International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

# A Steganographic Method with an Overlapping of Three Pixel Block of Image

**Jayeeta Majumder, Chittaranjan Pradhan**

***Abstract:*** ***In this paper a new image steganographic technique has been proposed which is capable of hiding data and produces a stego image that is totally indistinguishable from the original image by the human eye. To estimate the contrast and smoothness of pixels we check the relation between neighboring pixels. Our method first arranges the pixel in ascending manner, then takes the highest pixel value common with the other two pixels and then applies the pixel value differencing (PVD) method.*** *To hide the secret data PVD technique is used in each pixel block. The two overlapping blocks are readjusted to attain the modified three-pixel components.* ***Then calculate the new stego pixel block. In this way, take the middle and lowest pixel as the common pixel and apply the same procedure. In comparison, we get that if the highest value pixel value takes as a common one then the data hiding capacity is increased.*** *The embedding capacity of the cover image is increased by using the pixel block overlapping mechanism. It has been tested on a set of images and also maintains the visual quality of the image.*

***Keywords:*** *Data Hiding, Image Security, Pixel Value Differencing, PSNR, Steganography, Histogram*

## I. INTRODUCTION

In modern days, we need to protect our confidential data during transmission through a public channel. Generally, we process our secret data before transmission. It changes the context of the data into an unreadable form, but only the authorized person can retrieve the original data using reversible operation. In modern days different techniques are available to protect the data. Several cryptographic techniques are present to do this. To contrast this, steganography is to protect the secrecy of the data. Here, the cover media like audio, video, image are used as a carrier to embed the secret data. The cover media along with secret data is known as stego data. The aim of both cryptography and steganography is the same. Image data are frequently used in different applications.

## II. RELATED WORK

Through the literature survey, we found a number of image-based steganographic schemes. The LSB (Least Significant Bit) is the widely used method for high data hiding capacity. The basic LSB method only considers three LSB bits replacements. In this method, after replacement, the stego image is visually good and also increase embedding capacity. By using the optimal pixel adjustment process the visual quality can be improved.

**Revised Manuscript Received on February 28, 2020.**
***** Correspondence Author
**Jayeeta Majumder*,** Research Scholar, KIIT University, Orissa, India, jem2003_kolkata@yahoo.co.in.
**Chittaranjan Pradhan**, Associate Professor, CSE Department, KIIT University, Orissa, India.



In Yang [7] scheme, the cover pixels are not directly modified. The secret message bits are toggled and the new toggled patterns are recorded for extracting the secret message. Later Chen [8] proposed a modified scheme, where modulus function is used with LSB substitution which improves the visual quality for the stego image. To minimize the distortion in the stego image the repetition of the secret message is considered.
Then, Xu, et al. [9] proposed a steganographic scheme with a fixed payload. Some researchers [10-12] designed edge-based steganographic schemes. In paper [11], the authors classified the pixels into two categories. Edge-pixels and non-edge pixels.
Islam et.al [12] proposes a method that increases the high visual quality of the stego image. The process enhances the security level. Wu & Tsai [13] introduces Pixel Value Differencing (PVD) method. Khodei & Faez [14] design a combination of LSB & PVD Method. It improves the embedding Capacity.
In the literature survey, several different PVD methods are found. A tri-way PVD approach with the steganalysis method is discussed by Lee et al. [3]. Tseng & Leng [15] used the perfect square number (PSN) which improves the traditional PVD technique. Here, the secret message merge with the PSNR. Liao et.al.[16] developed a four-pixel differencing method. Swain [17] introduces 2X2 pixel non-overlapping PVD techniques.
In paper [18], where 3X3 non-overlapping block images are considered. To improve payload capacity a seven-directional PVD scheme [19] is considered. Using modulus function Zhao et. al. [20] proposed new PVD techniques. In paper [21], an adaptive approach falling-off boundary is discussed. In paper [22], the secret data bits are embedded in sequential order into another image pixel. In the paper [23] the LSB technique is used where the reference of the color plane is used to hide the secret bits.
In the proposed scheme, to form the overlapping pixel block, the neighboring pixel is grouped into two pairs, namely (p1, p2) and (p2, p3). For embedding the secret message bits, PVD is applied to each pair. The proposed readjustment process is applied on each pair to get the final modified stego pixel block, with p1, p2, and p3 components. In the decoding process, PVD is applicable to extract the secret message bits from the stego color pixel.
The proposed scheme will improve the embedding capacity due to the consideration of overlapping block concepts. The paper is organized as follows: Section 3 presents the basic idea of the PVD method. The detail of the proposed scheme with mathematical explanation is described in section 4 and section 5 respectively. Finally, section 6 concludes the paper.

