ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 8, August 2018

Steganalysis using RS method on Block Based Octal Pair Pixel Value Differencing Method

[1]HarshadaKorgaonkar
(Digital Systems, Electronics and Telecommunication Department, JSPM's Rajarshi Shahu college of engineering, Pune)
[2] Mrs. C.V. Rane
(Digital Systems, Electronics and Telecommunication Department, JSPM's Rajarshi Shahu college of engineering, Pune)

***Abstract*— The proposed method-BOPVD method uses new range table which is much meaningful and increases the security level in embedding and extracting of secret data. The proposed method uses 8-neighborhood pixels for embedding purposes. The cover image is split into 3×3 blocks. These blocks are randomly chosen for embedding so that it will increase the security and capacity of the proposed method when compared to other PVD methods.**

The proposed method is RS attack prone.The RS Steganalysis can identify both sequentially embedded messages and randomly embedded messages. No current steganography method can declare that they are free of image distortion while embedding secret inside because PSNR never becomes infinity.

The proposed method never embeds a secret directly or explicitly to an image, it can claim that it is free of any such kinds of steganalysis

Keywords—steganography; steganalysis; RS attack; PVD method;

I. INTRODUCTION

Wu et al.'s [1] first proposed an idea of Pixel Value Differencing (PVD) method. The main limitation of this method is distortion and a histogram deviation is more. In order to overcome the limitation of PVD method, Wang et al. [2] proposed a PVD method using modulus function, which gives histogram differences near to zero and also embeds more information in edges areas.

Modified version of Modulus Function based Pixel Value Differencing (MF-PVD) method [4] is proposed by Joo et al. In this method the image quality of stego image is lower than that of Adaptive Edge Pixel Value Differencing (AE-PVD) method [5]. But the histogram difference is well maintained to avoid steganalysis of histogram detection. Liao et al.'s [6] proposed another pixel value differencing with modified LSB substitution, and Yang et al.'s [7] proposed a data hiding scheme using the pixel value differencing in multimedia images. Most of the PVD steganography methods concentrate on increasing the embedding capacity and image quantity but only very few researches focuses on range table design.

W. Tseng and S. Leng [8] proposed new range table based on perfect square number. The perfect square number provides a mathematical model for new quantization range table. A Steganography Method for Digital Images Robust to RS Steganalysis was proposed by André R.S. Marcal and Patricia R. Pereira. In this method [9] based on the reversible histogram transformation functions to the image, before and after embedding the secret message, it also indicates the stego image seemingly do not contain any embedded data in their LSBs. Statistically values of stego image are same type of changes as the increment or decrement [10] in LSB pixels, either randomly or by using a function it is detectable. So the asymmetry artifacts of LSB replacement are completely avoided. In the proposed BOPVD method is practices W. Tseng and S. Leng's new quantization range table used as references table for embedding and extracting purposes. To improve the security, cover image is divided into 3x3 pixel blocks and these blocks are randomly chosen for embedding purpose. Each pixel blocks contains the eight pixels pairs for their embedding purpose. LSB-M is used for the embedding process. Then we are applying RS steganalysis on the stego image.

II. RELATED WORK

The statistics of a cover image undergo alterations due to information hiding. RS steganalysis is statistical analysis method as it analyses this underlying statistics of an image to detect the secret embedded information. It is considered as stronger than signature analysis as it relies on mathematical techniques. Also it targets specific embedding techniques and requires a detailed knowledge of embedding process and yield very accurate results when used against a target steganography technique. The first ever statistical steganalysis was proposed by Westfeld and Pfitzmann [3]. This approach is specific to LSB embedding and is based on powerful first order statistical analysis rather than visual inspection. The technique identifies Pairs of Values (POVs) which consist of pixel values, quantized DCT coefficients or palette indices that get mapped to one another on LSB flipping. After message embedding, the total number of occurrence of two members of certain POV remains same. This concept of pair wise dependencies is exploited to design a statistical Chi-square test to detect the hidden messages [4]. The reported results show that this method reliably detects sequentially embedded messages. Later, the method was generalized to detect randomly scattered messages [5].

