ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 2, February 2016

A Robust Image Steganography Technique Using Quantized Range Table And Local Area Pixel Value Differencing

Sukhjinder Singh, Kulbhushan Singla, Dr. Rahul Malhotra

***Abstract*— Steganography is a way of hiding the information transmitting from sender to receiver and making the communication invisible. To enlarge the capacity of hidden secret information and to produce indistinguishable stego-image from original image with human eye, a new steganographic approach using quantized range table using perfect square number and local area pixel value differencing is proposed in this paper. Our research provides a new viewpoint that if we choose the proper width for each range and use the proposed method, we can obtain better image quantity and higher capacity. In addition, we offer a theoretical analysis to show our method is well defined. The experiment results also show the proposed scheme has better image quantity and higher capacity.**

***Index Terms*—Steganography, PVD, Range Table, PSNR, MSE.**

I. INTRODUCTION

For transferring the information from sender to receiver, one of the first thoughts should be security issues for transferring data across network. Due to use of internet, there is most necessity of information security. Information security means protecting the information from the attacker or hacker. For transferring the information confidentially, a technique named Steganography is used. The steganography[5] is a way of concealing the information from unwanted sources .The purpose of steganography is covert communication to hide a message from a third party. The word "Steganography"[5] technically means "covered or hidden writing".

The design of an image steganographic system can be categorized into spatial domain methods and transform domain methods.

In spatial domain methods, the processing is applied on the image pixel values directly. Such as, Least Significant Bit Insertion methods and Pixel Value Differencing methods.

The pixel-value differencing (PVD) [1] scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Besides, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding.

In recent years, several studies have been proposed to improve the PVD method. In this work, we used a new quantization range table[ ] based on the perfect square number to decide the payload by the difference value of center pixel and its neighboring local pixels in the matrix of 3X3 pixels. It differs from the design of Wu and Tsai's scheme, in which the quantization range table is based on the range width of the power of two. The perfect square number provides an elegant mathematical model to develop a new quantization range table, which divides each range into two subranges for embedding different numbers of secret bits.

II. REVIEW OF CLASSICAL PVD APPROACH

In PVD method [4], gray scale image is used as a cover image for hiding the secret information. This cover image is partitioned into non-overlapping blocks of two consecutive pixels, P_i and P_{i+1}. A difference value is generated by subtracting P_i from P_{i+1} in each block. The difference value is represented by 'd_i'. The set of all difference values lies a range from -255 to 255. So $|d_i|$ ranges from 0 to 255. The blocks which generates small difference values that locate in smooth area and blocks which generates large difference values that locate at the sharp edged area. The human eyes can tolerate more changes in sharp-edge area than smooth area. So, more data can be embedded into edge area than smooth area. Therefore, in PVD method, a range table has been designed with n contiguous ranges R_k. Here the value of k varies from 1to n like k=1,2,….n. where the range is 0 to 255. The lower limit and the upper limit are represented by l_k and u_k respectively, then $R_k \in [l_k, u_k]$. The width of R_k is calculated using $w_k=u_k-l_k+1$.w_k decides how many bits can be embedded into a pixel block.The embedding algorithm is given as algorithm.

Algorithm:

- Find the difference value di of two consecutive pixel p_i and p_{i+1} for each segment in the cover image. This difference is given by $d_i=|p_{i+1}-p_i|$.

Manuscript received Feb, 2016.

***Sukhjinder Singh**, Research Scholar ECE Deptt., GTBKIET Chhapian Wali Malout,India, 09780464163*

***Kulbhushan Singla**, Assistant Professor ECE Deptt., GTBKIET Chhapian Wali,Malout,India,09463315234.*

***Dr. Rahul Malhotra**, Professor ECE Deptt., GTBKIET Chhapian Wali,Malout,India,,9317945017.*

- Find the optimal range in which the calculated difference value lies in the range table by using d_i. This is calculated as $R_k=\min(u_k- d_i)$, where $u_k \geq d_i$ for all $1 \leq k \leq n$.

