Neighbouring Pixel Matching Pixel Value Differencing Based Image Steganography

[1]**Jayeeta Majumder**

[1]Department of Computer Science & Engineering, Haldia Institute of Technology, India

ABSTRACT

Data hiding technique is very significant in the research area of information security. Using different directional way of pixel value comparison, we propose a new Reversible Data Hiding (RDH) scheme. The data extraction process successfully extract secret data as well as recover cover image. Here I observed the efficiency of the proposed method by performing experiments on some standard cover images and found significantly better result in terms of data hiding capacity compared with existing data hiding schemes. To estimate the contrast and smoothness of pixels it also checks the correlation between neighbouring pixels. Edge area pixels tolerate larger changes than the smooth area pixels. The paper considers two, three and four neighbouring pixel matching technique. Through the experimental result it produces the proposed method gives large data hiding capacity with minimum number of distortion.

Keywords: Information Security, Pixel matching, Pixel Value Differencing, Steganography, Reversible Data Hiding

1. INTRODUCTION

In modern days, we need to protect our confidential data during transmission through a public channel. Generally, first to contrast this, steganography is to protect the secrecy of the data. we process our secret data before transmission. It changes the context of the data into unreadable form, but only the authorised 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. Here, the cover media like audio, video, image are used as carrier to embed the secret data. The cover media along with secret data is known as stego-data. The aim for both cryptography and steganography are same. Image data are frequently used in different application.

2. Related Work

Through literature survey, we found a number of image based steganographic schemes. The LSB (Least Significant Bit) is the widely used methods 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 increases embedding capacity. By using optimal pixel adjustment process the visual quality can be improved[1-6].

In Yang [7] scheme, cover pixel 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 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 which 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.

The proposed scheme designs multi way Pixel Value Differencing using directional differences. The rest of the paper is organized as follows. Section 2 describes the basic idea of the PVD method proposed by WU & Tsai. . The proposed scheme is described in section 3. The experimental results are presented in section 4. Finally, section 5 concludes the paper.

3. Pixel-Value Differencing Method (WU & Tsai Method) (PVD)

In the pixel value differencing method [13] the cover image is generally a grey level image and different size secret message bits are used as secret data. Through 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 smooth area, and greater value is in the edge area. To maintain the intensity values of grey scale image the values of d_i is in the range of [0, 255]. The boundary of range R is denoted by $[\text{lower}_i,\text{upper}_i]$. The number of embedded secret bit sequences (t) in two consecutive pixels depends on the quantizationrange table and it is computed as $t= (\log_2 (\text{upper}_i - \text{lower}_{i)} + 1)$. The obtained bit sequence is converted into decimal value, t_d. The new difference value (d_i') is obtained by $d_i'=t_d + \text{lower}_i$. The final pixel values are calculate using the following condition,

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

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

4. Proposed Method

The following proposed method where the data is embedded by traversing the image in raster scan order. It was based on the human visibility system sensitivity. Depending on the correlation between neighbouring pixels the embedded bit capacity for each pixel is decided. At first, the concept of side matching embedding is proposed by Kim (1992). In this method the value of two neigh-boring blocks (upper pixel block and left pixel block) are used.

In this paper, to calculate the capacity estimation, for each input pixel the side information of neighbouring pixels is required. The correlation between the two neighbouring pixels decides that the location of the input pixel. The edge area location pixel embeds more data than those in smooth area. Our proposed method is two-sided side match method. In addition, to perform more accurate estimation the three-side and four-side side match methods are also discussed.

4.1 Two-Neighbour-pixel match steganography

For estimation here we use only upper side pixel P_U and left side pixel P_L, which is also the neighbouring pixel. Here, we exclude the first row and first column of the cover image from the data embeddingasshowninFig.1. The input pixel is P_X and equivalent grey value is g_x. The grey value of first neighbour pixel is P_U is g_u and second neighbour pixel is P_L is g_l. Then the difference value diff is computed as diff={ $|P_U - P_X| + |P_L - P_X|$}/2

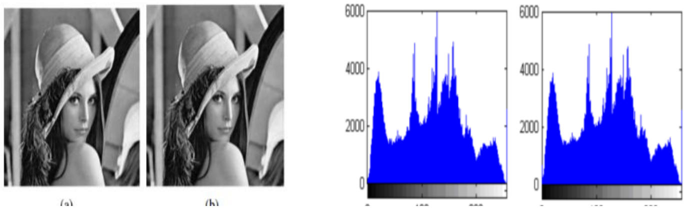


Fig.1.The Two-Neighbour-pixel(a) Lenna image (b) Stego image (c), (d) Histogram

The small difference, d value defines the pixel position either it is in smooth area or in edge area. Edge area pixels tolerate greater changes using the basic LSB substitution method. Depending on the d values the no. of embedded bits decided. If the values are (1, 0 or -1) then only one bit data is embedded into the LSB position of pixels P_X. Otherwise, the number of embedded bit n, is calculated by,

$$n= \log_2|diff|, \quad \text{if } |d| >1$$

The n bit sub stream is extracted from the embedding data and converted with its equivalent decimal value m.