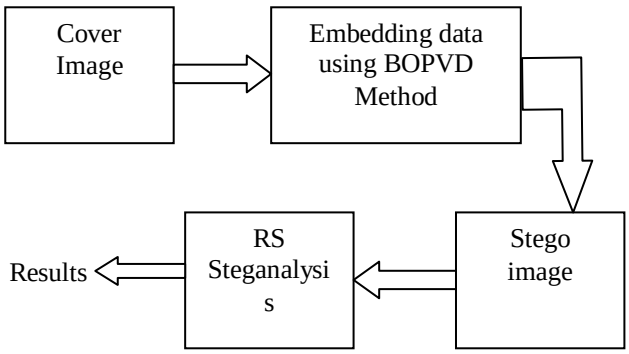
Another specific steganalytic method for detecting LSB embedding in 24-bit colour images—the Raw Quick Pair (RQP) method is proposed by Fridrich et al. [22]. The method is based on analyzing close pairs of colours created by LSB embed-ding. It has been shown that the ratio of close colours to the total number of unique colours increases significantly when

a message of a selected length is embedded in a cover image rather than in a stego image. It is this difference that enables to distinguish between cover images and stego images for the case of LSB steganography. The method works reliably well as long as the number of unique colours in the cover image is less than 30% of the number of pixels. As reported the method has higher detection rate than the method given in [18] but cannot be applied to gray scale images. A more sophisticated technique for detection of LSBs is introduced by J. Fridrich is knownas RS steganalysis method. This technique make use of statistics derived from spatialcorrelations in images. In this method image is divided into several blocks of 8X8 and then noise is measured by the mean absolute value of the differences between consecutive pixels. Depending on increment or decrement in noise level, each group is classified into 'Regular' and 'singular' components. RS steganalysis is more reliable than Chi-square method [2].

III. PROPOSED METHOD

We are here applying RS steganalysis on stego-image by first embedding data using BOPVD method.

Basic Flow diagram is shown below Fig(1)



Fig(1) RS Steganalysis on BOPVD Method

In this method we divide the cover image into 3×3 blocks and each 3x3 block includes nine pixels

Following figure(3) shows the example of one 3x3 pixel block, where x and y are the pixel locations in the image.

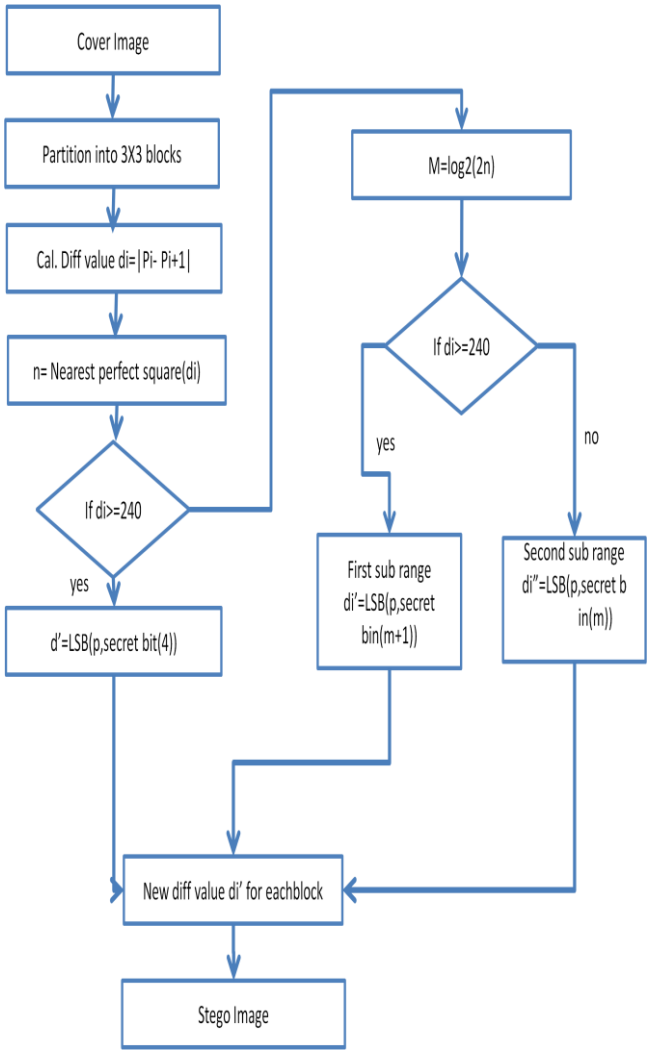
Then following are the two steps involved in this:

- Embedding Procedure
- Extraction Procedure
- RS Stegnalysis

P0 (x-1, y-1)	P1 (x-1, y)	P2 (x-1, y+1)
P7 (x, y-1)	P (x, y)	P3 (x, y+1)
P6 (x+1, y-1)	P5 (x+1, y)	P4 (x+1, y+1)

