# Image Steganography using Inverse Embedding Reversible Data Hiding Scheme

Subodh Karve
Computer Engg Department
DMCE, Airoli, Navi Mumbai

Vipul Dalal
Assistant Professor Computer Engg Department VIT, Wadala, Mumbai

## ABSTRACT
Image steganography is a technology that communicates the secret data by the carrier image. A quality data hiding scheme should hide huge secret data in the carrier without demeaning the quality of the carrier. This paper, discusses a high hiding capacity reversible data hiding scheme with low distortion.
It incorporates double-embedding strategy projected for storing secret data in carrier. The proposed scheme uses the inverse embedding method in thesecond embedding strategy to increase the hiding capacity and decrease the distortion at the same time for all type of images. The experimental results demonstrate that the proposed scheme performs well for embedding secret data into color image as well as gray scale images with desired characteristics of high hiding capacity and good stego image quality.

## General Terms
Steganography, Data Hiding, stego image

**Keywords** Double embedding,PSNR, MSE

## 1. INTRODUCTION

DATA HIDING [1] is referred to as a process to hide data, representing some information, into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out.In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications,such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying thisrequirement is referred to as *reversible*, *lossless*, *distortion-free*, or *invertible* data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

Obviously, most of the existing data hiding techniques are not reversible. For instance, the widely utilized spread-spectrum based data hiding methods (e.g., [2]–[5]) are not invertible owing to truncation (for the purpose to prevent over/underflow) error and round-off error. The well-known least significant bit plane (LSB) based schemes (e.g., [6] and [7]) are not lossless owing to bit replacement without "memory." Another category of data hiding techniques, quantization-index-modulation (QIM) based schemes (e.g., [8] and [9]), are not distortion-free owing to quantization error.

Most multimedia data embedding techniques modify, and hence distort, the host signal in order to insert the additional information. Often, this *embedding distortion* is small, yet irreversible, i.e. it cannot be removed to recover the original host signal. One of the earliest data embedding methods is the LSB (least significant bit) modification. In this well-known method, the LSB of each signal sample is replaced (over-written) by a payload data bit. During extraction, these bits are read in the same scanning order, and payload data is reconstructed.

Reversible data hiding [10, 11], also known as lossless data hiding, enables marked media to be restored to their original form without any distortion. This technique is applied in such fields as content authentication of multimedia data, law enforcement, medical imagery and astronomical research. Various reversible data hiding methods have been proposed for grayscale images.

With the development of the Internet, the security problems of the communication such as modification, forgery, duplication,interception are becoming more and more serious. There are various modern cryptosystems [19] that can be used to encrypt the data before the transmission to keep the data confidential in the Internet. However, the meaning-less form of the encrypted data can be got attention by the adversary. Data hiding is the technique to solve this problem. Data hiding is a general term encompassing a wide range of problems beyond that of embedding messages in content. The term hiding here can refer to either making the information imperceptible or keeping the existence of the information secret [16]. The content can be any general digital format, such as text, image, audio, video, etc. In the case of image, the image that is used to carry the secret data is referred to as the cover image and the image that carried the secret data is referred to as the stego image usually. To send

the secret data, the sender embeds the secret data into the cover image by modifying the pixel value to get the stegoimage at first, and then sends the stego image to the receiver.

After the receiver receives the stego image, the secret data can be extracted from it. By this way, the secret data can be transferred in high-level security. The secret data also can be encrypted by some encryption methods such as AES or DES before the embedding to achieve a more rigoroussecurity.Reversible data hiding is a technique that not only embeds data into cover images, but also restores the cover images from the stego image after the secret data have been extracted [12]. This is necessary in some extremely important images that cannot allow any distortion such as military images or medical images. On the other side, if the data hiding scheme is reversible, the hiding capacity can be increased by taking the stego image as the cover image to embed more secret data again, which is also called multi-layer embedding method. This is an effective way to increase the hiding capacity. There are many reversible data hiding schemes were proposed recently, and most of them use one of these three kinds of technique [14]: (1) loss-less compression technique [13, 15]; (2) difference expansion technique [20]; (3) histogram shifting technique [18].

A good data hiding scheme should have a high hiding capacity and a perfect image quality. The hiding capacity should be as high as possible under the condition that cannot be distinguished by human vision. In this paper, an inverse embedding method in the second embedding strategy is used to increase the hiding capacity and decrease the distortion at the same time. The experimental results demonstrate that the proposed scheme achieves very good performance in both the quality of stego image and the hiding
capacity. The rest of this paper is organized as follows. In Section 2, some reversible data hiding schemes are reviewed. The proposed scheme is described in Section 3 and the experimental results of the proposed scheme will be discussed in Section 4. Finally, Section 5 is the conclusion of this paper.

