ISSN 2229-5518

Data Hiding Based on Spatial Domain Concept (R, G, B Planes & Gray Images)

Dosa Naga Sudha, Shamanthula Manoj

Abstract—Data hiding is the technique of embedding data in an image and retrieval of the data with lossless reconstruction of original im age. In this paper, we present data hiding scheme based on histogram modification.This technique is based on differences of adj-acent pixels for embedding data and has more hiding capacity compared to existing methods.We exploit a binary tree structure to solve the problem of communicating pairs of peak points. Here, a histogram shifting technique is applied in order to prevent overflow and underflow problems of the pixels. Color image is divided into three planes i.e., r, g, b. In each plane data is embedded. Large amount of data is embed ded by using this type of algorithm. The performance of the algorithm has been evaluated with hiding capacity (data bits) and peak signal to noise ratio (db) of the reconstruction as the parameters.

Index Terms — Data hiding, Histogram modification, Histogram shifting, Individual components of r, g,b planes, Image authentication, lossless watermarking, lossless reconstruction.

1 Introduction

Data hiding is a Technique [1] that is mainly used for the authentication of data like images, videos, electronic documents etc. The main application of Reversible data hiding technique lies in IPR Protection, Authentication, Military, medical and law enforcement. We have different types of data hiding techniques. The Image watermarking technique is used for protection and authentication of intellectual property.

In visible watermarking of images, the watermark image is embedded in a primary image such that watermark is intentionally perceptible to a human observer whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted/detected by a computer program.

The lossless watermarking technique is a process that is used for the exact recovery of the original image. Lossless watermarks found applications in fragile authentication, integrity protection, and metadata embedding. It is especially important for medical and military images.

The lossless watermarking technique is also refer to as invertible, or distortion-free data hiding technique because it is capable of restoring the embedded image to its original state without accessing any side information. We can say that the embedding distortion can be erased or removed from the embedded image.The digital watermark is a signal that is embedded inside an image, and it can be extracted later by means of some operations for authentication. A digital watermark should be statistically invisible so it cannot be detected or erased.

- *Dosa Naga Sudha is currently working as Assistant professor in the Department of ECE,JNTU college of engineering ,jagtial ,India. E-mail: nayaniharshi@yahoo.co.in.*
- *Shamanthula Manoj is currently pursuing masters degree program in digital systems and computer electronics in JNTU college of engineering ,jagtial , India, E-mail: manojknrece@gmail.com.*

The hidden watermark is inseparable from the host image so that the original data remains accessible from the watermark. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. Because of this use, watermarking techniques are often evaluated based on their invisibility, recoverability, and robustness. Digital watermarks may be comprised of copyright or authentication codes, or a legend essential for signal interpretation.

The existence of these watermarks within a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video. In order to protect ownership or copyright of digital media data, such as image, video and audio, encryption and watermarking techniques are generally used. Encryption techniques can be used to protect digital data during the transmission from sender to the receiver. Watermarking technique is one of the solutions for the copyright protection and they can also be used for fingerprinting, copy protection, broadcast monitoring, data authentication, indexing, medical safety and data hiding.

Over the past few years digital watermarking has become popular due to its significance in content authentication and legal ownership for digital multimedia data. A digital watermark is a sequence of information containing the owner's copyright for the multimedia data. It is inserted invisibly in another image so that it can be extracted at later times for the evidence of rightful ownership. Available digital watermarking techniques can be categorized into one of the two domains, viz., spatial and transform, according to the embedding domain of the host image. An ideal watermarking system would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. Reversible data hiding techniques have also been proposed for various fields such as audio [9], MPEG-2 video [10] ,3-D meshes [11], visible watermarking [12], SMVQ-based compressed domain [13], and the integer-to-integer wavelet-domain [14]. Another novel histogram-based reversible data-hiding technique was presented by Ni et al. in [2], in which the message is embedded into the histogram bin. They used peak and zero points to achieve low distortion, but with attendant low capacity. Histogram modification techniques have been extended recently in [15], [16]. However, those techniques all suffer from the unresolved issue represented by the need to communicate pairs of peak and zero points to recipients.

