An Improved Image Steganography Technique using Quantized Range Table Pixel Value Differencing

Munish Kumar
M.Tech, Department of Electronics and Communication Engineering
Guru Teg Bhadhur Institute of Engineering & Technology, Malout, Punjab, India

Sukhjit Singh
Assistant Professor, Department of Electronics and Communication Engineering
Guru Teg Bhadhur Institute of Engineering & Technology, Malout, Punjab, India

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 improved pixel value differencing in a segment of four pixels and range table using perfect square number is proposed in this paper. The experimental results show that the proposed method is highly efficient in hiding the information and also the proposed scheme is secured against the RS detection attack. Besides, the embedded secret information can be extracted from stego-image without the assistance of original image.

General Terms
Protocol, quantized range table, pixel, algorithm

Keywords
Information hiding, pixel value differencing, steganography, stego-image

1. 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". In ancient times, messages were hidden on the back of wax tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been used for serious espionage by spies and terrorists.

2. PAGE SIZE
In modern terms, steganography[5] is usually implemented computationally; where cover objects like text files, images, audio files, and video files are used as such a way so that a secret message can be embedded within these used multimedia files . Steganography can be divided into five types depending upon the nature of cover object.

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

2.1 Text Steganography
For hiding the information in text, the text Steganography is historically the most important type of steganography. This method concealed a secret message in every nth letter of every word of a text message.In digital files, text steganography with digital files is not used very often because the text files have a very small amount of redundant data [6].

2.2 Image Steganography
In the image steganography, to hide the information, every bit of information may be encoded in the image or selectively embed the message in "noisy" areas because these areas draw less attention for color variation. The information may also be scattered randomly throughout the image [6].

2.3 Audio Steganography
In the audio steganography system, secret data is embedded in digital sound. This process is done by slightly altering the binary sequence of a sound file. One of most different techniques of audio steganography is masking which exploits the properties of the human ear to hide information unnoticeably.

2.4 Video Steganography
Generally, video files are a collection of images and sounds, therefore the present techniques of image and audio Steganography can be applied in video files. The advantage of video Steganography is that there are large amount of data which can be hidden in video in the form of moving stream of images and sounds. So any small noticeable distortions may be unobserved by humans due to the continuous flow of information.

2.5 Protocol Steganography
The term protocol steganography is a technique of hiding information within messages and network control protocols used in network transmission. In the layers of the OSI network model, there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/ IP packet in some fields that are either optional or are never used.

3. STEGANOGRAPHY SYSTEM
When a steganographic system [7]is developed, it is important to think what the most efficient cover work should be used, and also how the stegogramme, which is response of steganography encoder, to reach its recipient. With the help of Internet, there are many different ways to send messages to

people without anyone knowing they exist. For example, an image stegogramme could be sent to a recipient though email or it may be posted on a web forum for all to see.