## 2. ALLIED WORK

In 2003, Tian [18] proposed a reversible data hiding scheme using a difference expansion (DE) which embeds1 bit secret data in one pixel pairs of the cover image. In the embedding phase, the integer average m and the difference value d of a cover pixel pair (x, y) are calculated by $m = \lfloor (x + y)/2 \rfloor$ and $d = x - y$ firstly, where the notation $\lfloor x \rfloor$is the floor function meaning the greatest integer less than or equal to x. Secondly, the secret bit b is embedded into d by the difference expansion operation to obtain the new difference value $d'$ as follows $d' = 2d + b$. Finally, the stegopixel pair $(x', y')$ is calculated by $x' = m + \lfloor (d'+1)/2 \rfloor$, $y' = m - \lfloor d'/2 \rfloor$.

In the extraction phase, the integer average $m'$ and the difference value $d'$ are calculated by $m' = \lfloor (x' + y')/2 \rfloor$ and $d' = x' - y'$ at first. Secondly, the embedded secret bit is extracted by $b = LSB(d')$, where LSB(x) is the function taking the least significant bit of x. Finally, the original difference value is calculated by $d = \lfloor d'/2 \rfloor$, and the cover pixel pair (x, y) is restored by $x = m' + \lfloor (d + 1)/2 \rfloor$ and $y = m' - \lfloor d/2 \rfloor$.

In DE scheme, the maximum hiding capacity is no morethan 0.5 bpp, but the visual quality is not very well. In2009, DucKieu [17] proposed a new reversible data hidingscheme with good stegoimage quality and high payload by using the multiple embedding strategy to improve the image quality and the embedding capacity of DE method. In DucKieu's scheme, the horizontal and vertical embedding rules are used to embed the secret data, and the LSB replacement method is used to embed the compressed location maps.The experimental result shows that DucKieu's scheme iscapable of achieving a good visual quality of stego images and a high embedding capacity especially when multiplelayers embedding is performed. In this paper, a reversible data hiding scheme with a higher hiding capacity and a lower distortion by using the inverse embedding methods in the double-embedding strategies is proposed.

## 3. PROPOSED SCHEME

Reversible data hiding scheme [21] proposed is useful for 8 bit gray scale images. The scheme proposed here is applicable for any type of image and applied for 8-bit to 32-bit images. The proposed scheme

The steps for embedding phase are as follows.
1) Prepare the Secret data to be hidden such that each letter or
pixel is represented interms of 32 bits.
2) Get R, G, B components of cover image and store them in two dimensional matrices namely ir,ig,ib.
3) Get the storage capacity of ir, ig,ib as follows.
a) Let (i, j) be a position in cover image irand rc is the capacity count of ir.
for i varies from 0 to h and j varies from 1 to w if ir(I,j+1) is even then rc=rc+1.
This becomes hiding capacity for phase one of embedding.
b) Same way capacity for phase two can be added to rc by considering ir (i, j+1) to be odd.
c) Thus now rc represents hiding capacity of ir.
d) Following steps a,b,c for ig, get hiding capacityi.e. of ig.
e) Following steps a,b,c for ib, get hiding capacity i.e. of ib.
f) Total hiding capacity is tc= rc+gc+bc.
4) Capacity of data to be hidden is checked with tc.Thus hiding is possible only with tcis not less than data to be hidden.
5) Secret Data is splitted into 3 parts sr,sg,sb such that sr can be hidden ir, sg in ig and sb in ib.
6) Embedding takes place in two phases by following steps.