2 PROPOSED SCHEME

In [2], Ni et al. Introduced a reversible data hiding schemebased on histogram modification using pairs of peak and zero points. Let P be the value of peak point and Z be the value of zero point. The range of the histogram, $P + 1$, $Z - 1$, is shifted to the right-hand side by 1. Once a pixel with value Pis encountered, if the message bit is “1,” the pixel value is increased by 1. Otherwise, no modification is needed. Data extraction is actually the reverse of the data hiding process.

Note that the number of message bits that can be embedded into an image equals the number of pixels associated with the peak point. However, the histogram modification technique does not work well when an image has an equal histogram. While multiple pairs of peak and minimum points can be used for embedding, the pure payload is still a little low.

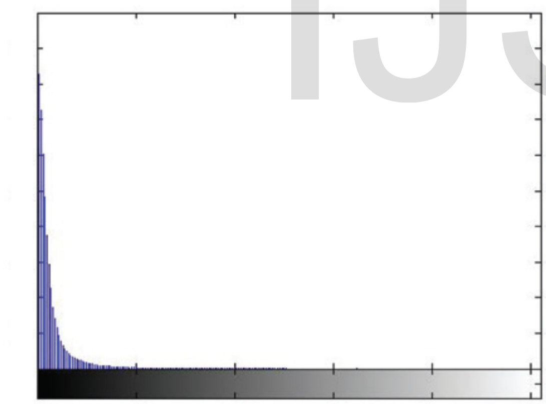

Fig. 1. Distribution of differences

Moreover, the histogram modification technique carries with it an unsolved issue in that multiple pairs of peak and minimum points must be transmitted to the recipient via a side channel to ensure successful restoration. Thus, we present an efficient extension of the histogram modification technique by considering the differences between adjacent pixels instead of simple pixel value. Since image neighbor pixels are strongly correlated, the distribution of pixel difference has a prominent maximum, that is, the difference is expected to be very close to zero, as shown in Fig. 1. We can find that the differences have almost a zero-mean and Laplacian-like distribution [3]. Distributions of other images also follow this model. Laplacian data can be applied to data hiding schemes [4]–[6] to improve their embedding ability. This observation leads us toward designs in which the embedding is done in pixel differences.

We also use a treestructure to solve the issue of communicating multiple pairs of peak points to recipients. Having explained our background logic, we now outline the principle of the proposed reversible data hiding algorithm.

2.1 Binary Tree Structure

Fig. 2 shows an auxiliary binary tree [8] for solving the issue of communication of multiple peak points. Each element denotes a peak point. Let us assume that the number of peak points used to embed messages is 2^L , where L is the level of the binary tree. Once a pixel difference d(i) that satisfies $d(i) < 2^L$ is encountered, if the message bit to be embedded is “0,” the left child of the node d(i) is visited; otherwise, the right child of the node d(i) is visited. Higher payloads require the use of higher tree levels, thus quickly increasing the distortion in the image beyond acceptable levels. However, all the recipient needs to share with the sender is the tree level L, because we propose an auxiliary binary tree that predetermines multiple peak points used to embed messages. A detailed embedding algorithm with the auxiliary binary tree is given later in this letter.