Fig(2)3X3 block example

A. *Embedding process:*



Fig(3) Embedding Procedure

Step1: The cover image is divided into non-overlapping blocks with 3 × 3 pixels. Each block includes nine pixels

Step2: The difference values di for the eight pixel pairs in each block is calculated as:

d0 = |P (x, y) – P0(x-1, y-1)|

d1 = |P (x, y) – P1(x-1, y) |

d2 = |P (x, y) – P2(x-1, y+1) |

d3 = |P (x, y) – P3(x, y+1) |

d4 = |P (x, y) – P4(x+1, y+1) |

d5 = |P (x, y) – P5(x+1, y) |

d6 = |P (x, y) – P6(x+1, y-1)|

d7 = |P (x, y) – P7(x, y-1) |

Step3: Calculate the square root of difference value di for each pixel pair in each block and then find the nearest perfect square number (n). According to perfect square number , select the range and sub ranged value. The length of secret bit for embedding (m) is decided by the range table.

Step4: Secret bit is matched with LSB of sub range value in the range table. The new pixel difference value d'i is obtained.

Step 5: After getting the new pixel difference value d'i then new pixel values P (i) and P (i+1) are obtained by the following 4 conditions.:

Case1: P(i,x)≥ P(i,y) , d'>d

(P'(i,x), P'(i,y))=(P'(i,x), P'(i,y) –[d'-d])

Case2: P(i,x)< P(i,y) , d'>d

(P'(i,x), P'(i,y))=(P'(i,x), P'(i,y) +[d'-d])

Case3: P(i,x)≥ P(i,y) , d'≤ d

(P'(i,x), P'(i,y))=(P'(i,x), P'(i,y) +[d'-d])

Case4: P(i,x)< P(i,y) , d' ≤d

(P'(i,x), P'(i,y))=(P'(i,x), P'(i,y) -[d'-d])

Step 6: When the above conditions are satisfied new stego pixels is obtained. Repeat the same steps in each pixel pair in all blocks.

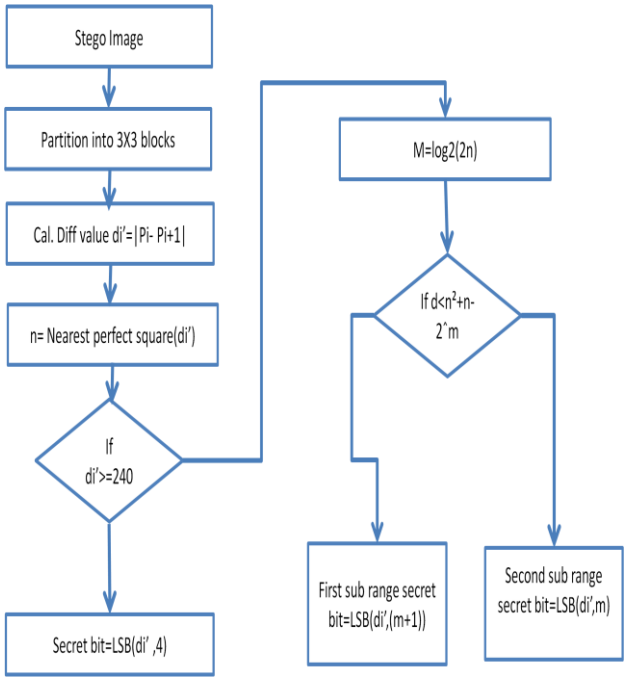
Fig(3) Shows illustration of Embedding Procedure

B. *Extraction Process:*

Step 1: For each block select pair of two consecutive pixels and compute the difference value.

Step 2: Find the nearest perfect square number by function and is in the range number of in New range table

Step 3: From table determine m value and sub range it belongs to, and extract the secret data according to m value in LSB of that differences value d'i. Finally, all secret data is extracted by same way in each blocks



Fig(4) extraction Procedure

C. *RS Steganalysis Algorithm:*

Initially, the image is divided into several blocks. Subsequently, flipping functions such as positive flipping and negative flipping are applied on each block of pixels.

Later, the variations between original and flipped blocks are calculated. Based on the variation results, the blocks are categorized into regular and singular groups.

Let us have a cover image with M×N DCT coefficients, their values are taken from set P = {−128,−127,...,127}. We need a discrimination function f, which will capture the frequency correlations.