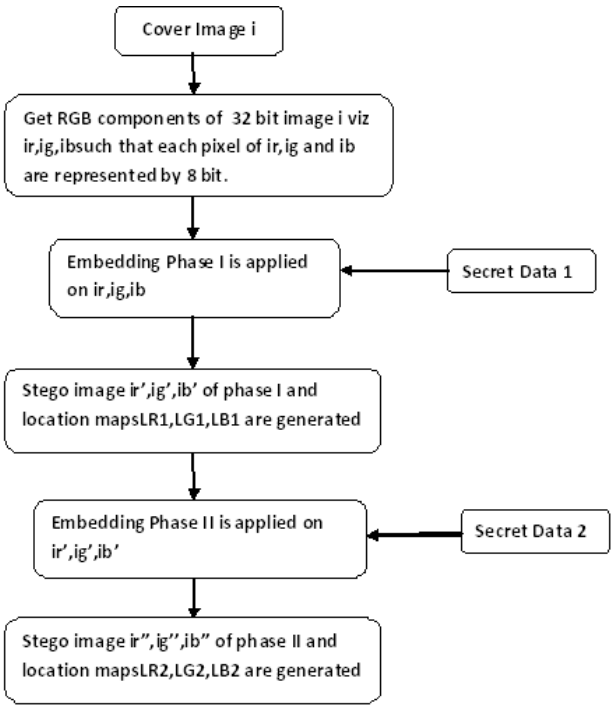


**Figure1: Embedding Phase of the Scheme**

**7) Embedding phase I**

Let ir be cover image with size M × N, and (i, j) be the pixel located on row i, column j in image ir, where $0 \le i \le M-1$, $0 \le j \le N-1$ . ir' is the stego image and its size is the same as the size of ir. The secret data is denoted by sr, sr = sr0sr1sr2 · · · srL−1, wheresrk ∈ {0, 1}, $0 \le k \le L-1$ and L is the length of Sr. The steps in the embedding phase are listed as follows:

Input: Cover image ir, secret data sr.

Output: Stego image ir', location maps LR1 and LR2.

Step 1: Set the initial location map $LR1_{i,j/2} = 0$, $0 \le i < M$, $0 \le j/2 < N/2$ and scan the image I to get the first pixel pair ($ir_{i,j}$, $ir_{i,j+1}$), i = j = 0.

Step 2: Select the even pixel value to embed the secret data:

(7.1) If $ir_{i,j+1}$ is odd, then set $ir'_{i,j} = ir_{i,j}$ , $ir'_{i,j+1} = ir_{i,j+1}$, and if j = N −2, then set i = i+1 and j = 0,otherwise update j by j+2, then get the next pixel pair($ir_{i,j}$, $ir_{i,j+1}$) and go to Step 2;

(7.2) If $ir_{i,j+1}$ is even, this pixel pair can be used to embed the secret data, then set $ir'_{i,j} = ir_{i,j}$ , and go to 7.3.

(7.3) Set the location map $LR1_{i,j/2} = 1$, and embed the secret bit by the following equation:

$Ir'_{i,j+1} = ir_{i,j+1}$ if $sr_k = 0$

$Ir'_{i,j+1} = ir_{i,j+1} + 1$ if $sr_k = 1$

If i = M − 1 and j = N − 2, go to Step 4; otherwise if j = N − 2, then set i = i + 1 and j = 0, otherwise update j by j + 2, then get the next pixel pair($ir_{i,j}$, $ir_{i,j+1}$) and go to Step 2.

(7.4) Set the initial location map $LR2_{i,j/2} = 0$, $0 \le i < M$, $0 \le j/2 < N/2$ and scan the image ir'to get the first pixel pair ($ir'_{i,j}$, $ir'_{i,j+1}$), i = j = 0.

8) Embedding phase II

(8.1)Select the odd pixel value to embed the secret data:

If $ir'_{i,j+1}$is even, then set $ir''_{i,j} = ir'_{i,j}$, $ir''_{i,j+1} = ir'_{i,j+1}$, and if j = N −2, then set i = i+1 and j = 0,otherwise update j by j+2, then get the next pixel pair($ir'_{i,j}$, $ir'_{i,j+1}$) and go to 8.1;

(8.2) If $ir'_{i,j+1}$is odd, this pixel pair can be used to embed secret, then set $ir''_{i,j} = ir'_{i,j}$, and go to 8.3.

(8.3)Set the location map $LR2_{i,j/2} = 1$, and embed thesecret bit by the following equation:

$ir''_{i,j+1} = ir'_{i,j+1} - 1$ if sk = 0

$ir''_{i,j+1} = ir'_{i,j+1}$ if sk = 1

If i = M − 1 and j = N − 2, go to Step 9; otherwise

if j = N − 2, then set i = i + 1 and j = 0, otherwise update j by j + 2, get the next pixel pair ($ir'_{i,j}$, $ir'_{i,j+1}$) and go to 8.1.

9) Output the stego image ir'' and the location maps LR1 and LR2.

10) Steps 1 to 7 are applied for ig to produce stego image ig'' and location maps LG1 and LG2

11) Steps 1 to 7 are applied for ib to produce stego image ib'' and location maps LB1 and LB2.

12) ir'',ig'',ib'' are merged to produce final stego image i''.Location maps LR1, LR2, LG1, LG2, LB1, LB2 are merged together to produce location maps L1 and L2. Thus steps taken in figure1helps generate final stego image and location maps.

**Extraction phase I to retrieve secret data**

Input: Stego image ir″, location map LR1 and LR2.

Output: Cover image ir, secret data sr.