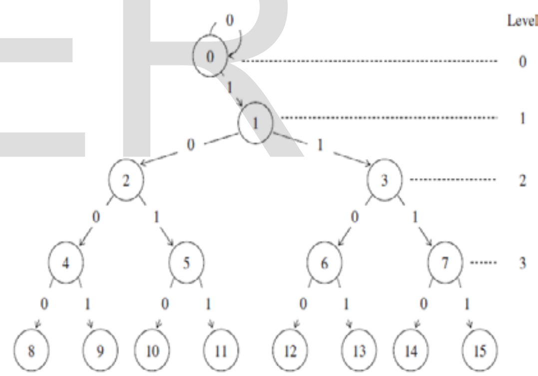

Fig. 2. Binary tree figure

2.2 Prevent Overflow and Underflow

Modification of a pixel may [8] not be allowed if the pixelis saturated (0 or 255). To prevent overflow and underflow, we adopt a histogram shifting technique that narrows the histogram from both sides, as shown in Fig. 3. Let us assume that the number of peak points used to embed messages is 2^L , where L is the level of the proposed binary tree structure.Thus, we shift the histogram from both sides by 2^L units to prevent overflow and underflow since the pixel x(i) that satisfies $d(i) \geq 2^L$ will shift by 2^L units after embedding takes place. After narrowing the histogram to the range 2^L ,$255 - 2^L$,we must record the histogram shifting information as overhead bookkeeping information. For this purpose, we create a onebit map as the location map, which is equal in size

ISSN 2229-5518

to the host image. For a pixel having grayscale value in the range 2^L , 255 – 2^L , we assign a value 0 in the location map; otherwise, we assign a value 1. The location map is losslessly compressed by the run-length coding algorithm, which will yield a large increase in compression ability since pixels out of the range 2^L , 255 – 2^L are few and are almost always contiguous. The overhead information will be embedded into the host image together with the embedded message. Note that the maximum modification to a pixel is limited to 2^L according to the proposed tree structure. As a result, shifting the histogram from both sides by 2^L units enables us to avoid the occurrence of overflow and underflow.

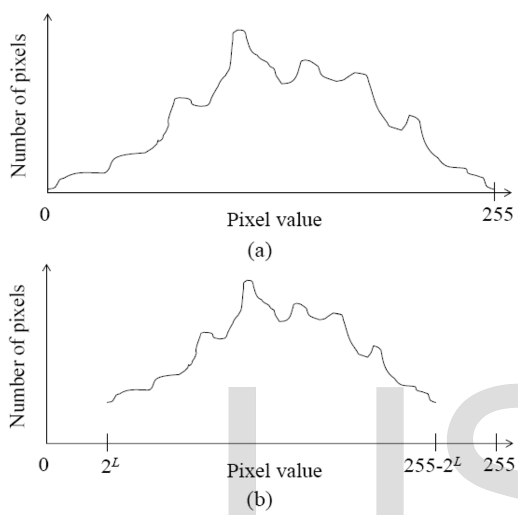

Fig. 3. Histogram shifting. (a) Original histogram. (b) Histogram shifting.

2.3 Algorithm for Embedding and Extraction of Message Bits in Grayscale Images

2.3.1 Embedding Process

For an [8] N-pixel 8-bit grayscale host image H with a pixel value x(i), where x(i) denotes the grayscale value of the ith pixel,0 ≤ i ≤ N − 1, x(i) ∈ Z, x(i) ∈ 0, 255.

1) Determine the level L of the binary tree.
2) Shift the histogram from both sides by 2^L units. Note that the histogram shifting information is recorded as overhead book keeping information that will be embedded into the image itself with payload.
3) Scan the image H in an inverse s-order. Calculate the pixel difference d(i) between pixels x(i−1) and x(i) .
4) Scan the whole image in the same inverse s-order.
If d(i) ≥ 2^L, shift x(i) by 2^L units

$$y(\mathrm{i}) = \begin{cases} x(\mathrm{i}), & if\ i = 0 \\ x(\mathrm{i}) + 2^{L}, & if\ d(\mathrm{i}) \geq 2^{L}\ and\ x(\mathrm{i}) \geq x(\mathrm{i}-1) \\ x(\mathrm{i}) - 2^{L}, & if\ d(\mathrm{i}) \geq 2^{L}\ and\ x(\mathrm{i}) < x(\mathrm{i}-1) \end{cases}$$

where y(i) is the watermarked value of pixel i.