## III. PIXEL VALUE DIFFERENCING (PVD) METHOD

In the pixel value differencing method [13] the cover image is generally a grey level image and a different size of secret message bits are used as secret data. Through a raster scan order, the cover image is divided into non-overlapping blocks with size 1X2. Consider $P_i$ and $P_{i+1}$ are the two consecutive pixels on the ith block. The difference value, $d_i$, is calculated by $d_i=|P_i-P_{i+1}|$. We take the absolute value of $d_i$ which represents the variation of each block. A lower value of $d_i$ signifies the presence of a smooth area, and greater value is in the edge area. To maintain the intensity values of the grey scale image the values of $d_i$ are in the range of [0, 255]. The boundary of range R is denoted by [$lower_i$, $upper_i$ ]. The number of embedded secret bit sequences (t) in two consecutive pixels depends on the quantization range table and it is computed as $t = (\log_2 (upper_i - lower_i) + 1)$. The obtained bit sequence is converted into decimal value, $t_d$. The new difference value ($d_i$') is obtained by $d_i'=t_d + lower_i$. The final pixel values are calculated using the following equation 1:

$$(P_i', P_{i+1}') = \begin{cases} \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), if\ P_i \geq P_{i+1}\ and\ d_i' > d_i \\ \left(P_i - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), if\ P_i < P_{i+1}\ and\ d_i' > d_i \\ \left(P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), if\ P_i \geq P_{i+1}\ and\ d_i' \leq d_i \\ \left(P_i + \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} - \left\lceil \frac{m}{2} \right\rceil\right), if\ P_i < P_{i+1}\ and\ d_i' \leq d_i \end{cases} \quad (1)$$

Where, $m = |d_i' - d_i|$.

## IV. PROPOSED METHOD

In the following proposed method, the data embedding is performed by traversing the image in a raster scan order and splitting the image into blocks of the size of consecutive three pixels. The embedding scheme is narrated in the following steps.

### *A.* Data Embedding Method

Input: Secret Data Message, long bitstream.
Cover image: color image of size 512 X 512
Step 1: Read three consecutive pixels from the color cover image and arrange it in ascending order.

| a | b | c |
|---|---|---|

Step 2: form two pairs of pixel blocks.

| c | a |
|---|---|

| a | b |
|---|---|

Take the first pair

| c | a |
|---|---|

Step 3: Calculate the difference: $d_i = |c - a|$.
Step 4. Based on d find out the range R.
Step 5. Determine the capacity of the embedded bit.
Step 6. Take the secret bit of the same capacity and convert it into equivalent decimal.
Step 7. Determine d'= d + decimal equivalent of secret bit.
Step 8. Determine the new stego pixel by applying the condition as used in the Wu & Tsai Method.
Step 9. Now apply the step1 to step 8 for the pixel pair:

| a | b |
|---|---|

Step 10. Now consider we get new stego pixel pair:

| c' | a' |
|---|---|

| a'' | b' |
|---|---|

Step 11. Perform readjustment process to form stego components based on the following sub steps:

$$a_{final} = \lceil (a' + a'')/2 \rceil \quad (2)$$

$$c_{final} = c' - (a' - a_{final}) \quad (3)$$

$$b_{final} = b' - (a'' - a_{final}) \quad (4)$$

Step 12. Final stego pixel block is:

| $a_{final}$ | $b_{final}$ | $c_{final}$ |
|---|---|---|

All the above steps continue for the rest of the pixel of the image.

### *B.* Data Extraction Method

The data extraction scheme is narrated in the following steps:
Input: stego image.
Step1. Read three consecutive pixels from stego image and arrange it in ascending order.
Step 2: Get two pairs of the pixel blocks.

| $c_{final}$ | $a_{final}$ |
|---|---|

| $a_{final}$ | $b_{final}$ |
|---|---|

Take the first pair:

| $c_{final}$ | $a_{final}$ |
|---|---|

Perform the following steps for each pair:
Step 3. Calculate the difference $d = |c_{final} - a_{final}|$
Step 4. Calculate the range:

$$b = \begin{cases} d - l_k, if\ d \geq 0 \\ -d - l_k, if\ \ d\ < 0 \end{cases} \quad (5)$$

Where, $l_k$ is the lower range.
Step 5. Calculate $M_1$ = equivalent binary of b.
Step 6. Now to get the secret message concatenate $M_1$ and $M_2$:
$M = M_1 \,||\, M_2$.
Now, the above embedding and extraction procedure is followed for the pixel block common with middle value and the lowest value, and compare.