Calculate the number of bits't' to be embedded in a pixel segment can be defined as $t=\log_2 w_i$. Where w_i is the width of the range where the pixel difference d_i lies

- Read t bits from binary secret data and convert it into its decimal value b.

- Now finding the new difference value d_i' using $d_i'=l_i+b$.

- Modify the values of p_i and P_{i+1} by the following method[1]:

$$(P_i', P_{i+1}') = (P_i + m/2, P_{i+1} - m/2),$$

if $P_i \geq P_{i+1}$ and $d_i'>d_i$.

$$(P_i - m/2, P_{i+1}+m/2),$$

if $P_i<P_{i+1}$ and $d_i > d_i$

$$(P_i-m/2, P_{i+1}+m/2),$$

if $P_i \geq P_{i+1}$ and $d'_I \leq d_i$

$$(P_i +m/2, P_{i+1} - m/2),$$

if Pi<P i+1 and di'≤di

Where $m=|d_i' - d_i|$. Repeat step 1-6 until all secret data are embedded into the cover image. After embedding all secret data, a resultant image is generated which is called Stego-Image.

While decoding the hidden data from the stego-image, the range table, which is used at encoding, is required. Here the same method is used for partitioning the stego-image into pixel blocks. Calculate the difference value for each block using $di'=|P_i'-P_{i+1}'|$.Now finding the optimum range R_i of d_i'.Compute the b' by b'= di'-li. Convert b' into binary of't' bits, where $t=\log2\ w_i$. These t bits are the hidden secret data.

III. Proposed Scheme

In the proposed scheme, first we separate RGB components of color image. We can embed our secret data using **local are pixel value differencing.** In this method, we choose a center pixel in a matrix of 3X3 pixels (for all three color components). We calculate the inter pixel difference in the matrix to find out highest difference in pixel values. This highest values of difference is compared in range table and we find the maximum number of bits of information (from secret message) that we can replace in center pixel.

In this section, the proposed scheme is described in three parts: the new quantization range table is based on the perfect square number, embedding procedure, and extraction procedure

A. Quantized Range Table

The new designed range table is based on perfect square number[1] and is described in table 1.For each pixel value difference ,choose the nearest perfect square number n, then we have range $n^2-n <= n^2 < n^2+n-1$ for n [1,16]. The width of this range is $n^2 + n - n^2 – n = 2n$, and embedding bit length is $m=[\log_2 2n]$. For each range, if the width of range is larger than 2^m, then we divide this range in two subranges : $[n^2 – n, n^2 +n – 2^m]$ and $[n^2 + n – 2^m +1, n^2 + n -1]$.

By the definition of subrange, if bits to be embedded m +1 equals one of m+1 lsb bits in the first subrange, then we can embed m+1 bits is first subrange. Otherwise the second subrange is used with embedding capacity m.

B. Embedding Algorithm

For embedding the secret data, we are using color image. The embedding procedure is explained below.

Table I: The quantized range table based on perfect square number

n	Range	Sub-ranges	t
1	[0, 1]	[0, 1]	1
2	[2, 5]	[2, 5]	2
3	[6, 11]	[6, 7]	3
		[8, 11]	2
4	[12, 19]	[12, 19]	3
5	[20, 29]	[20, 21]	4
		[22, 29]	3
6	[30, 41]	[30, 33]	4
		[34, 41]	3
7	[42, 55]	[42, 47]	4
		[48, 55]	3
8	[56, 71]	[56, 71]	4
9	[72, 89]	[72, 73]	5
		[74, 89]	4
10	[90, 109]	[90, 93]	5
		[94, 109]	4
11	[110, 131]	[110, 115]	5
		[116, 131]	4
12	[132, 155]	[132, 139]	5
		[140, 155]	4
13	[156, 181]	[156, 165]	5
		[166, 181]	4
14	[182, 209]	[182, 193]	5
		[194, 209]	4
15	[210, 239]	[210, 223]	5
		[224, 239]	4
16	[240, 255]	[240, 255]	4