This function measures the smoothness of DCT coefficients group G. It is expected that the value of f will increase after LSB embedding, because the LSB embedding increases the noisiness of the image

We can distinguish three types of DCT coefficients: R−regular, S− singular and U−unchanged, which are defined by the discrimination function f and flipping function F.

The operation of applying the flipping function F to the elements of the vector G =(x1,...,xn) will be denoted F(G)

The group of n DCT coefficients) is:

• regular if f(F(G)) >f(G),

• singular if f(F(G)) <f(G),

• unchanged if f(F(G)) = f(G).

The idea is that for a typical cover image, the relative number of regular groups RM is approximately equal to regular groups with inverse flipping mask R−M. This is also true for singular SM and S−M.

The tests were carried out on a single JPEG image with resolution 2000×3008 pixels. The results depended on the selection of the DCT coefficient frequency, group sizes, mask M and the discrimination function f .

Settings were the following:

• The first AC DCT coefficient frequency - coordinates (0, 1),

• Group size n = 5, then G =(x1,x 2,x 3,x 4,x 5),

• mask M = (0 ,1,1,1,0),

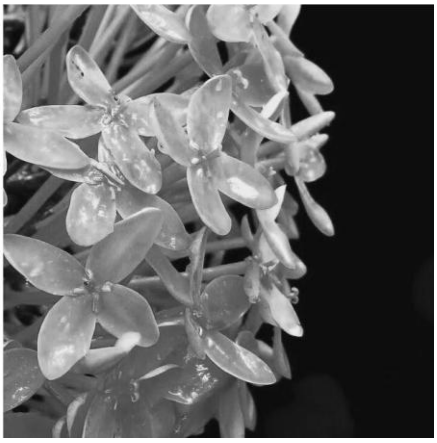
• Inverse mask −M = (0 ,−1,−1,−1,0),

• Discrimination function f (G)=[1]n−1 i=1 |xi+1 −xi|,

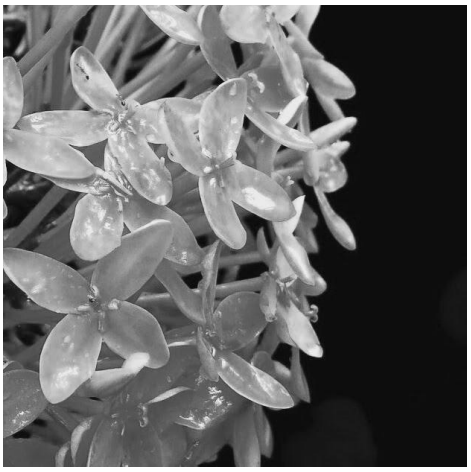
• flipping operation was applied to DCT coefficients with values 0 and 1, too.

IV. RESULTS

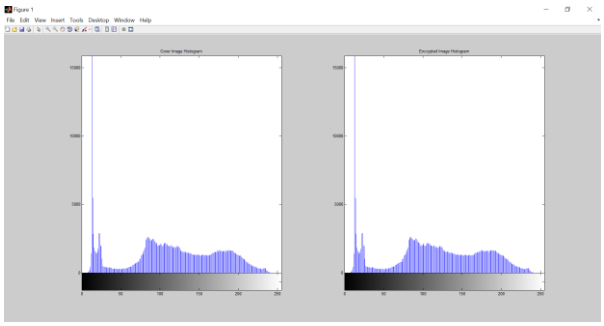
Text message was hidden in different images using BOPVD method below is one of the example which shows cover image and stego image which seem visually similar.



Fig(5) Nature.jpg Cover image



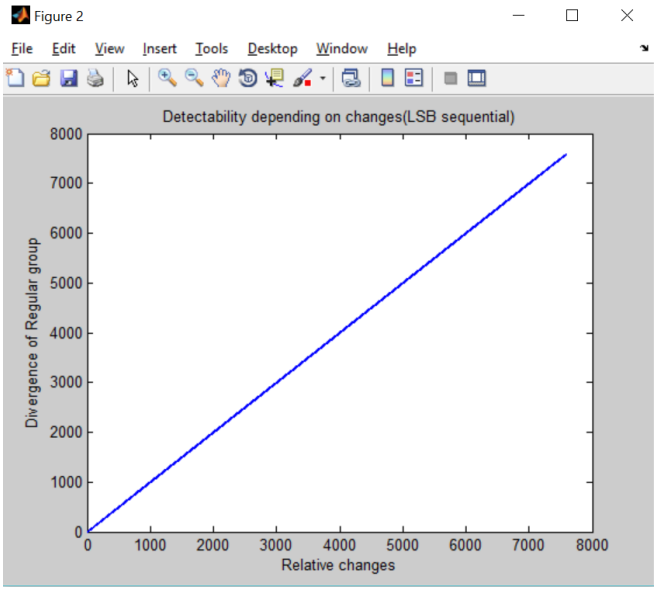
Fig(6) Nature.jpg Stego image



Fig(7) Histogram comparison of Nature cover and stego image.