1)Scan the image ir'' to get the first pixel pair($ir''_{i,j}$ ,$ir''_{i,j+1}$),i=j= 0.

2)If $LR2_{i,j/2} = 0$, then $ir'_{i,j} = ir''_{i,j}$and $ir'_{i,j+1} = ir''_{i,j+1}$ if j = N −2, then set i = i+1 and j = 0, otherwise updatej by j+2, then get the next pixel pair ($ir''_{i,j}$ ,$ir''_{i,j+1}$) and go to Step 2.If $LR2_{i,j/2} = 1$, then this pixel pair contains the secret data, go to 3).

3)(3.1)If $ir''_{i,j+1}$is even, extract the secret data $sr_k = 0$,and reconstruct the cover image by the following equation:

$ir'_{i,j+1} = ir''_{i,j+1} + 1$

(3.2)If $ir''_{i,j+1}$is odd, extract the secret data $sr_k = 1$,and reconstruct the cover image by the following equation:

$ir'_{i,j+1} = ir''_{i,j+1}$. If i = M − 1 and j = N − 2, go to Step 4; otherwise

if j = N − 2, then set i = i + 1 and j = 0, otherwise update j by j + 2, get the next pixel pair ($ir''_{i,j}$ ,$ir''_{i,j+1}$) and go to Step 2.

4)Scan the image ir'to get the first pixel pair ($ir'_{i,j}$ ,$ir'_{i,j+1}$),i=j=0.

5)If $LR2_{i,j/2} = 0$, then $ir_{i,j} = ir'_{i,j}$, $ir_{i,j+1} = ir'_{i,j+1}$, if j = N −2, then set i = i+1 and j = 0, otherwise update j by j+2, and get the next pixel pair ($ir'_{i,j}$,$ir'_{i,j+1}$)and go to Step 5;If $LR2_{i,j/2} = 1$, then this pixel pair contains the secret data, go to 6).

6)Extraction phase II to retrieve secret data

(6.1) If $ir'_{i,j+1}$is even, extract the secret data $sr_k = 0$, and reconstruct the cover image by the followingequation:

$$\mathbf{ir_{i,j+1} = ir'_{i,j+1}}$$

(6.2) If $ir'_{i,j+1}$is odd, extract the secret data $sr_k = 1$, and reconstruct the cover image by the following equation:

$$\mathbf{ir_{i,j+1} = ir'_{i,j+1} - 1}$$

If i = M − 1 and j = N − 2, go to Step 7; otherwise if j = N − 2, then set i = i + 1 and j = 0, otherwise update j by j + 2, get the next pixel pair ($\mathbf{ir'_{i,j}}$,$\mathbf{ir'_{i,j+1}}$)and go to Step 5.

7) Output the reconstructed cover image I&the secret data sr.

8) Steps 1 to 7 are applied for ig'' to produce secret data sg.

9) Steps 1 to 7 are applied for ib'' to produce secret data sb.

10) Combine sr, sg, sb to get secret data s either text or image. Thus steps taken in figure2 helps generate cover image and secret data.

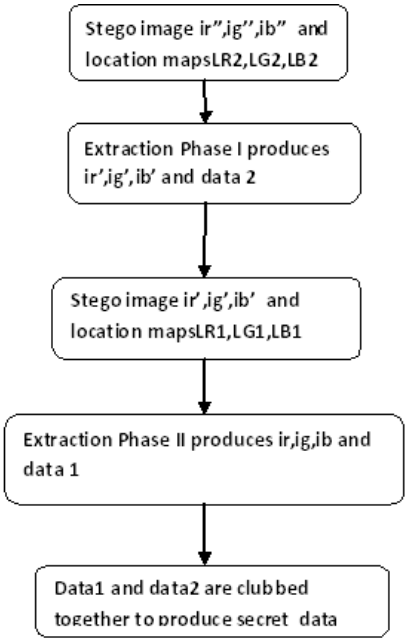


**Figure 2: Extraction Phase of the Scheme**

## 4. RESULTS

To evaluate the proposed scheme various parameters like PNR value, storing capacity are considered. The various image types like png, jpg, bmp are considered for testing. Images with different sizes are used to evaluate various parameters

Peak signal to noise ratio(PSNR) is used measure the distortion in stego image with respect to cover image.PSNR is defined by following equation:

PSNR=10 x log ( $(16777216)^2$/MSEa)

MSEa is adjusted Mean square error between stego and cover images.MSEa is defined by following equation:MSEa=MSE/3 and MSE is Mean square error between stego and cover images defined by following equation:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x_{i,j} - x'_{i,j})^2$$

wherexi, jand x'i,jrepresent the pixel values of the coverimage and the stego image, respectively.