## V. Mathematical Explanation

### A Data Embedding

Consider, Pixel pair block:

| 100 | 200 | 150 |
|---|---|---|

And the secret message bit is 110001101010110.
Arrange the block in ascending order. i.e., a= 200, b= 150, c=100.
Now consider the greatest pixel value as the common pixel. Here a value is 200. So, the pixel pair is:

| 100 | 200 |
|---|---|

| 200 | 150 |
|---|---|

Now, consider the first-pixel block:

| 100 | 200 |
|---|---|

Here, D= |100-200| = 100 and range R is 64-128. So, capacity is $l_k = 64(2^6) = 6\ bit$.
The first 6 bit of image is 110001 ~ $(49)_{10}$. So, d'= 64+49=113.
Here d'>d,. So, m=d'-d = 113-100=13, m/2= 13/2= 6.5.
Using PVD condition the pixel value now, 100-6=94, and 200+7= 207.

Now for the second-pixel block:

| 200 | 150 |
|---|---|

D= |200-150| = 50, range R is 32-64. So, capacity is $l_k = 32\ (2^5) = 5\ bit$.
The next 5 bit of image is 10101 ~ $(21)_{10}$. So, d'= 32+21=53.
Here, d'>d. So, m=d'-d = 53-50=3, m/2= 3/2= 1.5.
Using PVD condition the pixel value now, 200+2=202, and 150-1= 149.
Now, $a_{final}$ = (207+202)/2=204.5~205
Pixel readjustment:
$c_{final}$= c' – (207-205)= 94-2= 92.
$b_{final}$= 149 – (202-205)= 149+3=152.
Now, new stego pixel is:

| 92 | 205 | 152 |
|---|---|---|

**B Data Extraction**

Take the first pixel pair:

| 92 | 205 |
|---|---|

d=|92 – 205| = 113. Range is 64 – 128. So, $l_k$= 64.
B= – (– 113) – 64 = 49.
$M_1$= $(49)_{10}$= $(110001)_2$.
Take the second-pixel pair:

| 205 | 152 |
|---|---|

d=|205-152| = 53. The range is 32-64. So, $l_k$= 32.
B= 53-32 =21.
$M_1$= $(21)_{10}$= $(10101)_2$.
Concatenate $M_1$ and $M_2$ as M = $M_1$ || $M_2$= 11000110101.
Common pixel the lowest value C. pixel block is:

| 100 | 200 |
|---|---|

| 100 | 150 |
|---|---|

Then the generated stego pixel block is:

| 97 | 210 | 150 |
|---|---|---|

And secret data bit 1100011010.
Common pixel the lowest value b. Pixel block is:

| 100 | 150 |
|---|---|

| 200 | 150 |
|---|---|

Then the generated stego pixel block is:

| 94 | 208 | 150 |
|---|---|---|

And secret data bit 1100011010.

## V. EXPERIMENTAL RESULTS

To verify the minimum changes of the PVD method, the proposed method was compared with the methods of Wu & Tsai. Four images of size 512 X 512 were tested: Lena, Baboon, Boat, and Pepper. Figure. 1 shows the cover images and stego images generated by our method and no artifact can be distinguished by the human eye.

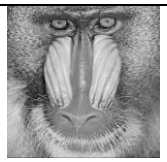
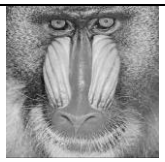
| Image Name | Cover Image | Stego Image |
|---|---|---|
| Lena |  |  |
| Baboon |  |  |
| Sheep |  |  |
| Peeper |  |  |

**Fig. 1: Cover Images and Stego Images using Proposed Method**

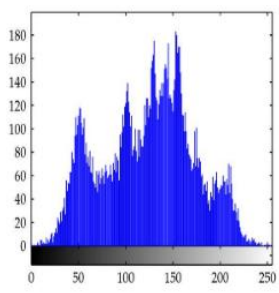
Table I shows the comparison of hiding capacity and visual quality of the images between Wu & Tsai method and the proposed method.

