Reverse Data Hiding Using Histogram Comparison

Ms.Baby Dayana[#1],Akhil Mantha[#2], Manideep Reddy[*2], V.S.P.P.K Prithvi[#3]

[#]*Department Of Computer Science & Engineering, SRM Institute Of Science &Technology*
Ramapuram, Chennai, 600089

[1]dianadevadhas@gmail.com

[2]akhilmantha@live.com

[3]manideepreddy2007@gmail.com
[4]prithvivobbbilineni@gmail.com

[5]karankhosla99@gmail.com

***Abstract*— Different from the previous applications of the process, a new approach is used. This method uses histogram shifting technique and also the modification of the prediction errors (MPE) algorithm by using the predictors. The embedding capacity and the output of the steganography-applied image directly depends on the efficiency of the predictors. This method uses two & three bins in the histogram to increase the embedding capacity of the image. The final and the initial image can be compared with their following histograms.**

***Keywords*—Prediction, Prediction Error, Steganography, RC7, Histogram Shifting, Histogram, Reversible Data Hiding.**

INTRODUCTION

Data hiding an important and crucial area where it deals with regular applications such as watermarking, copyright issues and it also has an important role in military applications. Data hiding also introduces a term called "Steganography" which means to secretly embed the data in any kind of a signal or a host (audio, images, text, video), which makes it difficult for unauthorized people to access it. In this domain, many different approaches were introduced. What lacks is the ability to restore a complete image along with lossless transmission.

Another interesting area to explore in RDH is a Difference Expansion algorithm. They are one important module of RDH and have low distortion and high embedding capacity. In this technique the cover image is differentiated into a series of non-overlapping pair of pixels.

Some of the characteristics of Data Hiding are

- **Capacity Of The Cover Medium:** Capacity of the cover medium can be defined as the number pixels that can be embedded into a cover medium.
- **Perceptibility:** The inability to detect hidden information.
- **Robustness:** The amount of modification the stego-image can withstand before an adversary can extract and destroy the hidden information.

I. REVERSIBLE DATA HIDING

Reversible Data Hiding can be defined as approach where the data is secretly embedded in the cover image, for an instance here it is an image. The most important property of RDH is the ability to recover the original image after extracting the secret data from the image. The block diagram of RDH is shown in Fig. Watermarking and Reversible Steganography can restore the original without any distortion after the extraction of secret data.

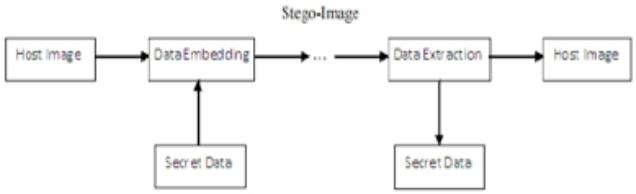


Fig.2. Reversible Data Hiding

Reversible Data Hiding has been there for several years now and there are a lot of different approaches to this problem. Following are different approaches to this problem. In a traditional approach where one considers carrier signal and a cover medium, only a certain length of the message can be embedded. Where as there is a way where one can hide two or more confidential data sets. This can be achieved by Circular visual cryptography, where the data set is displayed at inner and outer region of the circular images.

II. HISTOGRAM SHIFT BASED TECHNIQUE

The histogram-shifting based reversible data hiding schemes embed the data by shifting the histogram into a fixed direction. The peak point corresponds to the maximum number of pixels in the histogram of the giver image. And the zero point is usually the point where the number in histogram is zero. In algorithms, the pixels between the peak and the zero pair are modified in the embedding process. The pixel in the peak point was used to carry the secret message and others are modified and no secret data is embedded.

The hiding capacity of the histogram shifting based data hiding equals the number pixels in the peak points, the larger the number of pixels in the peak point, higher the hiding capacity. To increase the hiding capacity, more of the peak points and zero pairs can be used. Sometimes it is difficult to find the pair of peak and zero points.

Histogram-shift algorithm is as follows:

Step 1: Create the histogram of the image.

Step 2: Find the peak and zero points.

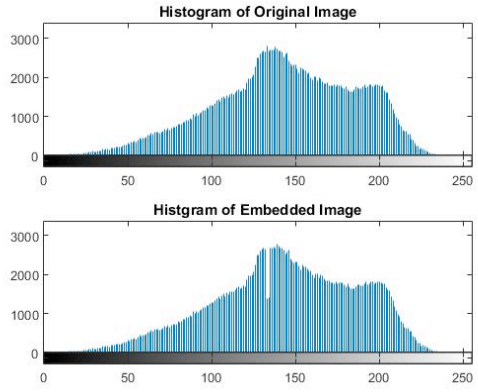
Step 3: We assume that the peak point is a, the zero point is b. (a>b), shift the points between b+1 and a-1 by reducing 1.

