Color Image Steganography using Combined Pixel Value Differencing and Pixel Indicator Technique in Spatial Domain

M.G.Gouthamanaath
Full-Time Research Scholar
Department of Computer Science
Government Arts College (Autonomous),
Salem-7

A.Kangaiammal, Ph.D
Assistant Professor/Computer Applications
Department of Computer Science
Government Arts College (Autonomous),
Salem-7

ABSTRACT
Steganography refers to the art of concealed writing which doesn't reveal a clue to an intruder who intended to access private information without authorization. Conventional schemes of spatial domain methods are prone to suspicion of secret information. Proposed technique combines both Pixel Value Differencing as well as Pixel Indicator technique ensuring higher security in addition no suspicion. In this work, any two selected planes from RGB planes of the image is partitioned into two pixel blocks and takes the difference between them. After scanning all the pixels, encrypted secret data is embedded inside the selected pixels in a random order. One plane acts as an indicator; any one of the other two planes holds the secret information. In this paper, by combining these methods the proposed work has been formulated for an optimal solution with high security, less computational cost and good image quality. The experimental results obtained shows that optimal solution with minimal cost and good image quality is achieved.

General Terms
Image Processing, Information Security, Steganography, Color Image Steganography.

Keywords
Pixel Value Differencing, Pixel Indicator technique, Spatial Domain, Image Steganography, Color Image Steganography.

1. INTRODUCTION
Steganography is the process of concealed writing which leads to better security for the secret data. In ancient days steganography is practiced in several ways. If a roman king wants to communicate with secrecy, he shaves the head of his slave and writes something on his head and covered it with a cap or wait for the hair to grow. When the slaves go to the destination, the receiver only knows the secret message that is written on his head [8].

In digital steganography the secret message is sent through the cover media. Media types are image, audio, video and animation. Even protocols on network carry some steganography methods to embed secret information [12]. The selection of media is associated with computational cost, level of security and embedding capacity. Image is one of the most chosen media, because it is having less complex structure than other media. Spatial domain deals with physical properties and transform domain with frequencies. The different types of steganography are depicted in Fig. 1 [2].

Spatial domain steganography is known for its embedding capacity and its implementation with less computational cost is noteworthy [11]. Transform domain steganography converts all the pixel values into transform domain coefficients and then it embeds the secret information. Even though transform domain steganography is known for its robustness lots of pitfall present in it. In Discrete Cosine Transform and Discrete Wavelet Transform that changes the x,y co-ordinates of pixel into transform coefficients and secret message is embedded into LSB of coefficients. Basically Transform domain steganography has complex structure and computational cost is high and also the embedding capacity is very lesser than spatial domain [6].

Least Significant Bit (LSB) substitution method takes the LSB of every color value and embeds the secret information in it. In LSB matching methods, the LSB is modified as per the index created in source and destination, and the matching is done for retrieving hidden data [3]. Pixel Value Differencing method (PVD) converts pixel into blocks and finds the difference between the values of the pixels [13]. Based on those difference values harder and softer regions of image are classified. The harder regions which have higher difference are apt for embedding secret information with lesser suspicion. In pixel indicator technique any one of the plane or bits is to indicate the pixel that has secret bits embedded in it [4].

2. RELATED WORK
A Pixel Value Differencing method was proposed by [5] in 2013. This method is partitioning an image into non-overlapping blocks of 2 pixels say p_i and p_{i+1}. In order to estimate the number of bits to be embedded into the pixels of cover image, authors of [5] designed a range table R_j (j=1,2,3…6) with continuous range between 0 and 255. There are six ranges in the range table as R_1 = [0, 7], R_2 = [8, 15], R_3 = [16, 31], R_4 = [32, 63], R_5 = [64, 127], R_6 = [128,255]. The lower and upper bound values of each ranges R_j are called l_j and u_j, respectively,(i.e. $Rj \in [li, ui], j = 1,2,\ldots 6$). Also, the width of Rj is denoted as [Rj]. After that, in p_i and p_{i+1} of each block is embedded with secret bits using the following procedure.

