ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

IMPROVED LOSSLESS DATA HIDING SCHEME USING HISTOGRAM OF ADJACENCY PIXEL DIFFERENCE

R Anushiadevi*, Kolluri Chennakesava Vinay, Majety B V S K Sita Ram,
Katta Bala Anil Kumar, Katti Krishna Murthy
School of Computing, Sastra University, Thanjavur, TamilNadu.
Email: thambivv@gmail.com

Received on 09-08-2016 *Accepted on 05-09-2016*

Abstract

There have been discussed several data hiding techniques in an image which can embed the data in secret manner. However, after extracting the data from animage, theoriginal image information cannot be recovered. It is an important issue to have a lossless data hiding scheme which can recover the original image without any loss after extracting the secret data. In this paper, a novel based idea is introduced for lossless data hiding using adjacencypixel difference.In this method, we can obtain good amount of security and good amount of data hiding capacity.

Keywords: Information Security**,** Lossless data hiding, Reversible data hiding.

1. Introduction

Invertible data secreting is a highly protected technology to implant clandestine data into host picture indiscernibly and enable the host picture to be regained without any fault upon extraction of the implanted clandestine data which gives additional information to the embedded data. This technology is used in digital watermarking techniques where clandestine data and the image are very important. Many reversible data hiding methodologies were developed in recent years.

Difference between two adjacent pixels is used to embed data indifference expansion method [1-3].To improves the performance of reversible data hiding various technologies have been introduced in [4-6]. In order to increase the information security, Zhang proposed the lossless data hiding technique in an encrypted image[7] [8]. In [9] separable lossless data hiding is introduced. Sorting and prediction method is used for Lossless Watermarking algorithm in [10].Ni et al's [11] scheme introducing a newembedding mechanism, which increases the data embedding capacity.In [12] [13] describes about PVD steganalysis to embed the data.[14],[15] gives the idea of lossless data retrieval with high data embedding mechanism.

2. Proposed Scheme

An efficient reversible data hiding method is proposed using Steganography. Here adjacency pixel difference is used for embedding. Neighboring pixel in an image is highly correlated. Hence maximum adjacency pixel difference is nearly zero, one, two, and three. Let us consider' as the difference between the adjacent pixels and add 'n' with each difference which have value of 'd=0,1,2,3' ,as shown in step 2 below, where 'n' value is of two bits embedding in each pixel at third and fourth position. The embedded bits in corresponding pixel positions are inserted into image and is send to the receiver .In some cases the value of 'd' may be greater than three, so in that case,we create a file which contains the embedding pixel position, that is the position of pixel to those 'n' is added is saved into the file. The corresponding image fileissending to the receiver. The receiver then uses the file to know the location of pixels where the bits are added and retrieve the secret bits in the third and fourth position of the pixel. The remaining bits value is added to previous value to obtain the corresponding pixel value.

Input: Cover image and hexadecimal secret message

Output: Stego image.

Step 1:

Construct Cover image P.

Step 2:

Calculate the difference between the adjacent pixels.

$$d_i = \begin{cases} p_i, \ if i = 0 \\ |p_{i-1} - p_i|, \ otherwise \end{cases}$$

Step 3:

If the difference is 0,1,2,3 then we insert secret data into those pixels.

Step 4:

After inserting the secret message in the appropriate pixel position it is then send to the receiver.

The process of embedding and extracting of data into an image is shown in 2.1 and 2.2 respectively.

2.1 Embedding algorithm:

Perform the operation for all pixels after the above procedure is done

1 if(difference between the adjacent pixels is 0 or1or 2or 3)

1.1 d= covert the difference in the binary

1.2 P=Get the original pixel value

1.3 While (length of p is less than 8)

1.3.1 Make its length to 8 by concatenating the ‘0’ in the front

1.3.2 K=concatenate (first four pixels of the original pixel, secret data two bits and d value)

1.3.3 Sp=finally convert the binary value into an integer and store it in the image

1.3.4 After inserting the data just mark that position as 1

2 Else

2.1 If data is not inserted then keep that position as 0.

2.2 Extracting Algorithm:

1 While (j<=s.length ())//where s is the bit map

1.1 s5=store the bit map value of the current position;

1.1.1 If (bit map value is 1 then retrieve that pixel from it)

1.1.1.1 s2=store the current pixel value in it in binary format;

1.1.2 While (s2 length is less than eight)

1.1.2.1 s2=pad the zeros in front of the pixel;

//This loop continues until the length is equal to eight

1.1.3 s1=store the last two bits of the pixels

1.1.4 n=convert that value into integer value

1.1.5 s3+=store the secret data from the s2 at specified portion

1.1.6 coverpixel_bit[j]=subtract that value n from the previous pixel

inorder to get the original pixel value

1.2 Increment the count (j) value

3. Experiment Result:

The result of proposed scheme is compared with Wang'et al.'s scheme in order to verify the hiding capacity (bits) and image distortion (PSNR). The image distortion is measuredusing PSNR. The definition of PSNR is as follows:

$$PSNR = 10 * \text{Log}_{10}((MAX)^2/(MSE))$$

The above equation is measured in log units, determined by the ratio of MAX^2 and MSE.

