IMAGE STEGANOGRAPHY TECHNIQUES USING PIXEL VALUE DIFFERENCING: A REVIEW

[1]JayeetaMajumder, [2]Chittaranjan Pradhan
[1] Assistant Professor, [2]Assistant Professor
[1]Computer Science & Engineering
[1]Haldia Institute of Technology

Abstract: Steganography is a technique of information hiding. Today there is a very large demand of applications which require data to be transmitted in a safe and secure manner. Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that does not attract attention from eavesdroppers and attackers. The main requirements of any steganography system are undetectability, robustness and capacity to hide data. There has been a tremendous growth in Information and Communication technologies during the last decade. Internet has become the dominant media for data communication. But the secrecy of the data is to be taken care. Steganography is a technique for achieving secrecy for the data communicated in Internet. This paper presents a review of the steganography techniques based on pixel value differencing (PVD) method. The various techniques proposed in the literature are discussed and possible comparison is done along with their respective merits. The comparison parameters considered are, (i) hiding capacity, (ii) distortion measure, (iii) security and (iv) Computational complexity.

Index Terms — **Information hiding, Steganography, pixel value differencing, PSNR.**

I. Introduction :

In modern days Steganography is the widely used technique to provide secret communication [1]. Steganography focuses on keeping the existence of a message secret. It was originated from Greek words Steganos (covered) and Graptos (writing), called it as "covered writing" [3]. Steganography is a branch of security which deals with hiding of information in any cover medium like image, audio, video, and text [40-41]. The original image used for hiding data is called cover-image, and the image after hiding secret data into it is called stego-image. Steganography techniques are proposed by different researchers in both spatial domain and transform domain. Steganalysis is an art and science of discovering the hidden data from stego-image [5, 35]. The efficiency of any steganographic technique depends upon various parameters. Some of the important parameters are, (i) capacity, (ii) distortion measure, (iii) security and (iv) computational complexity. Capacity is the maximum amount of data that can be hidden inside the image. It is usually represented in terms of bits per pixel. The distortion in the stego image can be measured by peak signal-to-noise ratio (PSNR). Higher the PSNR means lesser is the distortion. A good steganographic technique should be resistant to various steganalysis attacks. The computational complexity refers to the time required to hide the data inside the cover image. The requirements for a good steganographic technique are as shown in Table 1. There are different techniques in spatial domain. Those are, (i) Least Significant Bit (LSB) substitution, (ii) Pixel Value Differencing (PVD), Exploiting modification direction (EMD) etc.

Table 1. Performance parameters

Parameters	Requirement
Capacity	Should be High
Distortion	Should be Low
Security	Should be High
Computational Complexity	Should be low.

II. Analysing Techniques of Stego Image and Cover Media

For measuring the quality of reconstructed image that is stego image as compared to the original image, the metric needs to be define. There are two common error metrics used for estimating noise on images are PSNR, and NCC.

A. **PSNR:** The PSNR (Peak Signal to Noise Ratio) measures the similarity between two images (how two images are close to each other. The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\text{dB}$$

where: I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=255. MSE is the mean square error.

B. **NCC**: The Normalized cross correlation (NCC) has been commonly used as a metric to evaluate the degree of similarity (or dissimilarity) between two compared images. The main advantage of the normalized cross correlation over the cross correlation is that it is less sensitive to linear changes in the amplitude of illumination in the two compared images. Furthermore, the NCC is confined in the range between –1 and 1 to evaluate the performance the Normalized CrossCorrelation (NCC) which is given by the following equation.

$$NCC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(x_{ij} \times y_{ij})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(x_{ij})^2}$$