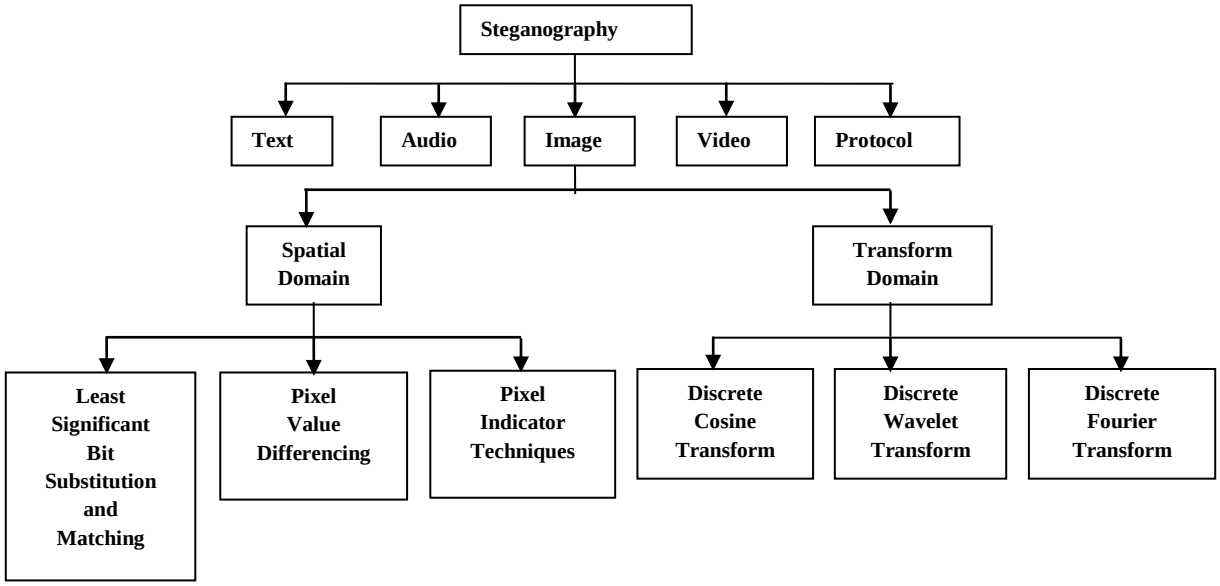

Fig. 1. Types of Steganography

Calculate the difference value d_i for each block with two successive pixels by using $\boldsymbol{d_i = |p_i + p_{i+1}|}$.

1. Determine the range for which di belongs to (e.g. $R_j \in [l_i, u_i]$).

Calculate how many bits tj of secret data can be embedded in each pair p_i and p_{i+1} by using $\boldsymbol{t_j = [\mathbf{Log\,2}\,(|R_j|)]}$

2. Read t_j bits from binary secret data and transform the binary bit-stream into a decimal value si. For instance, if the bit-stream = 101, then $s_i = 5$.
3. Compute difference value d_i'as $\boldsymbol{d_i' = l_i + s_i}$
4. Modify the p_i and p_{i+1}

Where $\boldsymbol{z = |d_i - d_i'|}$. Finally, ($p_i$, p_{i+1}) is replaced by (p_i',p_{i+1}') and the process is repeated for each block to obtain the stego-image. In destination, this process is reversed as well and the secret message is recovered from it. Authors of [5] proposed a new method namely PVD method with LSB replacement which differs from the above method in secret message embedding. Let six bit secret data be s = a1, a2, a3, a4, a5, a6.

1. Place a1, a2, a3 into 3-LSB of p_i

2. Place a4,a5,a6 into 3-LSB of pi to obtain $p_i'_{+1.}$

$$(\boldsymbol{p_i' - p_{i+1}'}) = \begin{Bmatrix} (\boldsymbol{p_i + [z/2], p_{i+1} - [z/2]}))\ \boldsymbol{if\ p_i \geq p_{i+1}\ and\ d_i' > d_i} \\ (\boldsymbol{p_i - [z/2], p_{i+1} + [z/2]}))\ \boldsymbol{if\ p_i < p_{i+1}\ and\ d_i' > d_i} \\ (\boldsymbol{p_i - [z/2], p_{i+1} + [z/2]}))\ \boldsymbol{if\ p_i \geq p_{i+1}\ and\ d_i' \leq d_i} \\ (\boldsymbol{p_i + [z/2], p_{i+1} - [z/2]}))\ \boldsymbol{if\ p_i < p_{i+1}\ and\ d_i' \leq d_i} \end{Bmatrix} \quad (1)$$

3.Calculate the new difference value $\boldsymbol{d_i' = |p_i' - p_{i+1}'|}$.