5) If d(i) < 2^L , modify x(i) according to the message bit

$$y(\mathrm{i}) = \begin{cases} x(\mathrm{i}) + (\mathrm{d(i)} + \mathrm{b}), & if\ \ x(\mathrm{i}) \geq x(\mathrm{i}-1) \\ x(\mathrm{i}) - (\mathrm{d(i)} + \mathrm{b}), & if\ \ x(\mathrm{i}) < x(\mathrm{i}-1) \end{cases}$$

where b is a message bit to be embedded and b {0, 1}.

Note that the overhead information is included in the image itself with payload. Thus, the real capacity Cap that is referred to as pure payload is Cap = Np−|O|, where Np is the number of pixels that are associated with peak points and |O| is the length of the overhead information.

2.3.2 Extraction Process

This process extracts [8] both overhead information and pay load from the watermarked image and losslessly recovers thehost image. Let L be the level of the proposed binary tree. For an N-pixel 8-bit watermarked image with a pixel value y(i) , where y(i) denotes the grayscale value of the ith pixel, 0 ≤ i ≤ N − 1, y(i) ∈ Z, y(i) ∈ 0, 255.

1) Scan the watermarked image W in an inverse s-order.
2) If |y(i) x(i−1)| < 2^(L+1), extract message bit b by

$$b = \begin{cases} 0, & if\ |y(i) - x(i-1)|\ \ is\ even \\ 1, & if\ |y(i) - x(i-1)|\ \ is\ odd \end{cases}$$

Where x(i−1) denotes the restored value of y(i−1)

3) Restore the original value of host pixel x(i) by

$$\mathrm{x(i)} = \begin{cases} y(\mathrm{i}) + \left\lceil \dfrac{|y(\mathrm{i}) - \mathrm{x(i-1)}|}{2} \right\rceil, \\ \quad if\ |y(\mathrm{i}) - \mathrm{x(i-1)}| < 2^{L+1}\ and\ y(\mathrm{i}) < \mathrm{x(i-1)} \\ y(\mathrm{i}) - \left\lceil \dfrac{|y(\mathrm{i}) - \mathrm{x(i-1)}|}{2} \right\rceil, \\ \quad if\ |y(\mathrm{i}) - \mathrm{x(i-1)}| < 2^{L+1}\ and\ y(\mathrm{i}) > \mathrm{x(i-1)} \\ y(\mathrm{i}) + 2^{L},\ if\ |y(\mathrm{i}) - \mathrm{x(i-1)}| \geq 2^{L+1}\ and\ y(\mathrm{i}) < \mathrm{x(i-1)} \\ y(\mathrm{i}) - 2^{L},\ if\ |y(\mathrm{i}) - \mathrm{x(i-1)}| \geq 2^{L+1}\ and\ y(\mathrm{i}) > \mathrm{x(i-1)} \\ y(\mathrm{i}), \qquad otherwise. \end{cases}$$

4) Repeat Step 2 until the embedded message is completely extracted.
5) Extract the overhead information from the extracted Message. By following way
If a value 1 is assigned in the location i , restore x(i) to its original state by shifting it by 2^L units; otherwise, no shifting is required.

ISSN 2229-5518

2.4 Algorithm for Embedding and Extraction of Message Bits in Color Images

Consider, a color image [7] with N pixels. Each pixel in the color image will have three individual color components of red(R), green(G), and blue(B). The pixel values of all these color components will be in the range of [0. 255].The message bits can be embedded in all the three planes and these planes can be recombined to form the original color image.so,the embedding capacity of the color image is three times greater when compared to the grayscale images. The algorithm for histogram modification based on pixel differences for color images are as follows.

1. Read the input color image.
2. Seperate the whole image into three planes of individual Components R, G, B.

Consider that we are embedding the message bits in B plane.The remaining steps of the algorithm are similar to the steps in section 2.3.Finally after extraction of the message bits from the R,G, and B planes,these planes are combined to form an RGB image.