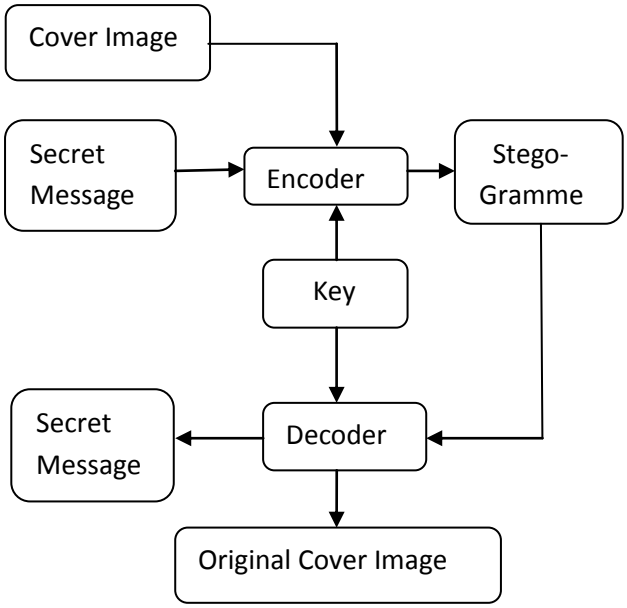

Figure 1

4. REVIEW OF PVD METHOD

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, Pi and Pi+1. A difference value is generated by subtracting Pi from Pi+1 in each block. The difference value is represented by 'di'. The set of all difference values lies a range from -255 to 255. So |di| 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 Rk. Here the value of k varies from 1to n like k=1,2,….n. where the range is 0 to 255. The loweimit and the upper limit are represented by lk and uk respectively, then Rk [lk, uk]. The width of Rk is calculated using wk=uk-lk+1.wk 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 pixels pi and pi+1 for each segment in the cover image. This difference is given by di=|pi+1-pi |.
- Find the optimal range in which the calculated difference value lies in the range table by using di. This is calculated as Rk=min(uk- di), where uk ≥di 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=log2wi. Where wi is the width of the range where the pixel difference di lies.
- Read t bits from binary secret data and convert it into its decimal value b.
- Now finding the new difference value di' using di'=li +b.
- Modify the values of pi 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=|di' - di|. 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'=|Pi'-P i+1'|.Now finding the optimum range Ri of di'.Compute the b' by b'= di'-li. Convert b' into binary of't' bits, where t=log2 wi. These t bits are the hidden secret data.

5. PROPOSED METHOD

In this method we are dividing the cover image into number of segments of four pixels. Each segment is processed separately. In each segment, we calculated inter pixel differences and two pairs with highest difference values are selected for embedding the information. Tseng[1] had designed a new quantized range table based on perfect square number and it is used with improved pixel value differencing technique that increases the embedding capacity and imperceptibility of the system. In this section, the proposed scheme is described in three parts: the new quantized range table based upon perfect square number, embedding procedure and extraction procedure.

5.1 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 n2-n <= n2 < n2+n-1 for n [1,16]. The width of this range is n2 + n - n2 – n =2n, and embedding bit length is t=[log22n]. For each range, if the width of range is larger than 2t, then we divide this range in two subranges : [n2 – n, n2 +n – 2t] and [n2 + n – 2t +1, n2 + n -1].

Table1: 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

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

5.2 Embedding Algorithm

Step 1: Take a Gray Scale Cover – Image of size 512 * 512.

Step 2: Read this Cover Image.

Step 3: partitioning the image which image is used as a cover image for hiding the information into segments. A segment consists of two consecutive non- overlapping pixel pairs.

Step 4: Calculate the difference value 'di' for each segment of two consecutive non-overlapping pixels pi and p(i+1).This is given by di=|pi - p(i+1) |.

Step 5: Now find the two highest difference values which are not made by a Common pixel value.

Step 6: Find nearest perfect square number n for two difference values and compute the length of embedding bits t =[log22n]. 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.

Step 7: Calculating the difference between di' and di for finding the value of m.

Step 10: Now modify the pixel values of each pair according to basic PVD described earlier.

Step 11: Repeat the steps from 4 to 12 for embedding the whole secret data into segments.

For example we have selected the segment with following pixel values

164	186
142	172

Calculate inter pixel value difference values :

d1=22 ; d2=14; d3=30; d4=22

Select highest pixel difference values with no common pixel i.e. d1=22 and d3=30.The nearest perfect square number for both difference values is n=5 and the no. of bits can be embedded t=log2(2n)=3.The following two conditions are discussed.

Case 1 : Secret data is "0100" or "0101"

In the first subrange for selected n value [20,21] and no. of bits to be embedded are t+1=4, the four LSBs are same as secret data. Suppose the data to be embedded is "0101", then the new difference value would be d1'=21[00010101].m=d1'-d1=1 and modified pixel values are [165,186].

Case 2: Secret data is "011"

In the first sub range there is no matching LSB, so we will go with second sub range [22,29] and no. of bits to be embedded are t=3.The new difference value from sub range is d3'=27[00011011] and m=d3'-d3=3. The modified pixel values are [144,171].

5.3 Extraction Algorithm

The following steps used for extracting the hidden data are as follows:

Step 1: Read the stego –image.

Step 2: Partition the stego-image into pixel segments consist of two consecutive non-overlapping pixel pairs.

Step 3: Now calculate the difference value di of two consecutive pixels of each segment by using the formula di=|pi-pi+1| .

Step 4: Now find the two highest difference values which are not made by a common pixel value.

Step 5: Find the appropriate range Ri for the difference di.

Step 6: Find nearest perfect square number n for two difference values and compute the length of embedding bits t =[log22n]. Search the sub range and determine which subrange it belongs to, and extract the secret data (secret (t+1)) = (LSB d',t+1) for first sub range and (secret t) = (LSB d',t) for second sub range. Finally we extract all secret data.

Step 7:After that, these binary information is converted in to the string. This string is known as original information.