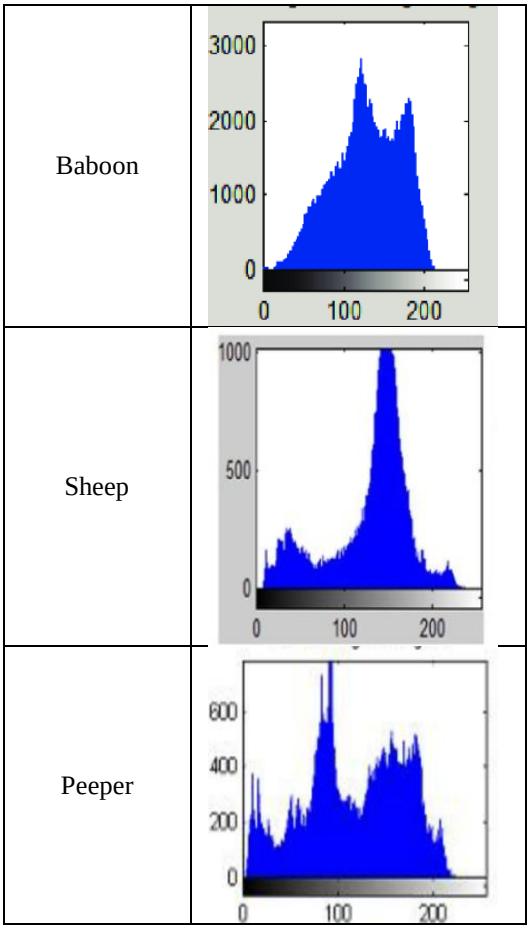
**TABLE I. CAPACITY (BYTES) AND VISUAL QUALITY (DB)**

| | Wu & Tsai Method | | Proposed Method | |
|---|---|---|---|---|
| IMAGE | Capacity | PSNR | Capacity | PSNR |
| **Lenna** | 50.894 | 41.5 | 51.74 | 46.3 |
| **Baboon** | 57.028 | 37.0 | 57.077 | 38.4 |
| **Sheep** | 52.230 | 39.6 | 52.450 | 40.6 |
| **Pepper** | 50.657 | 41.5 | 50.815 | 42.8 |

Table II shows the histogram analysis of the sample images considered.

**TABLE II. HISTOGRAM ANALYSIS OF THE SAMPLE IMAGES**

| Image Name | Histogram Analysis |
|---|---|
| Leena |  |




## VI. CONCLUSIONS

In this paper, a secure steganographic method with a high capacity method is proposed in order to enhance the security of the stego images. Compared with the method of the Wu & Tsai method, our proposed method yields the least differences in the stego image and the cover image. Our proposed method guarantees secure communication with a high embedding capacity and good imperceptibility to the naked human eye. The experimental results support the contention that the proposed method shows the best similarities between the stego and cover image.