- Read Cover Image and separate its RGB components.
- Take the selected pixel in each colour domain and make a matrix of 9X9 pixel by placing selected pixel in center of matrix.
- Calculate the difference value ***'d_i '*** between two consecutive pixels, that are above and to the left side of center pixel.
- Now find the highest difference value among four difference values of each colour plane.
- Find nearest perfect square number n for two difference values and compute the length of embedding bits t =[$\log_2 2n$]. There are two cases: Search the first subrange and find a value p in the sub range such that LSB(p, t+1) = Secret (t+1) and then set d'=p. Otherwise search the second subrange and find a p in subrange such that LSB (p, t) = Secret (t) and then set d'=p.
- Calculating the difference between d_i' and di for finding the value of m.
- Modify the values of P_i and P_{i+1} by the original PVD method as discussed in review section. (where P_i and P_{i+1} are center pixels from matrix of R and B color planes). Here only R and B components are selected because these two components add very little to Y value and uniformly distributing the difference does not alter their values to much extent and Y values remains almost same
- Now repeat the steps for next pixel that is immediate neighbour to center pixel and repeat the process for all pixels moving to right side and then down in the color selected block of image.

When you submit your final version, after your paper has been accepted, prepare it in two-column format, including figures and tables.

C. *Extraction Algorithm*

For the extraction process, the range table, which is used at encoding, is required. The following steps used for extracting the hidden data:

- Read this Cover Image and separate its RGB components.
- Starting from the last pixel, consider it as center pixel of selected block for all three colour components
- Now calculate the difference values of other pixels of matrix
- Now find the greatest difference value among the differences.
- Find nearest perfect square number n for two difference values and compute the length of embedding bits t =[$\log_2 2n$]. Search the sub range and determine which subrange it belongs to, and extract the secret data secret m+1 = LSB d',m+1 for first sub range and secret m = LSB d',m for second sub range. by subtracting the lower value of selected range from difference value d_i
- Now convert this decimal value into binary equivalent. These binary bits are the original data.
- Now repeat the process for other pixels by moving right to left and then to top for an image and extract the message bits before the previously extracted bits.
- After that these binary information is converted in to watermark image

IV. EXPERIMENTAL RESULTS

We tested the reliability and efficiency of the proposed system using PSNR, MSE and Capacity as stego image quality measures. The method is tested on various color images. The original and corresponding stego images are shown in figure 1. The computing of the PSNR, the widely-used image quality measure, is very easy and fast. Therefore, PSNR is the most common metric used to measure the quality of digital images in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods. Mostly, digital image steganography uses the PSNR to evaluate the quality of stego images or the imperceptibility of steganography methods. Thus, PSNR measures the efficiency of a particular steganography method over another in terms of imperceptibility or stego image. This influenced our choice to use the PSNR measure in order to evaluate the quality of stego images. Table II, shows the comparison between proposed method and T.Seng's[1] method. The comparison shows that the proposed method is better in performance and shows improved PSNR ,MSE valies. The efficiency of the proposed method in this paper is compared against T.Seng's method[1]. The results, as presented in Table , show good improvement in similarity between the original and the extracted watermark in comparison with the previous methods.

V. CONCLUSIONS

In this paper, we have discussed a steganographic method for data hiding by using quantized tange table and local area pixel differencing. Experimental results show the proposed scheme has a much better performance than Tseng's scheme in terms of stego-image quality. The steganographic capacity and imperceptibility represent the most important aspects of any steganography technique. Thus, this paper addresses and improves these two fundamental aspects of digital steganography methods: steganographic capacity and stego image quality. This research proposed novel steganography methods in order to increase the steganographic capacity and enhance the imperceptibility (i.e. stego image quality).