MSE is defined:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where I(i, j) and K(i,j) represent pixel values of the cover-image and the stego-image of size M x N. The hiding capacity is measured by bits. The proposed scheme compared with Wang et al 's scheme as shown in Table I. The Fig.1(a) represents lena ,where data is embedded into it and is shown in Fig.1(b) and is called as stego image. The image after retrieving data is called as retrieved image and is shown in Fig.1(c).The corresponding histograms of lena are shown in Fig.2(a),(b),(c).Similarly, all the original images ,stego images and retrieved images with their corresponding histograms are shown below.

Table I: **The comparison between Proposed and Wang et al.'s scheme.**

Test Image	Wang et al.'s scheme		Proposed Scheme	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Lena	142,003	51.7166	154,898	39.0476
Jet	147,351	51.4937	213,108	38.1506
Boat	146,564	49.8144	158,430	38.9514
Zelda	137,284	51.4598	150,900	39.4318
Tiffany	142,684	51.7558	180,658	38.6528
Average	145,306	51.0082	175,478.66	38.7165

Fig.1(a) Original Lena (b) Stego Lena(c) Recovered Lena

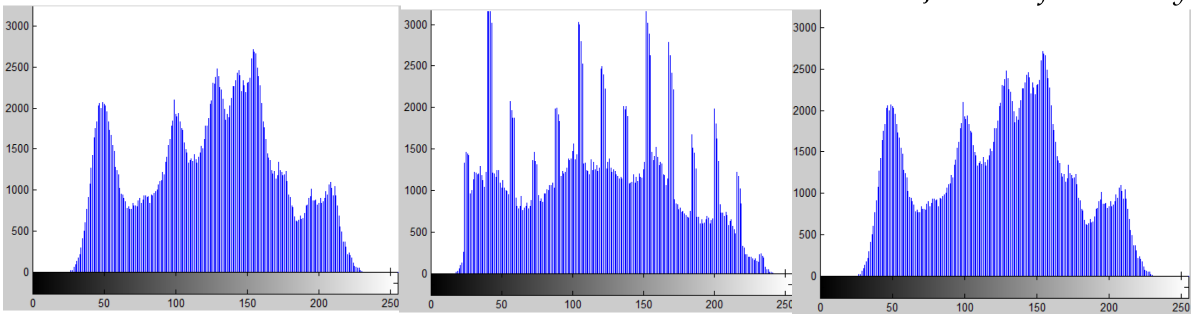

Fig.2(a)Histogram of original Lena(b) Histogram of Stego Lena(c) Histogram of Recovered Lena.

Fig.3(a) Original Jet (b)Stego Jet (c) Recovered Jet

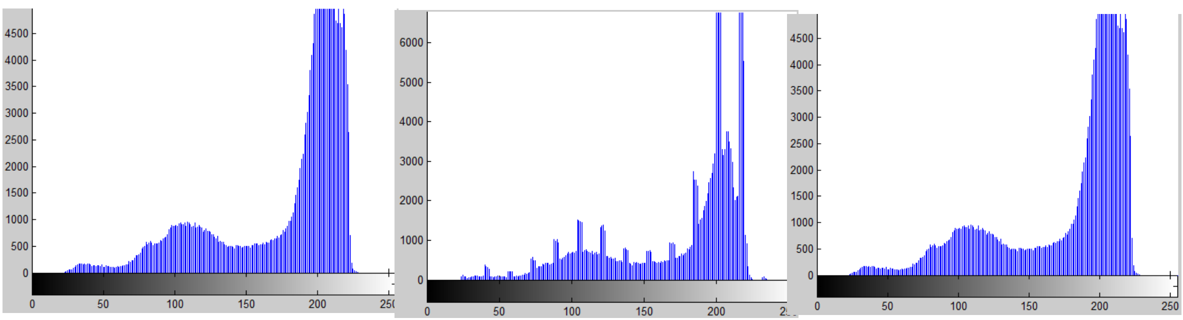

Fig.4(a)Histogram of original Jet(b) Histogram of Stego Jet(c) Histogram of Recovered Jet