## REFERENCES


1. W. Trappe, L. C. Washington: "Introduction to Cryptography with Coding Theory", Pearson, 2nd edition, 2011.
2. C.K. Chan, L.M. Cheng: "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, Elsevier, vol. 37, 2004, pp. 469-474.
3. Y.P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. Su, C. P. Chang: "High-Payload Image Hiding with Quality Recovery using Tri-Way Pixel-Value Differencing", Information Sciences, Elsevier, vol. 191, 2012, pp. 214-225.
4. N. A. Al-Otaibi, A. A. Gutub" "Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority", International Conference on Advanced Engineering Technologies, Dubai, 2014, pp. 250-256.
5. R. Das, I. Das: "Secure Data Transfer in IoT Environment: Adopting both Cryptography and Steganography Techniques", International Conference on Research in Computational Intelligence and Communication Networks, IEEE, Kolkata, India, pp. 296-301.
6. X. Zhou, W. Gong, W. Fu, L. J. Jin: "An Improved Method for LSB based Color Image Steganography combined with Cryptography", International Conference on Computer and Information Science, IEEE, Okayama, Japan, 2016, pp. 1-4.
7. C. H. Yang: "Inverted Pattern Approach to Improve Image Quality of Information Hiding by LSB Substitution", Pattern Recognition, Elsevier, vol. 41, no. 8, 2008, pp. 2674-2683.
8. S. K. Chen: "A Module-based LSB Substitution Method with Lossless Secret Data Compression", Computer Standards & Interfaces, Elsevier, vol. 33, no. 4, 2011, pp. 367-371.
9. W. L. Xu, C. C. Chang, T. S. Chen, L. M. Wang: "An Improved Least-Significant-Bit Substitution Method using the ModuloThree Strategy", Displays, vol. 42, 2016, pp. 36-42.
10. W.J. Chen, C. C. Chang, T. H. N. Le: "High Payload Steganography Mechanism using Hybrid Edge Detector", Expert Systems with Applications, vol. 37, no. 4, 2010, pp. 3292-3301.
11. A. K. Pal, T. Pramanik: "Design of an Edge Detection Based Image Steganography with High Embedding Capacity", International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Springer, 2013, pp. 794-800.
12. M. R. Modi, S. Islam, P. Gupta: "Edge Based Steganography on Colored Images", International Conference on Intelligent Computing, Springer, 2013, pp. 593-600.
13. D.C. Wu, W.H. Tsai: "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letters, Elsevier, vol. 24, no. 9, 2003, pp. 1613-1626.
14. M. Khodaei, K. Faez: "New Adaptive Steganographic Method using Least Significant-Bit Substitution and Pixel-Value Differencing", Image Processing, IET, vol. 6, no. 6, 2012 pp. 667-686.
15. H. W. Tseng, H. S. Leng: "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics, Hindawi, 2013.
16. X. Liao, Q. Y. Wen, J. Zhang: "A Steganographic Method for Digital Images with Four-Pixel Differencing and Modified LSB Substitution", Journal of Visual Communication and Image Representation, Elsevier, vol. 22, no. 1, 2011, pp. 1-8.
17. G. Swain: "A Steganographic Method Combining LSB Substitution and PVD in a Block", International Conference on Computational Modeling and Security, Elsevier, vol. 85, 2016, pp. 39-44.
18. O. Hosam, N. B. Halima: "Adaptive Block-based Pixel Value Differencing Steganography", Security and Communication Networks, Wiley, vol. 9, no. 18, 2016, pp. 5036-5505.
19. A. Pradhan, K. R. Sekhar, G. Swain: "Digital Image Steganography based on Seven Way Pixel Value Differencing", Indian Journal of Science and Technology, vol. 9, no. 37, 2016.
20. W. Zhao, Z. Jie, L. Xin, W. Qiaoyan: "Data Embedding based on Pixel Value Differencing and Modulus Function using Indeterminate Equation", The Journal of China Universities of Posts and Telecommunications, Elsevier, vol. 22, no. 1, 2015, pp. 95-100.
21. J. K. Mandal, D. Das: "Steganography using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow", International Conference on Computer Science, Engineering and Applications, Delhi, India, 2012.
22. A. Gutub, A.Al-Qahtani, A. Tabakh: "Triple-A: Secure RGB Image Steganography based on Randomization", International Conference on Computer Systems and Applications, IEEE, Rabat, Morocco, 2009, pp. 400-403.
23. A.A.A. Gutub: "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 1, 2010, pp. 56-64.
24. M. T. Parvez, A. A. A. Gutub: "Vibrant Color Image Steganography using Channel Differencing and Secret Data Distribution", Kuwait Journal of Science & Engineering, vol. 38, 2011, pp. 127-142.
25. V. Nagaraj, V. Vijayalakshmi, G. Zayaraz: "Color Image Steganography based on Pixel Value Modification Method using Modulus Function", International Conference on Electronic Engineering and Computer Science, vol. 4, 2013, pp. 17-24.
26. C. Prema, D. Manimegalai: "Adaptive Color Image Steganography using Intra Color Pixel Value Differencing", Australia Journal of Basic Applied Science, vol. 8, pp. 161-167.
27. C. Y. Yang, W.F. Wang: "Block-Based Colour Image Steganography using Smart Pixel-Adjustment", Genetic and Evolutionary Computing, Springer, 2015, pp. 145-154.
28. G. Swain: "Adaptive Pixel Value Differencing Steganography using both Vertical and Horizontal Edges", Multimedia Tools and Applications, Springer, vol. 75, no. 21, 2016, pp. 13541-13556.
29. S. Prasad, A. K. Pal: "An RGB Colour Image Steganography Scheme using Overlapping Block-based Pixel-Value Differencing", Royal Society Open Science, 2017.

## AUTHORS PROFILE

**Jayeeta Majumder,** is a research scholar of KIIT university. She has enrolled as a Phd Scholar in the year 2016. She completed her MCA from IGNOU in 2006 and the Qualify the GATe examination in the year 2007. She completed M.Tech in CSE in the year 2009. Her research interest in Information Security. Now, she continuing her research in the field of image steganography. She published more than 10 research papers in this area in different international journal and conferences. She is a member of CSI.

**Dr. Chittaranjan Pradhan,** is an Associate Professor of KIIT University. He completed his M.Tech and PhD degree both from the KIIT University. His research area is digital watermarking. Now, he is associated with different journal and professional bodies. He reviewed many research papers. He also published more than 20 journal and conference papers and also book chapters.