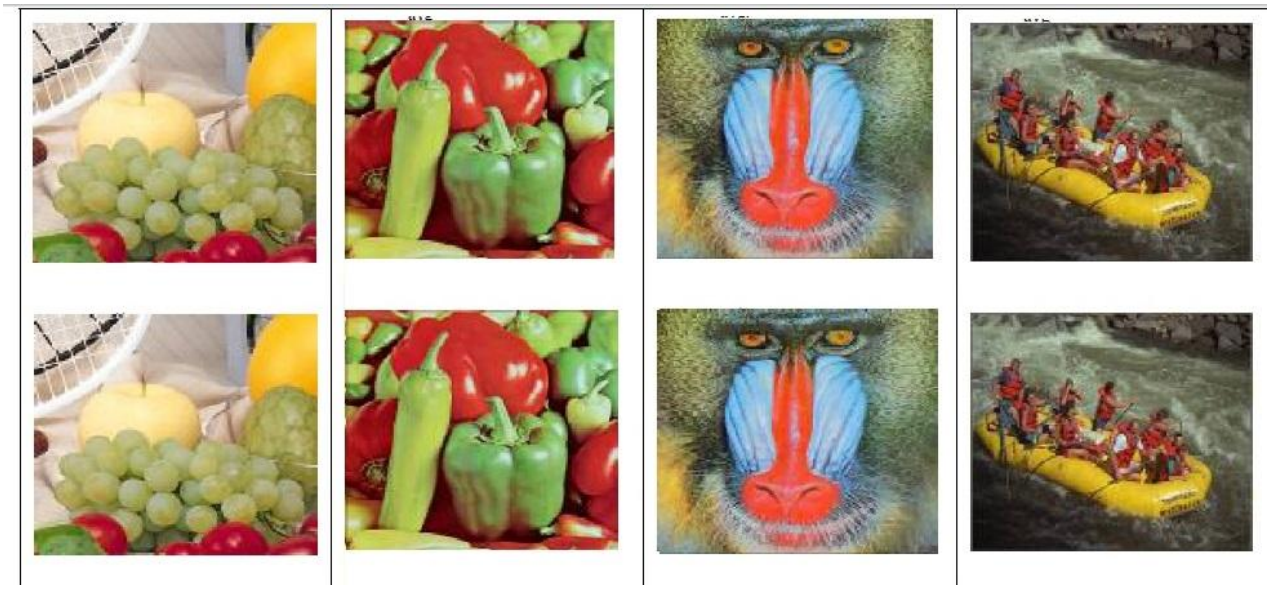

Figure 1 Cover and Stego Images

Table II : Result analysis

Tseng's[1] Mathod			Our Proposed System			
	PSNR	MSE	Capacity	PSNR	MSE	Execution Time
Fruits	49.23	0.85	Minimum capacity by considering only 2 bits inserted in pixels: 1040400 bits	50.09	0.79	20.71
Pepper	46.17	1.15		46.95	1.14	18.50
Baboon	47.87	1.10		48.08	1.00	16.74
Boat	49.10	0.92		48.86	0.91	19.29

REFERENCES

[1] H.W.Tseng and H.S.Leng,"A Steganographic Method Based on PixelValue Differencing and Perfect Square Number"Hindwai Journal of Applied Mathematics,2013.

[2] J. K. Mandal and Debashis Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow." CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 93–102, 2012.

[3] K.C. Chang, C.P. Chang, P.S.Huang and T.M. Tu, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Volume. 3, No. 2, June 2008.

[4] Regunathan Radhakrishnan, Kulesh Shanmugasundaram and Nasir Memon, "Data Masking: A Secure-Covert Channel Paradigm".

[5] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing, "Pattern Recognition Letters, Vol. 24, pp.1613-1626, 2003.

[6] S.K. Bandyopadhyay , D. Bhattacharyya ,D. Ganguly , S.Mukherjee and P. Das , "A Tutorial Review on Steganography"

[7] Ms.B.Veera Jyothi, Dr.S.M.Verma and Dr.C.Uma Shanker, "Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification" International Journal of Computer Applications (0975 – 8887) Volume 5– No.5, August 2010

[8] C. Cachin, "An Information-Theoretic Model for Steganography",in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.