Then the new difference diff$^{'}$ is calculated as

$$diff' = \{ 2^n +m, \quad \text{if } diff>1; \quad - (2^n +m), \text{ if } diff<1;$$

Finally, the modified value of the pixel P_X is as

$$g'_x==|\{ |P_U -P_X | + |P_L -P_X |\}/2 -diff'|$$

The mathematical explanation of data embedding is as follows.

For the pixel P_X the grey value is 45.Thecorresponding neighboring pixels with their values 40 and 84. Then the difference diff=(|40-45|+|84-45|)/2=22.The embedded bit no. is $n=\log_2|22|=4$. Consider, the leading four bits sub stream of the secret data are $m=1101_2 =13$. Then the new difference $diff'=2^n + m= 2^4+13=29$.

Finally, the modified pixel value is $g'_x= =(|40-45|+|84-45|)/2=|22 -29|=7$.

For data embedding and extracting the falling-off boundary checking process is applied.

For checking with falls off the boundary, if it satisfies then the pixel P_X is not used.

Similarly, in data extraction, if the pixel value satisfies the falls off the boundary, then the pixel is not used, it is skipped from extraction.

4.2 Three-Neighbour-pixel match steganography

Using raster scan method, the cover image is scanned and the pixels are considered with three types as shown in the following figure 2. The dark grey color pixels used for data embedding and declared as neighbor pixels. The non-colored pixels are only neighbor pixel. The light grey color pixels are not used for data embedding. In three side match method, to estimate the no. of bits for embedding the upper, upper-right and upper-left neighbor pixels are used. If P_X is the pixel with grey value g_x, then P_U is the upper neighbor pixel with grey value g_u. P_{UR} is the upper right pixel with grey value g_{ur} and finally, the P_{UL} is the upper left neighbor pixel with grey value g_{ul}. Then the difference value, diff is computed as in equation

$$diff = \{ |P_U -P_X | + |P_L -P_X |+|P_R-P_X|\}/3 – g_x.$$

Depending on the d values the no. of embedded bits decided. If the values are (1, 0 or -1) then the pixel is discarded for embedding. If the difference value is greater than or equal to 2 then we can hide n no. of bits, where n is calculated as,

$n= \log_2|diff|$, if $|diff| >1$

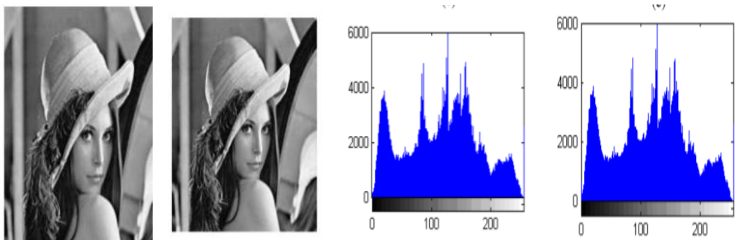
The n bits of secret data taken as a sub-stream which is converted into decimal value m. and the new value diff' is computed.

$$diff' = \{ 2^n +m, \quad \text{if } diff>1; \\ - (2^n +m), \text{ if } diff<1;$$

Finally, after embedding n secret bits the new pixel value is calculated,

$g'_x= \{ |P_U -P_X | + |P_L -P_X |+|P_R-P_X|\}/3 -diff'$

The extraction method is same as two neighbor pixel method.



(a) (b) (c) (d)

Fig.2.The Three- Neighbour-pixel. (a) Lenna image (b) Stego image (c), (d) Histogram

4.3 Four-Neighbour-pixel match Steganography

Using raster scan method, the cover image is scanned and the pixels are considered by three types as shown in the following figure 3. The dark grey color pixels used for data embedding and declared as neighbor pixels. The non-colored pixels used as only neighbor pixel. The light grey color pixels are not used for data embedding.