Fig.5(a) Original Boat (b)Stego Boat (c) Recovered Boat

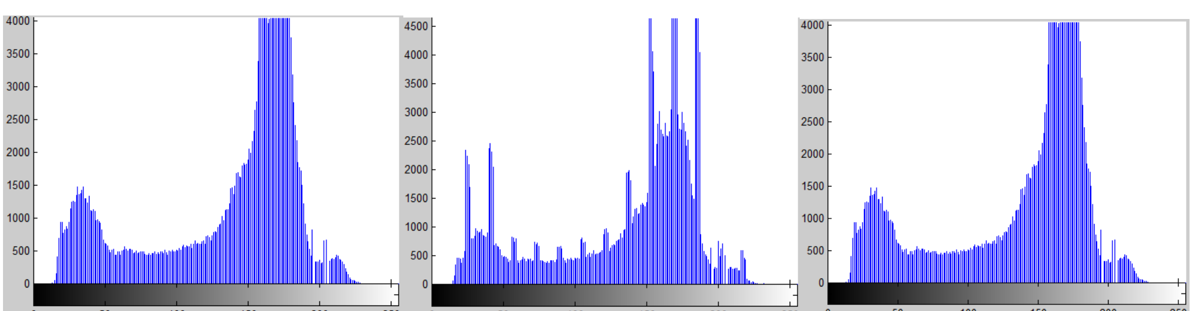

Fig.6(a)Histogram of original Boat(b) Histogram of Stego Boat(c) Histogram of Recovered Boat

Fig.7(a) Original Zelda (b)Stego Zelda (c) Recovered Zelda

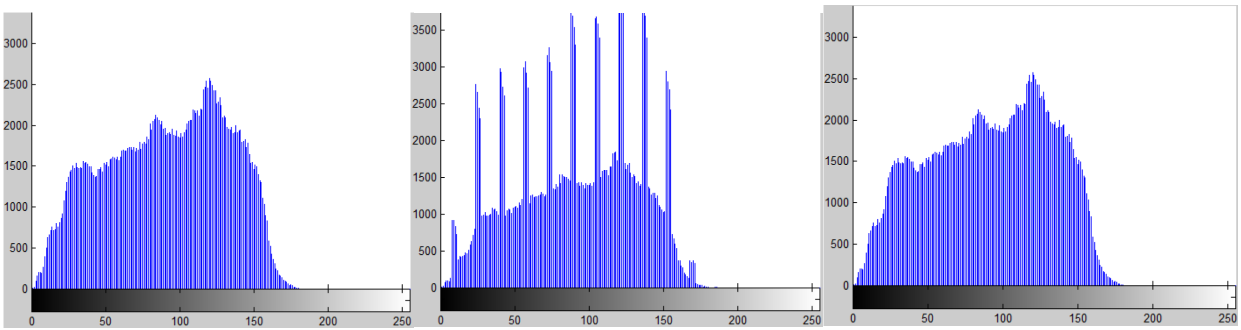

Fig.8(a)Histogram of original Zelda(b) Histogram of Stego Zelda(c) Histogram of Recovered Zelda