4. If difference value d_i' belongs to the higher level, perform readjusting operation by

$$(\boldsymbol{p_i', p_{i+1}'}) = \begin{Bmatrix} \boldsymbol{p_i' - 8, p_{i+1}' + 8\ if\ p_i' \geq p_{i+1}'} \\ \boldsymbol{p_i' + 8, p_{i+1}' - 8\ if\ p_i' \leq p_{i+1}'} \end{Bmatrix} \quad (2)$$

Pixel indicator technique indicates the receiver that the secret bit is hidden inside the pixel. Secret bits are embedded based on the order (Table 1).

Table 1. Indicator channel bits and indication in channels

Indicator Channel	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	No hidden data
10	2 bits of data	2 bits of data
11	2 bits of data	2 bits of data

3. PROPOSED METHOD

In order to achieve robustness in spatial domain steganography combining PVD and Pixel indicator technique together to get good quality stego-image [2]. R and G planes are used for embedding secret information and B plane is used for indicating the secret bits. The proposed algorithm is given below.

Embedding Algorithm

1. Separate the R,G,B planes.

2 $$\begin{matrix} \sum_{i=1}^{n} \boldsymbol{R(i)\ \ where\ 1 \leq i \leq n,} \\ \sum_{i=1}^{n} \boldsymbol{G(i)\ \ where\ 1 \leq i \leq n,} \end{matrix} \quad (1)$$

Where n is the total number of pixels

3. Calculate the difference $\boldsymbol{d_i = p_i - p_i'}$ **where** $\boldsymbol{0 \leq d_i \leq 255}$

4. Determine l_k and u_k where l_k is lower bound and u_k is upper bound.

5. Remove the last range of lower bound where $d_i' = d_i - l_k$which is easily predictable by the intruder and define the eligible pixels to embed the secret data.

$$\sum_{i=1}^{n'} \boldsymbol{d'(i)\ where\ 1 \leq i \leq n'} \ldots\ldots\ldots (2)$$

where, n' = number of eligible pixels.

6. Pseudo random numbers are generated with a key(seed) .

$$\sum_{i=1}^{n'} \boldsymbol{rand(i)\ where\ 1 \le i \le n'} \ldots\ldots\ldots (3)$$

where n' = number of eligible pixels

7. Combining (1),(2),(3) we get (4)

$$\sum_{i=1}^{n'} \boldsymbol{B\left(Rand\left(Bin\left(En(s(j))\right)\right)\right)\ where\ 1 \le i \le n'} \ldots\ldots\ldots (4)$$

where

- $1 \le i \le n'$, g the indicator
- En – Encryption function that apply RS2 algorithm on secret message.
- Bin – Bin function converts encrypted value into binary value
- Rand – Random numbers with seed [1].
- B – B-plane for indicator bit embedding.

8. Binary values are embedded randomly through n' and the indicator channel embedded with the new table of bit indicators as given in Table-2.

Table 2. 3-bit indicator in channel 1 and 2

Indicator Channel	Channel 1	Channel 2
000	No hidden data	No hidden data
001	2 bits of data	2 bits of data
010	4 bits of data	4 bits of data
011	4 bits of data	4 bits of data
100	No hidden data	No hidden data

Random numbers are generated and based on which the secret data is embedded in it. In destination, reverse the same process to extract the secret data in it [2]. The pixel indicator technique acts like a parity bit. Unlike other Pixel indicator technique, here 3 bits are used to indicate the number of bits embedded in it. By calculating the Peak Signal Noise Ratio (PSNR) value for the stego-image it would be realized that it yields optimum result in comparison to few other existing methods.

4. EXPERIMENT RESULTS AND DISCUSSIONS

4.1 PSNR and MSE

PSNR and Mean Square Error (MSE) are used for comparing the squared error between the original image and the reconstructed image. There is an inverse relationship between PSNR and MSE. Therefore, a higher PSNR value indicates that the image quality is high and hence it is better. As many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale [9].

PSNR and Mean Square Error (MSE) are calculated through the following formula [10].

$$MSE = \left({}^{1}/_{(m \times n)}\right) \times sum(sum((f-g)^2))$$

$$PSNR = {}^{20 \times \log\left(max(max(f))\right)}/_{((MSE)^{0.5})}$$

In Table 3, Image capacity is the maximum number of pixels available to hide an image whereas payload is the secret message embedded inside the cover image and the eligible pixels are n' determined by the algorithm.