3 Experimental Results

The performance of the proposed data hiding scheme on different images has been evaluated. To obtain a better understading of how different host images affect the performance of the proposed reversible data hiding scheme, we present some results in a graphical form.all experiments were performed with commonly used grayscale and color images.

3.1 For Grayscale Images

According to the proposed method, assume that the number of peak points used to embed messages is 2^L , where L is the level of the binary tree. Once a pixel difference d(i) that satisfies d(i) < 2^L is encountered, if the message bit to be embedded is “0,” the left child of the node d(i) is visited; otherwise, the right child of the node d(i) is visited. Higher payloads require the use of higher tree levels.results are tabulated in Table 1. The experiments were done by considering grayscale image of size 256x256.

Table1 :- Hiding capacity and distortion for grayscale images of size 256x256.

Host image (256x256)	Pure payload cap for tree level L=0,1,2,........					
	0	PSNR in db	1	PSNR in db	2	PSNR in db
Lena	10220	33.09	10388	32.93	10401	31.88
Baboon	4791	28.74	4960	28.73	5091	28.55
Boat	7991	31.97	8051	31.07	8149	30.67

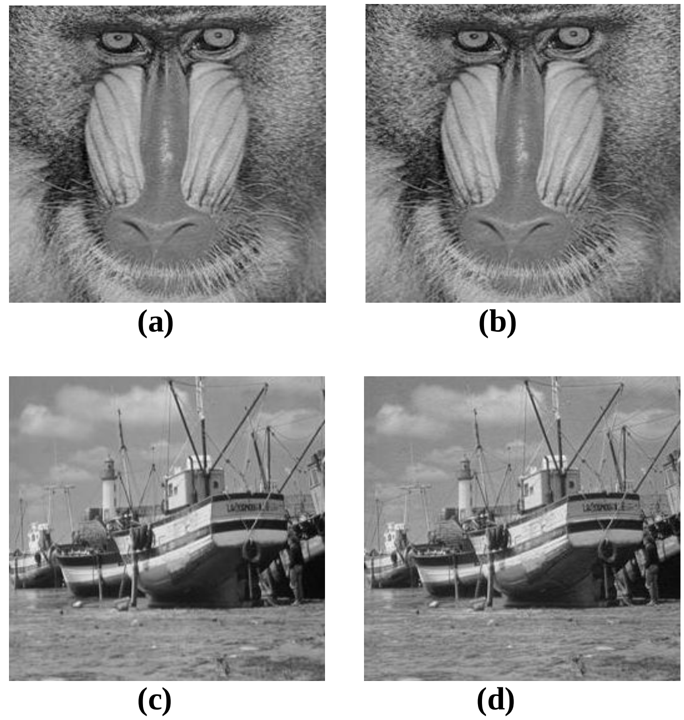

Fig.4 Host images (a) Baboon (c) Boat, Watermarked images (b) Baboon (d) Boat

3.2 For Color images

Color image is divided into three individual planes i.e., red(R), green(G),blue(B).In each plane data is embedded by using same procedure of the grayscale image.

Results are tabulated in Table 2,3&4. The experiments were done by considering color image of size 256x256.

Fig.5 Host images (a) Lena (b) waterlily (c) sunset

Table 2:- Hiding capacity and distortion for color images of size 256x256

Host image (256x256)	Payload for tree level 0				PSNR(db)		
	R	G	B	Total	R	G	B
Lena	10602	10208	10528	31338	33.86	32.07	34.30
Waterlily	7313	7348	8989	23650	28.80	28.33	29.55
sunset	10384	12288	11543	34215	30.92	36.15	39.88

Table 3:- Hiding capacity and distortion for color images of size 256x256.