Table1: Observed PSNR values

| Image | Type | Size | Grayscale | psnr |
|---|---|---|---|---|
| lena | png | 54.7kb | yes | 54.78933 |
| Baboon | png | 332kb | no | 57.50333 |
| Bluehills | jpg | 10.8kb | no | 56.55 |
| Bluehills1 | jpg | 23.3.kb | no | 59.42 |
| Water lilies | bmp | 432kb | no | 57.50333 |

Results showed in table1 indicate that proposed scheme works for grayscale as well as colored images of any type. Due to inverse embedding, the hiding capacity increases.

## 5. CONCLUSION

This paper proposes a reversible data hiding scheme usingthe inverse embedding methods in the double-embeddingstrategies. The proposed scheme increasedthe hiding capacity and decreased the distortion of the stegoimage by using the inverse embedding method in the secondembedding strategy. The distortion which produced in thefirst embedding strategy can be balance out in the inverseembedding method. The experimental results demonstratedthat the proposed scheme achieved very good performancein both the quality of stego image and the hiding capacity. The scheme works for grayscale and color images of any type.

## 6. REFERENCES

1] W. Zeng, "Digital watermarking and data hiding: technologies and applications,"in Proc. Int. Conf. Inf. Syst., Anal. Synth., vol. 3, 1998, pp.223–229.

[2] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[3] A. Z. Tirkel, C. F. Osborne, and R. G. Van Schyndel, "Image watermarking- a spread spectrum application," in Proc. IEEE 4th Int. Symp. Spread Spectrum Techn. Applicat., vol. 2, Sep. 1996, pp. 785–789.

[4] J. Huang and Y. Q. Shi, "An adaptive image watermarking scheme based on visual masking," Electron. Lett., vol. 34, no. 8, pp. 748–750, 1998.

[5] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding image watermarks in DC component," IEEE Trans. Circuits Syst.: Video Technol., vol. 10, no. 6, pp. 974–979, Sep. 2000.

[6] J. Irvine and D. Harle, Data Communications and Networks: An Engineering Approach. New York: Wiley, 2002.

[7] M. M. Yeung and F. C. Mintzer, "Invisible watermarking for image verification," Electron. Imag., vol. 7, no. 3, pp. 578–591, Jul. 1998.

[8] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.

[9] F. Perez-Gonzlez and F. Balado, "Quantized projection data hiding," in Proc. IEEE Int. Conf. Image Process., vol. 2, Sep. 2002, pp. 889–892.

[10] M. Awrangjeb, "An overview of reversible data hiding," in Proceedings of International Conference on Computer and Information Technology, 2003, pp. 75-79.

[11] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: fundamentals, algorithms and applications," in Proceedings of IEEE International Symposium on Circuits and Systems, Vol. II, 2004, pp. 33-36.

[12]A. M. Alattar. Reversible watermark using the difference expansionof a generalized integer transform. IEEE Transactions

on Image Processing, 13(8):1147–1156, 2004.

[13] M. U. Celik, G. Sharma, a. Murat Tekalp, and E. Saber. Reversibledata hiding. Proceedings of the International Conferenceon Image Processing, II:157–160, 2002.

[14] J. Feng, I. Lin, C. Tsai, and Y. Chu. Reversible watermarking:Current status and key issues. International Journal ofNetwork Security, 2(3):253–266, 2006.

[15] J. Fridrich, M. Goljan, and R. Du. Lossless data embedding – new paradigm in digital watermarking. EURASIP Journal on

Applied signal Processing, 2002(2):185–196, February 2002.

[16] I. J.Cox, M. L.Miller, J. A.Bloom, J. Fridrich, and T. Kalker. Digital Watermarking and Steganography. Morgan Kaufmann Publishers, MA, 2007.

[17] D. Kieu and C.-C. Chang. A high stego-image qualitysteganographic scheme with reversibility and high payloadusing multiple embedding strategy. Journal of System andSoftware, 82(10):1743–1752, October 2009.

[18] Z. Ni, Y. Shi, N. Ansari, and W. Su. Reversible data hiding.

IEEE Transactions on Circuits and Systems for Video Technology,16(3):354–361, 2006.

[19] W. Stallings. Cryptography and Network Security: Principlesand Practice. Pearson Education, New Jersey, 2003.

[20] J. Tian. Reversible data embedding using a difference expansion.IEEE Transactions on Circuits and Systems for VideoTechnology, 13(8):890–896, August 2003.

[21]Lin Jia and Kee-Young Yoo." A reversible data hiding scheme using inverse embedding methods indouble-embedding strategies"