Step 4: If the embedded bit is 1, then the peak point value is reserved otherwise change the peak point value by reducing 1.

Step 5: To achieve the reversibility requirements, the location of the pixel in the minimum point must be recorded and embedded. Then record some peak, zero points and some auxiliary information. We assume the cover image is 2-(a). Figure 2-(b) is the histogram of the image, we can see that the peak point is 9 and the zero point is 7. The value of peak point is at 10 i.e. we can embed 10 bits into host image.

9	8	8	8	9	5
9	5	9	9	6	5
8	6	9	8	5	3
6	5	10	9	6	4
5	5	10	9	9	5
8	4	9	6	8	4

(a)



(b)

III. Proposed Approach

In this approach the to enhance the data hiding capacity and image quality, the original image considered is divided into blocks. The data that can be embedded into the image can be compared to the embedding capacity of a cover medium. This approach consists of mainly three blocks, 1) Dividing the image into two blocks, 2) Processing the image and 3) Embedding the secret information.

First stage consists of dividing the image into two blocks and the processing stage involves the generation of histogram of the each block and comparing it with the histogram of the image. The embedding stage involves placing the secret message inside the image block. Using the binary tree structure the number of peak points used for data embedding is assumed to be 2_L.

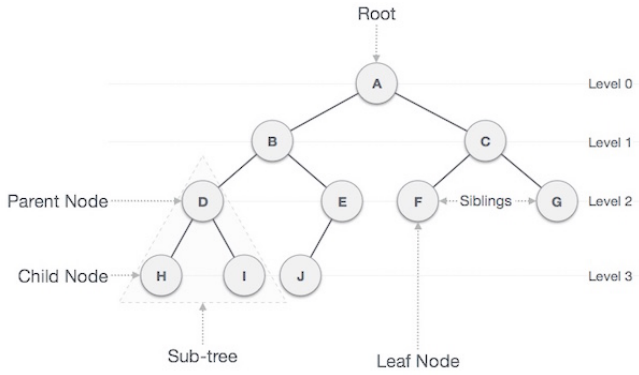


Fig.3. Binary Tree Structure

Pixel modification cannot be done if the pixel is saturated i.e. if overflow and underflow occurs. Overflow means that the generated grey value here crosses the value of 255 and underflow means that the generated value is below 0. In general to prevent the above factors flags are used but here the approach histogram shifting has a range of 2_L.

A. Embedding Process

First consider an N pixel 8-bit grey scale image with the pixel value between (0-255)

1) Divide the image into two blocks.
2) Generate the histogram of each block.
3) Find the tree level L, of the tree structure.
4) For the first block, perform the following:
   a) Narrow the histogram in the range 2_L, $255-2_L$ by shifting the histogram both sides.
   b) Scan the image in the order and find the difference between the adjacent pixels.
   c) Scan the image block and fins the difference, if the difference is greater than 2_L then the shifting is done by 2_L units.
5) The above steps a) – c) are repeated for the rest of the blocks.

B. Extraction Process

Consider an N pixel 8-bit watermarked image with the pixel value z_i. The given pixel value should be in the range. Message bits can be extracted from the watermarked image blocks using the following steps:

a) Locate the watermarked image in an order.
b) Extract the message bit if $|z_i\ y_{i-1}| < 2_{(L+1)}$ where y_{i-1} denotes the restored value.
c) Original value of the host image block is restored by z_i, otherwise the process is repeated until the message is fetched from the image blocks.

IV. RESULTS

This process is tested on the datasets of size 512*512 with 8 bit of resolution. First the below image is divided into two blocks.

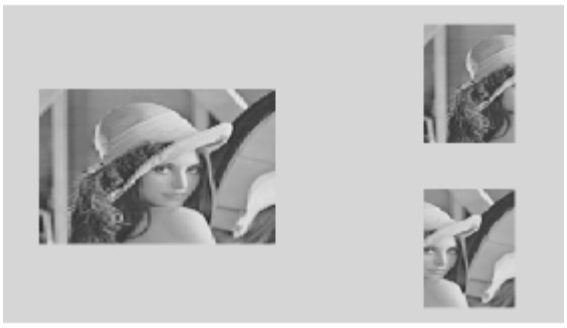


Fig.4. Division of Image Into Blocks

The above figure shows the division of image into blocks. Creating the histogram of the image makes it possible to divide the message across the complete image. Generating histogram and comparing them also increases the final image quality.