Table 3. PSNR value generated for Samples

Cover Image	Image capacity	Payload in bits	PSNR Value
Lena	140356	6963	54.50
Baboon	132864	6536	52.10
jet	187272	7150	55.35
boat	218934	9545	56.12
pepper	146521	6530	54.63

Table 3 shows the PSNR values obtained for the samples images before embedding the secret message in an image; while Table 4 shows the comparative results of the proposed with existing methods of stego-image. The results reveal that the PSNR obtained is comparatively very high and that assures the image quality as good one. It is interesting to note that high PSNR values obtained for higher payload.

Table 4. Comparative Results

Cover Image	Wu and Tsai's Method		Hsien and Hui Method		Proposed Method	
	Pay-load	PSNR	Pay-load	PSNR	Pay-load	PSNR
Lena	51219	38.94	12560	40.21	22920	54.15
Baboon	57146	33.43	14873	41.35	21546	56.17
Jet	51224	37.42	18529	40.85	25450	54.45
Peppers	50907	37.07	19583	41.53	23861	56.52

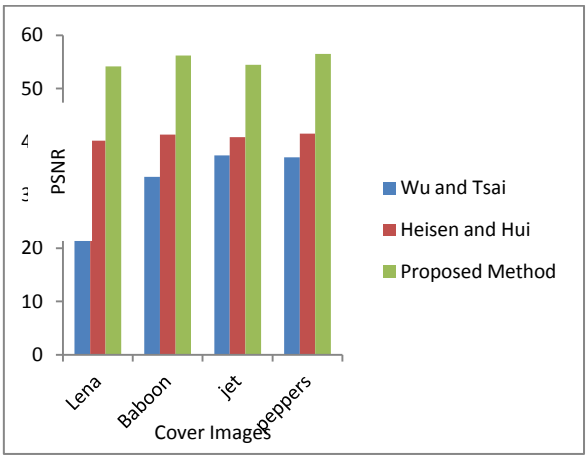

Fig. 2. Comparative PSNR Test Results

From the chart given in Fig. 2 it is very evident that the PSNR attained during stego-image preparation varies significantly with the existing methods. Wu and Tsai's approach could yield the minimum yet Heisen and Hui has improved PSNR and hence image quality. On the other hand, the proposed

approach yields overwhelming attainment with above 50. This depicts that the proposed method achieve optimum and better solution with minimum cost and fine image quality.

5. CONCLUSION

This paper unveils the fact that by combining PVD as well as Pixel Indicator Techniques, a high resolution stego-image with high PSNR rate can be obtained. It is demonstrated from the experiments that for high payload, better PSNR value is possible. The PSNR is improved on stego-image unlike the usual; improved image quality is ensured. Hence the color image steganography using the proposed approach ensures optimum solution. As a future work, the author intends to implement a different mix and match of approaches to get still better results than the present steganographers achieved so far.

6. ACKNOWLEDGEMENT

My sincere thanks to my research supervisor Dr.A.Kangaiammal who supported me to successfully work and develop a paper.

7. REFERENCES

[1] Adnan Abdul-Aziz Gutub, "Highly Secured And Randomized Image Steganographic Algorithm", Journal of Global Research in Computer Science, Vol.3, No.9, September 2012.

[2] Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1, February 2010.

[3] Bender D.W., N.M. Gruhl, A. Lu, Techniques for Data hiding, IBM Systems Journal, Vol. 35, 1996, pp.313–316.

[4] Chung Ming Wang and Nan-I Wu, "A High Quality Steganographic method with pixel value differencing and modulus function", International Journal of System and Software, 2007.

[5] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc.-Vis. Image Signal Process., Vol.152, No.5, October 2005.

[6] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath, "A Secure Color Image Steganography in Transform Domain", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013.

[7] Hsien-Wen Tseng1 and Hui-Shih Leng "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics Volume 2013.

[8] Jain Y. K. and Ahirwal R. R., "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, March 2010.

[9] Niveditta Thakur, Swapna Devi, "A New Method for Color Image Quality Assessment". International Journal of Computer Applications, Vol.15, No.2, February 2011.

[10] Prabhakar.Telagarapu, V.Jagan Naveen, A.Lakshmi..Prasanthi, G.Vijaya Santh, "Image Compression Using DCT and Wavelet Transformations", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.4, No.3, September, 2011.

[11] Sravanthi G.S., Sunitha Devi B., Riyazoddin S.M. and Janga Reddy M., "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision Vol.12, No.15, 2012.

[12] Sumathi C.P., Santanam T.and Umamaheswari G., "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[13] Xin Liao A., Qiao-yan Wen A. , JIE Zhang B., "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", Journal of Visual Communication and Image Representation, 2011.