The upper, upper-right, upper-left and left neighbor pixels are used to estimate the no. of bits for embedding in the target pixel in four side match method. Suppose P_X is a target pixel with gray value g_x, P_U is its upper neighboring pixel with gray value g_u, g_{ur} is the grey value of P_{UR} which is the upper right neighboring pixel, P_{UL} is its upper-left neighboring pixel with gray value g_{ul} and $g_l$is the grey value of the left neighboring pixel P_L. The difference value diff is computed as in equation

$$diff = \{ |P_U -P_X | +|P_D -P_X| + |P_L -P_X |+|P_R-P_X|\}/4 – g_x$$

Depending on the d values the no. of embedded bits decided. If the values are (1, 0 or -1) then the pixel is discarded from embedding If the difference value is greater than or equal to 2 then we can hide n no. of bits, where n is calculated as,

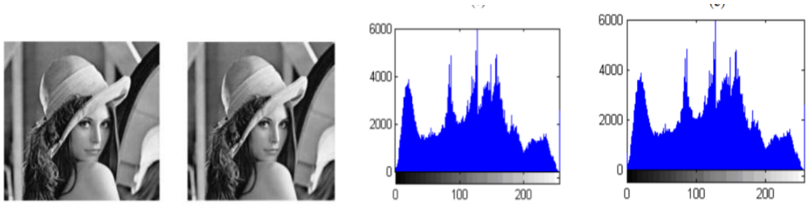
$n= \log_2|d|$, if $|d| >1$

The n bits of secret data taken as a sub-stream which is converted into decimal value m. and the new value diff' is computed.

$$diff' = \{ 2^{n} + m, \quad \text{if } diff > 1;$$
$$- (2^{n} + m), \text{ if } diff < 1;$$

Finally, after embedding n secret bits the new pixel value is calculated,
$g'_{x} = \{ |P_{U} - P_{X}| + |P_{D} - P_{X}| + |P_{L} - P_{X}| + |P_{R} - P_{X}| \}/4 - diff'$.

The extraction method is same as two **Neighbour-pixel** method.



(a) (b) (c) (d)

Fig.3 . The Four-Neighbour-pixel match. (a) Lenna image (b) Stego image (c), (d) Histogram

5. Result & Discussion

The different steganography algorithm performance can be expressed by using three-parameters. i) Data embedding capacity, ii) Data Security, iii) imperceptibility. Our, proposed methods are secured because here we cannot directly replace the LSB pixel value. The pixel value is calculated by using neighbouring pixel values. The basic LSB method has some drawbacks. By using, RS Steganalysis, it is found that the pixel value changes asymmetrically. But, the proposed method, not change the LSB value instead of changing the values. Using histogram, we see that the original image and stego-image are identical. Histogram steganalysis also cannot detect it.

For capacity, our target is always to hide secret message as high as possible. Here, for each case, only first row and first column of the cover medium is left to hide the data.

The distortion of the stego-image is measured by PSNR value. The higher PSNR value means less distortion. The PSNR values of the sample image is shown in the following Table 1.1 and also shows that for same amount of hidden data the four sided match method has minimum distortion compared to other two methods. To check the similarity between the cover image and stego-image the correlation is measured, which is recorded in Table 1.2 If the cover image and stego images are very similar then the correlation value will be close to 1.

Table 1.1 PSNR values of proposed neighbour matching pixel methods (Two, Three, and Four)

Image Name	Image Size(KB)	Amount of hidden data (bytes)	PSNR(dB)		
			Two-Neighbour	Three-Neighbour	Four-Neighbour
Lena	535	20480	42.2	41.6	40.5
Baboon	580	21440	40.2	41.3	39.8

Table 1.2Correlation values of proposed neighbour matching pixel methods (Two, Three, and Four)

Image Name	Image Size(KB)	Amount of hidden data (bytes)	Correlation		
			Two-Neighbour	Three-Neighbour	Four-Neighbour
Lena	535	20480	0.9997	0.9998	0.9996

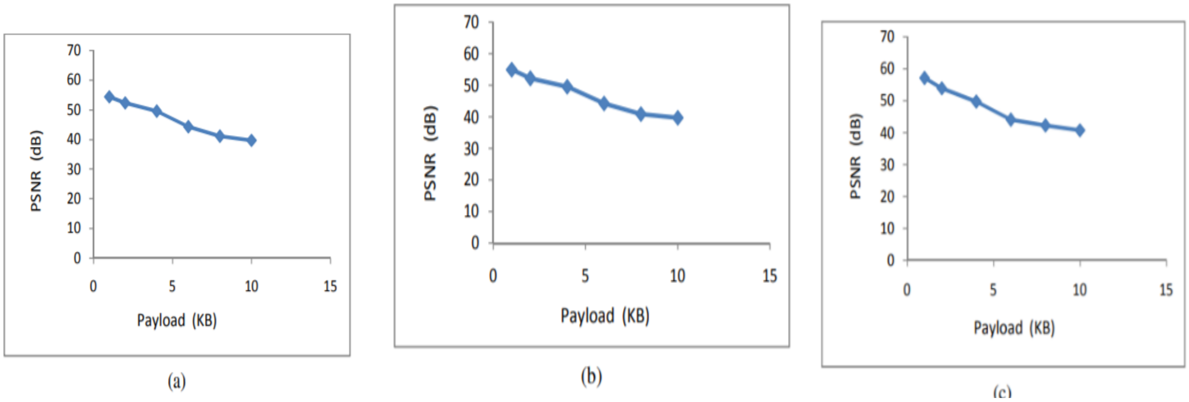
Baboon	580	21440	0.9982	0.9983	0.9986

The embedding capacity of the proposed two, three and four sided side match methods are compared with the two, three, and four sided side match methods of Chang and Tseng, in Table 1.3. In our two and three sided methods the capacity is almost doubled as compared to Chang and Tseng's methods. And in four-side match method the capacity is almost four times improved.