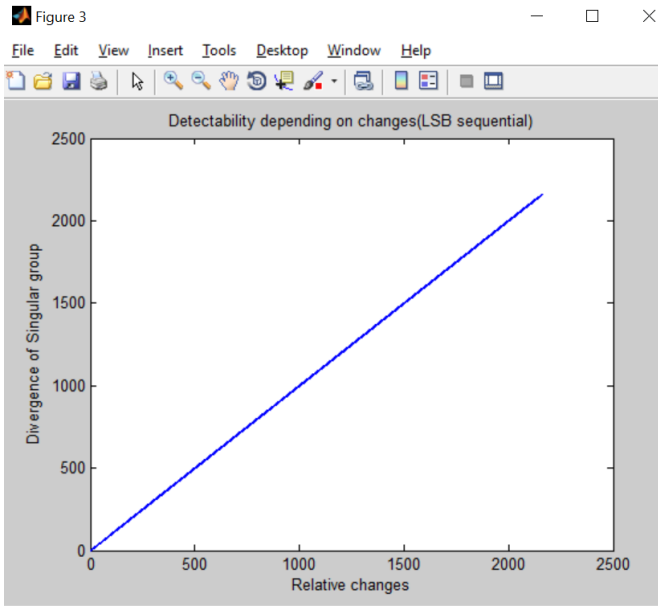
Result shows that PSNR of new image is 63.48 which shows image has low noise.

Figure(7) demonstrates the difference between relative numbers of RM and R−M groups



Fig(7) Relative changes in regular component when the mask M = (1 0 1 0 1) is applied

Figure(6) also shows the difference between the relative numbers of SM and S−M groups. As in the case of regular groups, the greater the difference is, the more DCT coeffcients were changed. Again, when there is an image without any message, ideally SM = S−M applies.



Fig(8) Relative changes in Singular component when mask M = (1 0 1 0 1) is applied

V. CONCLUSION:

Using BOPVD steganography method for data hiding by using eight pixel pair value differences in color images is done which will be RS attack prone.

This has decreased histogram distortion and increase data capacity also increase stego image quality.

The results of RS analysis indicate detectability in all modes of embedding. The results of RS Steganalysis depend on the size of the groups the image is partitioned into, and the "mask". The mask is the same size as the pixel groups and consists of zeros and ones, determining which pixels in each group are flipped as noise is measured. The limitation to RS steganalysis is that its performance is highly dependent on compression. The reliability of RS steganalysis can be increased by using different types of masks.

ACKNOWLEDGMENT

Perfect and precise guidance, hard work, dedication and full encouragement are needed to give a Project successfully. In the life of every student illumination of Project stage-I work is like engraving a diamond.

I am very much thankful to my Guide – Mrs. C. V. Rane At critical occasions her affectionate and helping attitude very much helped me in rectifying my mistakes and proved to be source of unending inspiration for which I am grateful to her.

REFERENCES

[1] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magaz., Special Issue on Security (October– November 2001) 22–28.

[2] J. Fridrich, M. Goljan, Practical steganalysis of digital images-state of the art, in: Proc. SPIE Photonics West, Electronic Imaging (2002), Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 4675, January 2002, pp. 1–13.

[3] A. Westfeld, A. Pfitzmann, Attacks on steganographic systems, in: Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany, September 28–October 1, 1999, pp. 61–75.

[4] T. Moerland, Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, http://www.liacs.nl/home/tmoerl/privtech.pdf.

[5] A. Westfeld, Detecting low embedding rates, in: Lecture Notes in Computer Science, vol. 2578, Springer-Verlag, Berlin, 2002, pp. 324–339.

Harshada Korgaonkar: ME(Digital Systems) student in JSPM's Rajarshi Shahu college of engineering, Tathavde, Pune under Savitribai Phule Pune University.