III. Pixel value Differencing (PVD) Techniques:

A new concept called pixel value differencing (PVD) has been proposed by Wu and Tsai [3] in the field of image steganography for gray images. The PVD method divides the total image into smooth and edge areas. The difference value d is calculated between the two pixels. A range table has been specified for the value d. A new difference value d' replaces the old d value to embed the secret data. The width of the range table decides the number of bit that is allowed to embed. This method gives better results in terms of imperceptibility and capacity as compared to LSB techniques. Zhang and Wang [4] noticed that, the original PVD technique proposed by Wu and Tsai [3] is vulnerable to histogram-based steganalysis. That is the stego-image exhibit an abnormal behaviour in the histogram. They proposed a pseudo-random dithering to get dynamic range of values instead of static or fixed range for the blocks. This technique preserves the advantages like capacity of original PVD and also avoids the unusual behaviour shown by the histogram. Hence the security is an added advantage. Chang et al. [7] found that the capacity of the PVD technique presented by Wu and Tsai [3] can be increased further for a gray-level image. There is a gain of 84.16% on average hiding capacity by the overlapping concept proposed by the authors while maintaining satisfactory image quality. A new steganographic method has been proposed by Wang et al [8] to minimize the distortion on the stego-image. The proposed method is the combination of pixel value differencing (PVD) and modulus function. At first the difference value is computed from two consecutive pixels by applying PVD method. The difference value suggests the number of bits to hide. Then by using modulo operation the remainder of the two consecutive pixels is derived, and the secret data are hidden in the pixels by altering the remainder. Experimental results reveal that the use of modulo operation greatly minimizes the distortion and increases the attack resistance. To increase the capacity of original PVD technique proposed by Wu and Tsai[3], a steganographic technique called Tri-Way PVD has been proposed by Chang et al. [9] by using 2×2 pixel blocks with multi-directional differences. It has been experimentally concluded that the capacity and security can be further enhanced compared to the original PVD method. A novel lossless data hiding technique has been proposed by Lin et al [10] by taking three non-overlapping pixel blocks having two absolute differences called as block difference. Experimentally it has been proved by the authors that the average embedding capacity can be increased. This has been observed that the PVD method introduces distortion to stego-image no matter how much the capacity is reduced. So keeping this in view by avoiding more data embedding to smooth regions Luo et al [11] proposed a new way of embedding secret data to cover image. At first the image is partitioned into small squares. The squares are further made rotation of 0, 90,180, and 270 degrees. The two difference value of three non-overlapping consecutive pixels is calculated and middle pixel is used to hide the secret data. The amount of secret bits will be embedded depending upon the differences among the three non-overlapping consecutive pixels. The proposed technique resists to PVD histogram analysis. Wang et al [8] in 2008 proposed a new direction for data embedding which is the combination of PVD and modulus function. Although good capacity is achieved but the security is not improved. So Joo et al [12] proposed a novel method to improve the stego-image quality which will ensure the security for the secret data. According to them the algorithm is divided into four steps. The first one is the pixel pairing step where the cover image is divided into two consecutive pixels of non- overlapping sub-blocks. Secondly in the embedding step by using the modulus function the pixel value is increased or reduced to match with the message. Thirdly in the adjusting step it solves the out-of-sub-range problem so that there is no variation in the PVD histogram. Finally in the last step, if the pixel value goes beyond the range of 0 to 255 then it will bring back into the range. The results suggest that this method proves to be better compared to Wang et al. [8] in terms of security and capacity. Hong et al [13] proposed a new technique of data embedding using the diamond encoding (DE) technique. A multiple-base notational system (MBNS) has been introduced using modified diamond encoding. The proposed method modifies the diamond encoding to embed in multiple bases and solves the overflow and underflow problem. Experimentally it has been shown that the proposed technique has