Host image (256x 256)	Payload for tree level 1				PSNR(db)		
	R	G	B	Total	R	G	B
Lena	10634	10326	10647	31607	33.80	31.88	33.97
Water lily	7340	7652	8999	23991	28.73	28.31	29.46
sunset	10445	12297	11606	34348	30.90	35.37	38.35

Table 4:- Hiding capacity and distortion for color images of size 256x256

Host image (256x 256)	Payload for tree level 2				PSNR(db)		
	R	G	B	Total	R	G	B
Lena	10674	10499	10884	32057	32.74	30.96	32.60
Water lily	7354	7841	9009	24204	28.33	27.93	28.96
sunset	10454	12304	11617	34375	30.46	33.30	34.93

4 CONCLUSION AND FUTURE WORK

In this paper, an efficient extension of the histogram modification technique is presented by considering the differences between adjacent pixels rather than simple pixel values. We exploit a binary tree structure to solve the problem of communicating pairs of peak points. The adjacent pixels are highly correlated and this enables us to achieve large payload capacity, so the payload capacity of the RGB images and gray scale images can be seen in this letter.In future this approach can be used for video sequences by separating them into individual frames.

ACKNOWLEDGMENT

The author wishes to thank Mr.B.Prabhakar (Assoc. Prof. and Head, ECE Dept. JNTUHCEJ) for his guide lines.

REFERENCES

[1] Dhananjay Yadav , Vipul Singhal and, Devesh Kumar Bandil," Reversible data hiding techniques," *International Journal of Electronics and Computer Science Engineering* ISSN-2277-1956/V1N2-380-383.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding,"*IEEE Trans. Circuits Syst. Video Tech* nol.,vol. 16, no. 3, pp. 354–362, Mar 2006.

[3] R. M. Norton, "The double exponential distribution: Using calculus to find a maximum likelihood estimator,"*Amer. Stat.*, vol. 38, no.2, pp. 135–136, May 1984.

[4] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digita watermarking scheme based on integer wavelet transform," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1294–1300, Oct 2006.

[5] Z. Ni, Y. Q. Shi, N. Ansari,W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 4, pp. 497–509,Apr. 2008.

[6] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo,"A novel difference expansion transform for reversible data embedding,"*ieee Transactions Inf. Forensic Secur.*, vol. 3, no. 3, pp. 456–465, Sep. 2008.

[7] Rajkumar,and Ramaswamy,"Lossless Data Hiding Based on Histograam Modification," *The International Arab Journal of Information Technology*,"Vol. 9,No.5,September 2012.

[8] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang," Reversible Data Hiding Based on Histogram Modification of Pixel Differenes," *ieee Transactions On Circuits And Systems For Video Technology*,Vol.19, NO. 6, JUNE 2009.

[9] M. Van der Veen, F. Bruekers, A. Van Leest, and S. Cavin, "High capacity reversible watermarking for audio," *in Proc. SPIE Security Watermarking Multimedia Contents* V, Santa Clara, CA, Jan. 2003, vol. 5020, pp. 1–11.

[10] D. Rui and J. Fridrich, "Lossless authentication of MPEG-2 video," in Proc. IEEE Int. Conf. Image Process., vol. 2. Rochester, NY, 2002, pp. 893–896.

[11] J. Dittmann and O. Benedens, "Invertible authentication for 3-D meshes," *in Proc. SPIE Security Watermarking Multimedia Contents* V, Santa Clara, CA, Jan. 2003, vol. 5020, pp. 653–664.

[12] Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recovery of original images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

[13] C. C. Chang, W. L. Tai, and C. C. Lin, "A reversible data hiding schemebased on side match vector quantization," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 16, no. 10, pp. 1301–1308, Oct. 2006.

[14] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forensic Secur.*, vol. 2, no. 3, pp. 321–330, Sep. 2007.

[15] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," *IEICE Electron*. Exp., vol. 4, no. 7, pp. 205–210, Apr. 2007.

[16] S. K. Lee, Y. H. Suh, and Y. S. Ho, "Reversible image authentication-based on watermarking," *in Proc. IEEE Int. Conf. Multimedia* Expo,Toronto, ON, Canada, Jul. 2006, pp. 1321–1324.