Khan, “A New Symmetric Key Encryption Algorithm Using Images as Secret Keys” 13th IEEE International Conference on Frontiers of Information Technology, pp. 1-5, 2015.

[7] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color and gray-scale images,” IEEE MultiMedia, vol. 8, no. 4, pp. 22-28, October 2001

[8] Fu Bing, Zhou Xiansan," Information Hiding Technique in Most Significant Bit of Still Image", IEEE, 2009.

[9] R. Zhibin, S. Yongxin, Y. Yinghui and Y. Huai-jiang, “Study of the MSB information- hiding technique in a carrier image,” Optics and Precision Engineering, pp.182-185, Apr . 2002, (in Chinese).

[10] Z. Binglian and X. JieYong, “A kind of anti-cuts information hiding algorithm of MSB for spatial domain,” Computer Applications, pp138- 140, Dec. 2007, (in Chinese).

[11] A. A. Ali and A. H. Seddik, “New Text Steganography Technique by using Mixed-Case Font”, International Journal of Computer Applications, Vol. 62, No. 3, PP. 6-9, January 2013.

[12] N. J. Qasim and I. Barazanchi, “Unconstrained Joint Face Detection and Recognition in Video Surveillance System,” *Jour Adv Res. Dyn. Control Syst.*, vol. 11, no. 1, pp. 1855–1862, 2019.

[13] Y. Yalman, F. Akar, and I. Erturk, "An image interpolation based reversible data hiding method using R-weighted coding," IEEE 13th International Conference on Computational Science and Engineering, pp. 346-350, 2010.

[14] Z. Abdulelah Al-Sudani, S. Q. Salih, A. Sharafati, and Z. M. Yaseen, “Development of multivariate adaptive regression spline integrated with differential evolution model for streamflow simulation,” *J. Hydrol.*, vol. 573, no. 2, pp. 1–12, 2019.

[15] S. A. Raj and T. Soumya, “A Youthful Procedure for Spatial Domain Steganography”, Third International Conference on Advances in Computing and Communications, IEEE, PP. 300-303, 2013.

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

[17] A. S. Abdullah, M. A. Abed, and I. Al Barazanchi, “Improving face recognition by elman neural network using curvelet transform and HSI color space,” *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 430–437, 2019.

[18] Z. Khan, M. Shah, M. Naeem, D. Shahzad, T. Mahmood, “LSB Steganography using Bits Complementation”, International Conference on Chemical Engineering and Advanced Computational Technologies, Pretoria, South Africa, pp. 84-87, 2014.