better embedding capacity and tolerant against RS scheme and histogram analysis steganalysis attack. A new way of data embedding proposed by Mandal and Das [14] which extends the PVD technique to color images. Each pixel have 24 bits contains R, G, B components. All the 3 color components are used for data embedding. Initially the difference value d_i for each block can be found by $d_i=|p_i-p_{i+1}|$, where p_i and p_{i+1} are the two consecutive non-overlapping pixels of an cover-image. The difference value determines how many bits will be embedded in which componet of a pixel. Basing upon the contribution of R, G, B components in a color image the maximum secret bits that can be embed in each of R, G, B component of a pixel will be 5, 3, 7 bits respectively. Again for embedding of secret bits it uses the original PVD concept proposed by Wu and Tsai [3]. This results of this schema reveals that better stego-imagequality and security compared to original PVD concept proposed by Wu and Tsai [3] also the falling-off boundary problem can be avoided. In 2012, Lee et al [15] proposed a method which increases the capacity of stego-image. This technique uses the JPEG2000 compression and tri-way pixel value differencing for embedding the secret image. The proposed method is useful for sending large secret image without any distortion. To increase the capacity and security of stego-image, Chang and Tseng [16] proposed a novel technique called two, three, four sided side match method. The pixels are visited in raster scan order. In the two sided side match steganography, let $P_x$be the target pixel where secret data will be embedded and g_x be the gray value for P_x. Let g_u and $g_l$be the gray values for the upper pixel P_u and left pixel P_l of a target pixelP_x. The difference value d is calculated as $d= (g_u+ g_l)/2 - g_x$. If the difference value are in the range of -1 to 1 then there is only 1 bit allowed to embed in the LSB bit of the target pixel P_x , otherwise, if d >1 then $b=\log_2 |d|$, bits are allowed to embed. A new value is assigned to the difference value d and target pixel g_x. At times the new value of the pixel P_x may fall off the boundary of the range {0, 255}. Any pixel that suffers with fall off boundary problem (FOBP) will be not considered for data embedding. The three sided side match method have three variants. In first variant the three neighbouring pixels such as upper, left and right are used. In variant 2 instead of right the bottom pixels taken along with upper and left. Left-upper, right-upper, left-bottom and right-bottom are taken to find the difference value in case of last variant. Similarly upper, left, right and bottom neighbouring pixels are exploited for secret data embedding in a target pixel in four sided side match method. This method has the clear advantage of more stego-image capacity and better security compared to LSB techniques. The capacity and quality of the stego-image plays a vital role for a stego-image in secret data communication, In this regard Liao et al [17], have proposed a technique called four pixel differencing and modified LSB substitution. In this work the cover image is separated into non-overlapping four pixel blocks having gray values. The average difference value (k) is used to locate the range. The concept of modified LSB substitution is used to embed k-bits of data bits in the pixels located in that block. As this technique is highly inclined towards LSB substitution, so the stego-image has less attack resistance, but the hiding capacity is more. The capacity of stego-image and security of secret data have major role behind the success of any steganographic algorithm. Yang et al [18] suggested a new technique to achieve this. In contrast to Wu and Tsai [3] where a pair of pixels are processed at a time, the authors considered two pair of pixels for processing. There are three ways the four pixels can be grouped. The grouping of pairs of two pixels is done by taking the vertical, horizontal and diagonal pairs. Also to prevent the fall-off boundary problem they proposed a shifting schema. The proposed method avoids the Fridrich et al.'s detection [23] with improved hiding capacity. In case of PVD technique the more the difference values the more the data that can be embedded. But to embed more data so as to increase the capacity sometimes the pixel values cross the boundary values. If the pixel values exceed the boundary values then, this is called fall-off boundary problem. Swain and Lenka [19] marked this issue and then proposed revised variants of two, three and four sided side match with higher embedding capacity. Swain[20] has proposed a steganographic technique using pixel value differencing. There are four different methods and each has their unique idea to find the difference value. In five neighbours differencing method the difference value is calculated by taking the difference of maximum to minimum of gray values among five pixels namely right, upper, left, upper-right, bottom and upper-right corner pixel of a target pixel. In six neighbours differencing method the difference value is calculated by same way as in five neighbour differencing method with one extra pixel as upper-left corner. Similarly for seven neighbours differencing method one extra pixel as bottom left corner and for eight neighbours differencing method one more extra pixel such as bottom left corner. Experimental study shows that the quality of the image is better in case of five neighbours differencing and the capacity is higher in eight neighbours differencing. Pradhan et al [21]proposed a pixel value differencing technique based on PVD called two neighbour method, three neighbour method and four neighbour method. The result reveals that the capacity is good in four neighbour method with acceptable stego-image quality. An adaptive pixel value differencing method using vertical and horizontal edges has been proposed by Swain [22]. Two techniques is given as first one uses 2×2 pixel blocks and second one uses 3×3 pixel blocks. The first technique offers good capacity and second one provides good stego-image quality.

Table 3. Comparison between various PVD methods.

Ref No	Security	Capacity	Distortion	Complexity	Advantages
3	Moderate	Moderate	Moderate	Low	Data Hiding using new Methods
4	High	Moderate	Low	Low	Avoids the histogram steganalysis occurred in Wu and Tsai [3] method.
7	Moderate	High	Moderate	Moderate	Capacity increase in 84.16% compared with Wu and Tsai Method [3].
8	Moderate	High	Moderate	High	Better stego-image quality and security compared to Wu and Tsai [3]
9	High	High	High	High	Increased Capacity and security with Wu and Tsai [16]
11	High	Moderate	Moderate	High	Security to stego-image is better compared to Ref. [4] and Ref. [5].
12	High	High	Moderate	High	Differences is minimum in the PVD histograms between the cover and stego-images compared to Wang et al [8]
13	High	High	Low	High	Embedding performance is better compared to previous PVD-based methods in terms of payload and image quality.
14	High	Moderate	Low	Moderate	New direction for data embedding in color images.
15	High	High	Low	High	Capacity and Security are high.
16	Moderate	High	Moderate	Low	Better capacity and security compared to conventional LSBs substitution method.
17	Moderate	High	Moderate	Low	Capacity is more compared to LSB methods.
18	Moderate	High	Moderate	High	More edge areas present compared to Wu and Tsai [3]
19	Moderate	High	Moderate	Moderate	Falling-off boundary problem caused in Ref. [16] is solved
20	Moderate	Moderate	Moderate	Moderate	Adds more flexibility in choosing data embedding method.