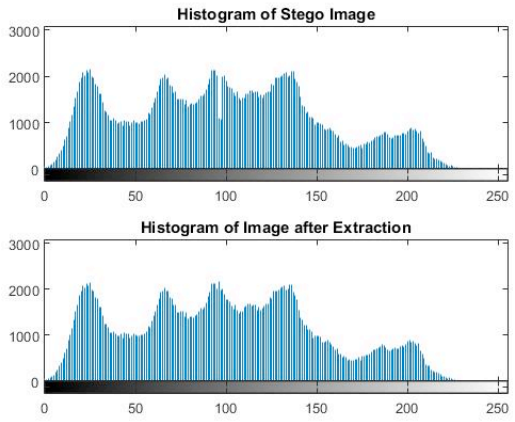


Fig.4 (a). Histogram Of The Image Before Extraction

The following figure shows the implementation of the stego-image into a histogram. Generating the histogram of the image also helps to depict the peak-zero pairs.

C. Finding PSNR Value Of The Image

PSNR stands for (peak signal to noise ratio) and this is expressed in terms of logarithmic decibel scale. PSNR value is defined in terms of mean square error (MSE). Given a monochromatic image, the MSE can be defined as

1) $PSNR = 20\ log_{10}(MAX_I) - 10.\ log_{10}(MSE)$
2) The signal in this case is the original image and The noise
3) In this case is introduced by embedding the secret Data.
4) Generally the PSNR value is more when the embedding process is performed. Then the image is divided into blocks to obtain the image quality.

V. CONCLUSION

This paper proposes a new approach for data hiding where the pixel difference is considered rather than a single pixel. One of the main drawbacks of the histogram comparison technique is that it is difficult to communicate and identify the peak-zero points pair. Here this is overcome by introducing the binary tree structure and. In this approach the tree level determines the number of peak points. The number of pixels to be embedded is determined by the number of pixels associated with peak points. To help distribute the message along the complete image, the image is divided into blocks.

REFERENCES

[1] Jassim, Firas A., "A novel steganography algorithm for hiding text in
image using five modulus method", arXiv preprint arXiv, Vol. 72, No.
17, PP. 39-44, 2013.
[2] Bandyopadhyay, Debiprasad, et al., "A Novel Secure Image
Steganography Method Based on Chaos Theory in Spatial
Domain", International Journal of Security, Privacy and Trust
Management (IJSPTM), Vol. 3, No. 1, PP. 11-22, 2014.
[3] Jain, Nitin, Sachin Meshram, and Shikha Dubey., "Image Steganography
Using LSB and Edge–Detection Technique", International Journal of
Soft Computing and Engineering (IJSCE), Vol. 2, No. 3, PP. 217-222,
2012.

[4] RAKHI1 & VIJAY PRAKASH SINGH., " DATA HIDING IN SKIN
TONE OF IMAGES USING STEGANOGRAPHY", International
Journal of Electronics and Communication Engineering (IJECE), Vol. 2,
No. 4, PP. 105-112, 2014.
[5] Goel, Stuti, Arun Rana, and Manpreet Kaur., "Comparison of image
steganography techniques", International Journal of Computers and
Distributed Systems, Vol. 3, No. 1, PP. 20-30, 2013.
[6] R.Norcen, M.Podesser, A.Pommer, H.Schmidt, and A.Uhl, “Confidential
Storage and Transmission of Medical Image Data” Computers in Biology and
Medicine 33, pp.277–292, 2003.
[7]J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding-new paradigm
in digital watermarking,” Eur. Assoc. Signal Process. J. Appl. Signal Process.,
vol. 2002, no. 2, pp. 185–196, Feb. 2002.
[8] T. Kalker and F. M. J. Willems, “Capacity bounds and constructions for
reversible data hiding,” Security Watermarking Multimedia Contents V, vol.
5020, pp. 604–611, Jun. 2003.
[9] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless
generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14, no.
2, pp. 253–266, Feb. 2005
[10] J. Tian, “Reversible data embedding using a difference expansion,” IEEE
Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[11] L. Kamstra and H. J. A. M. Heijmans, “Reversible data embedding into
images using wavelet techniques and sorting,” IEEE Trans. Image Process.,
vol. 14, no. 12, pp. 2082–2090, Dec. 2005.