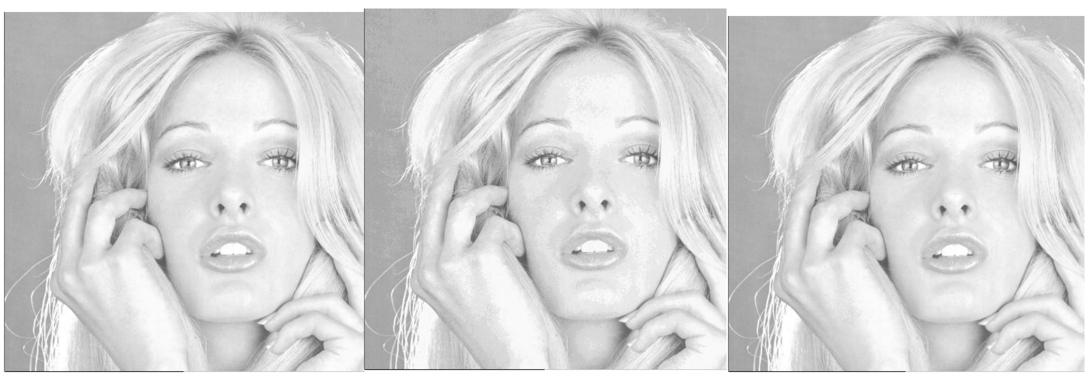

Fig.9(a)Original Tiffany(b)Stego Tiffany(c) Recovered Tiffany

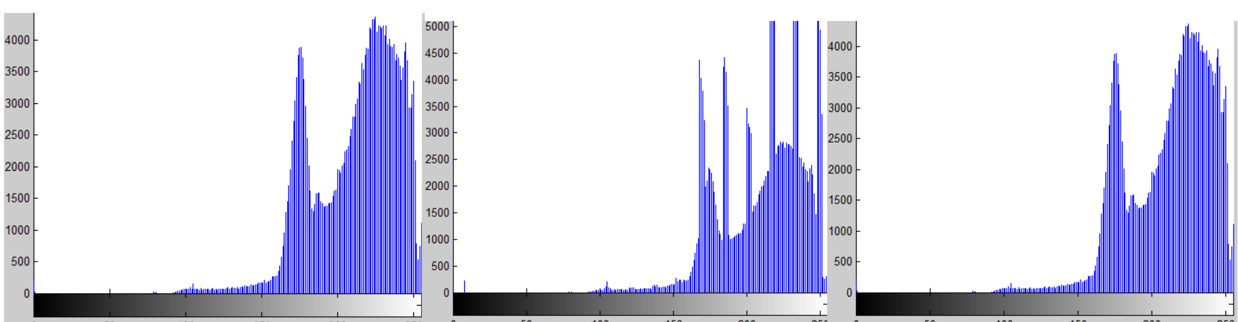

Fig.10 (a)Histogram of original Tiffany(b)Histogram of StegoTiffany(c) Histogram of Recovered Tiffany.

4. Conclusion:

This paper gives us an overall view about the reversible data hiding technique using steganography .This can be achieved by calculating the difference between two adjacent pixels. This is a lossless data and image retrieving technique. We can embed more amount of secret data when compare to the older ones. This technique is successfully compiled and executed using jdk1.8. In the years to come, this powerful algorithm will find a wide range of applications. One such instance is the direction of video sequences where each sequence can be separated into single frames. In each frame, we can apply the same lossless data hiding technique and combine those frames to get the original.

5. References:

1. J. Tian, "Reversible data embedding using a difference expansion,"*IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896,Aug. 2003.

2. Zhang, T., Li, W., Zhang, Y., Zheng, E., Ping, X. Steganalysis of LSB matching based on statistical modeling of pixel difference distributions (2010) Information Sciences, 180 (23), pp. 4685-4694.

3. Steganalysis by subtractive pixel adjacency matrix,(2010) IEEE Transactions on Information Forensics and Security, 5 (2), art. no. 5437325, pp. 215-224.

4. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible imagewatermarking using interpolation technique," *IEEE Trans. Inf. ForensicsSecur.*, vol. 5, no. 1, pp. 187–193, 2010.

5. W. Hong, T.-S.Chen, Y.-P.Chang, and C.-W.Shiu, "A high capacityreversible data hiding scheme using orthogonal projection and predictionerrormodification," *Signal Process.*, vol. 90, pp. 2911–2922, 2010.

6. C.-C. Chang, C.-C.Lin, and Y.-H. Chen, "Reversible dataembeddingscheme using differences between original and predicted pixel values," *Inform. Secur.*, vol. 2, no. 2, pp. 35–46, 2008.

7. Improvedsteganographic method preserving pixel-value differencing histogram with modulus function (Article) Lee, H.-K.a , Joo, J.-C.a , Lee, H.-Y.b

8. X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, Apr. 2011, pp. 255-258.

9. X. Zhang, "Separable reversible data hiding in encrypted image,"IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr.2012.

10. "Reversible watermarking algorithm using sorting and prediction, "IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

11. Ni, Z., Shi, Y. Q., Ansari, N., Su, W., Sun, Q., & Lin, X. (2008). Robust lossless image data hiding designed for semi-fragile image authentication. *IEEE Transactions on Circuits and Systems for Video Technology, 18*(4), 497-509. doi:10.1109/TCSVT.2008.918761

12. Han, T., Chen, X., Zhu, Y.-F.Subtractive pixel adjacency matrix based features for steganalysis of spatial color images (2016) Tongxin Xuebao/Journal on Communications, 37 (2), pp. 157-164.

13. A Comparative Study of PVD-Based Schemes for Data Hiding in Digital Images, El-Sayed M. El-Alfy, Azzat A. Al-Sadi .

14. A Novel Difference Expansion Transform for Reversible Data Embedding Hyoung Joong Kim, *Member, IEEE*, VasiliySachnev, Yun Qing Shi, *Fellow, IEEE*, Jeho Nam, *Senior Member*, *IEEE*, and Hyon-Gon Choo.

15. Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding," in *Proc. IEEE Int. Conf. Multimedia Expo.*, Taipei, Taiwan, R.O.C., 2004, pp. 2199–2202.

Corresponding Author:

R. Anushiadevi,

Email: *thambivv@gmail.com*