IV. Conclusion:

This paper reviews the various research papers based on LSB and PVD and compares them with regard to embedding capacity, distortion, security and computational complexity. Least Significant Bit (LSB) and Pixel Value Differencing (PVD) are the most generally utilized strategies for steganography The PVD steganography can provide higher security. A combination of PVD and LSB can offer both higher embedding capacity and better security.

V. References:

[1] Anderson RJ, Petitcolas FAP. On the limits of steganography. IEEE Journal on Selected Areas in Communications. 1998; 16(4): 474-481.

[2] Johnson NF, Jajodia S. Exploring steganography: seeing the unseen. IEEE Computer Journal. 1998; 31(2): 26-34.

[3] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters. 2003; 24: 1613-1626.

[4] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters. 2004; 25: 331-339.
[5] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEEE Proceedings on Vision, Image and Signal Processing. 2005; 152(5) 611-615.
[6] Yang CH, Weng CY, SJ. Wang, Sun HM. Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. The Journal of Systems and Software. 2010; 83: 1635–1643.
[7] Chang CC, Chuang JC, Hu YC. Spatial Domain image hiding scheme using pixel-values differencing. FundamentaInformaticae. 2006; 70: 171–184.
[8] Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganographic method with pixel-value differencing and modulus function. The Journal of Systems and Software. 2008; 81: 150.-158.
[9] Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganographic method using tri-way pixelvalue differencing. Journal of Multimedia. 2008; 3(2): 37-44.
[10] Lin CC, Hsueh NL. A lossless data hiding scheme based on three-pixel block differences. Pattern Recognition. 2008; 41: 1415 – 1425.
[11] Luo W, Huang F, Huang J. A more secure steganography based on adaptive pixel-value differencing scheme. Multimed Tools Appl. DOI 10.1007/s11042-009-0440-3. 2010: 407-430. [12] Joo JC, Lee HY, Lee HK. Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function. EURASIP Journal on Advances in Signal Processing. doi:10.1155/2010/249826. 2010: 1-13.
[13] Hong W, Chen TS, Luo CW. Data embedding using pixel value differencing and diamond encoding with multiple-base notational system. The Journal of Systems and Software. 2012; 85: 1166-1175.
[14] Mandal JK, Das D. Color image steganography based on pixel value differencing in spatial domain. International Journal of Information Sciences and Techniques. 2012; 2(4): 83-93.
[15] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences. 2012; 191: 214-225.
[16] Chang CC and Tseng HW. A steganographic method for digital images using side match. Pattern Recognition Letters. 2004; 25: 1431-1437.
[17] Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J. V is. Commun. Image. R. 2011; 22: 1-8.
[18] Yang CH, Weng CY, Tso HK, Wang SJ. A data hiding scheme using the varieties of pixel-value differencing in multimedia image. The Journal of Systems and Software. 2011; 84: 669-678.
[19] Swain G, Lenka SK. Steganography using two sided, three sided, and four sided side match methods. CSI Transactions on ICT. 2013; 1(2): 127-133.
[20] Swain G. Steganography in digital images using maximum difference of neighboring pixel values. International Journal of Security and Its Applications. 2013; 7(6): 285-294.
[21] Pradhan A, Sharma DS, Swain G. Variable rate steganography in digital images using two, three and four neighbor Pixels. Indian Journal of Computer Science and Engineering. 2012; 3(3): 457-463.
[22] Swain G. Adaptive pixel value differencing steganography using both vertical and horizontal edges. Multimedia Tools and Applications. DOI: 10.1007/s11042-015-2937-2, 2015: 1-16.
[23] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in grayscale and color images. in: ACM Workshop on Multimedia and Security. 2001: 27–30.