For example we have selected the same segment with following pixel values

165	186
144	171

Calculate inter pixel value difference values :

d1=21 ; d2=15; d3=27; d4=21

Select highest pixel difference values with no common pixel i.e. d1=21 and d3=27.The nearest perfect square number for both difference values is n=5. The no bits embedded in pixel

pair are t+1=4 (t=log2(2n)) for first sub range and t=3 for second subrange.

For first difference value d1=21 from first subrange, thus secret embedded data is last four LSB of 21 i.e. 0101 and for second difference value d3=27, the secret embedded data is last three LSB of 27 i.e. 011. Like this all secret bits are recovered.

5.3.1.1 Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

5.3.1.2 Subsubsections

The heading for subsubsections should be in Times New Roman 11-point italic with initial letters capitalized.

6. EXPERIMENTAL RESULTS

The proposed method is implemented on various images. We had given a theoretical analysis of our research and experimental results performed on various cover images show that the new proposed scheme with quantized range table and improved pixel value differencing is better in performance. The hiding capacity (in bits), PSNR values (in dB), MSE values and Execution Time (in seconds) are calculated for our proposed scheme. The listed values in

Fig 2(a). Cover-Image Fig 2(b). Stego-Image

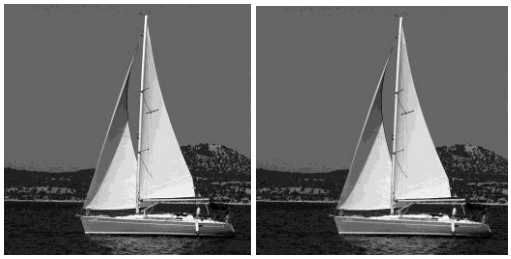

Fig 3(a). Cover-Image Fig 3(b). Stego-Image

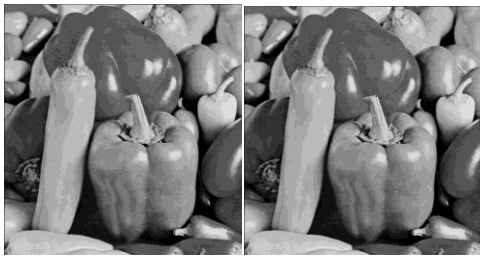

Fig 4(a). Cover-Image Fig 4(b). Stego-Image

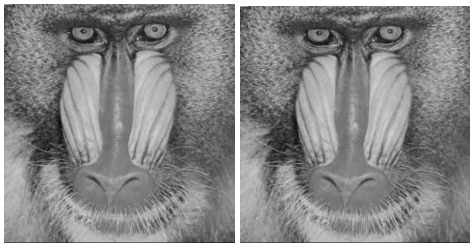

Fig 5(a) Cover-Image Fig 5(b) Stego-Image

Table 2 are the average results after embedding randomly generated bits from 1 to 50,000 into the gray scale cover images of size 512 *512. The minimum capacity of embedding data with proposed scheme and according to the range table of proposed scheme in a gray scale cover image of size 512 * 512 is 264144 (on average if we embed 2 bits in each pair). We have used MATLAB to implement our proposed scheme. The comparison between the parameters of proposed method and Tseng and Leng 's[1] method are shown in Table2.

7. CONCLUSIONS

In this paper, we have discussed a new and more effective range table designed by Tseng[1] with improved pixel value differencing based on highest pixel value difference among four pixel values. Our research provides a new view point that if we choose the proper width for each range and use the proposed pixel value differencing technique, we can obtain better image quality and higher capacity.The theoretical analysis and experimental results shows that proposed scheme is well defined and better results than Tseng and Leng's[1] method.

8. ACKNOWLEDGMENTS

This research paper is made poosible through the help and support from everyone, including: parents, teachers, family and friends. We would specially like to thank Kulbhushan Singla, Assistant professor for his support and encouragement.We are also thankful to the intellectual beings whose references we have taken while writing this paper.

9. REFERENCES

[1] H.W.Tseng and H.S.Leng,"A Steganographic Method Based on Pixel Value 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, EA, 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 vol. 1525, pp. 306-318, 1998.

[8] C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop

Table 2: Comparison of Results

	Tseng and Leng's[1] method.			**Our Proposed System**			
	Capacity	PSNR	MSE	Capacity	PSNR	MSE	Execution Time
Lena	198209	49.23	0.85	262144	50.09	0.79	20.71
Baboon	229459	46.17	1.15	262144	46.95	1.14	18.50
Boat	209494	47.87	1.10	262144	48.08	1.00	16.74
Pepper	200831	49.10	0.92	262144	48.86	0.91	19.29