Table 1.3Hiding capacitiescomparison with Chang and Tseng's methodand proposed neighbour matching pixel methods (Two, Three, and Four)

Image Name	Image Size(KB)	Proposed methods			Chang and Tseng's method		
		Two	Three	Four	Two	Three	Four
Lena	535	710538	653012	639519	433979	366302	168634
Baboon	580	690538	625044	618724	419267	343436	186626

Fig.4 (a)-(c) represents the variation of PSNR value with payload for the sample image. Here, it is observed that from the following graph that if I increase the payload up to a certain allowable value, the PSNR not reach less than 40.



(a) (b) (c)

Fig.4 Variation of PSNR with payload for Lena image in (a) two-neighbour match (b) three-neighbour match, and (c) four-neighbour match methods.

6. Conclusion

Here the improved versions of two neighbour matches, three neighbour matchesand four neighbour matches'schemes have been proposed. The number of bits embedded in a target pixel is decided depending upon the correlation of the target pixel with its neighbouring pixels. The embedding capacity of the proposed schemes is very good. After the information is embedded the change in quality of the images are not noticeable. The observed PSNR values are also good. The distortion is lesser in four neighbour matchesscheme compared to the other two schemes.

REFERENCES

[1] Chan CK, Cheng LM. 2004 Hiding data in images by simple LSB substitution. Pattern Recognit. **37**,469–474. (doi:10.1016/j.patcog.2003.08.007)

[2] Lee YP, Lee J-C, ChenW-K, Chang K-C, Su I-J, ChangC-P. 2012 High payload image hiding with quality recovery using tri-way pixel-value differencing. Inf. Sci. **191**, 214–225. (doi:10.1016/j.ins.2012.01.002)

[3] Das R, Das I. 2016 Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. On Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301.

[4] Zhou X, Gong W, Fu W, Jin L. 2016 An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4.

[5] Yang C-H. 2008 Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognit. **41**, 2674–2683. (doi:10.1016/j.patcog.2008.01.019)

[6] Chen S-K. 2011 A module-based LSB substitution method with lossless secret data compression. Comput. Stand. Interfaces **33**, 367–371. (doi:10.1016/j.csi.2010.11.002)

[7] Xu W-L, Chang C-C, Chen T S,Wang L-M. 2016 An improved least-significant-bit substitution method using the modulo three strategy. Displays **42**, 36–42. doi:10.106/j.displa.2016.03.002)

[8] Chen WJ, Chang CC, Le TH. 2010 High payload steganography mechanism using hybrid edge detector. Expert Syst. Appl. **37**, 3292–3301. (doi:10.1016/j.eswa.2009.09.050)

[9] Pal AK, Pramanik T. 2013 Design of an edge detection based image steganography with high embedding capacity. LNICST **115**, 794–800.
(doi:10.1007/978-3-642-37949-9_69)

[10] Chen WJ, Chang CC, Le TH. 2010 High payload steganography mechanism using hybrid edge detector. Expert Syst. Appl. **37**, 3292–3301. (doi:10.1016/j.eswa.2009.09.050)

[11] Pal AK, Pramanik T. 2013 Design of an edge detection based image steganography with high embedding capacity. LNICST **115**, 794–800.
(doi:10.1007/978-3-642-37949-9_69)

[12] Islam S, Modi MR, Gupta P. 2014 Edge based steganography on colored images. In Intelligent computing theories (eds DS Huang, V Bevilacqua, JCFigueroa, P Premaratne). Lecture Notes in Computer Science, vol. 7995, pp. 593–600. Berlin, Germany: Springer. (doi:10.1007/978-3-642-39479-9_69)

[13] Wu D-C, TsaiW-H. 2003 A steganographic method for images by pixel value differencing. Pattern Recognit. Lett. **24**, 1613–1626. (doi:10.1016/S0167-8655(02)00402-6)

[14] Khodei M, Faez K. 2012 New adaptive steganographic method using least significant bit substitution and pixel value differencing. IET ImageProcess**10**, 667–686. (doi:10.1049/iet-ipr.2011.0059)