Indonesian Journal of Electrical Engineering and Computer Science
Vol. 2, No. 3, June 2016, pp. 712 ~ 719
DOI: 10.11591/ijeecs.v2.i3.pp712-719

A Review on LSB Substitution and PVD Based Image Steganography Techniques

Aditya Kumar Sahu*, Gandharba Swain
CSE, KL University, Vaddeswaram-522502, Andhra Pradesh, India
*Corresponding author, e-mail: adityasahu.cse@gmail.com

Abstract

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 least significant bit (LSB) substitution and pixel value differencing (PVD). 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.

Keywords*: cryptography; steganography; least significant bit substitution; pixel value differencing*

1. Introduction

Cryptography and Steganography are the two widely used techniques to provide secret communication [1]. But the way they functions are different. Cryptography is the technique of transforming any plaintext into ciphertext. 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]. This is something like cryptanalysis. Many steganalytic attacks present on spatial domains are RS analysis, Histogram analysis, Chi-square attack, Weighted-Stego (WS) analysis etc. The efficiency of any steganographic technique depends upon various parameters. Some of the important parameters are, (i) capacity, (ii) distortion measure, (iii) security or attack resistance, 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

Received March 24, 2016; Revised May 10, 2016; Accepted May 25, 2016

The rest of the paper is organized as follows. In section 2 the LSB substitution techniques are represented, in section 3 the PVD techniques are described. In section 4, LSB+PVD techniques are described and in section 5 the paper is concluded.

2. LSB Substitution Techniques

To achieve secure communication in spatial domain the secret data is embedded in the cover medium. It can be achieved by modifying the bits at the LSB planes. LSB substitution can be extended u to 4-LSB planes to achieve high capacity. Johnson and Jajodia [2] proposed various steganographic software tools like S-Tools and EzStego tool using least significant bit (LSB) substitution. Wang et al [3] proposed a new way of embedding bit to LSB plane by using pixel adjustment process. In their method they introduced the concept of Moderately-Significant-Bit (MSB) i.e. they targeted the intermediate bit of the cover image. So by this means the secret data can be secured if any damage to the LSB bit is caused in future. Furthermore, to improve the stego-image quality it uses the concept of pixel adjustment process. Wang et al [4] again came up with a unique idea to hide the data from the interceptor. They used the concept of genetic algorithm to hide the valuable data in the k-LSBs of the cover image. Although it increases the computational time, but provides greater security.

To decrease the computational time and increase the hiding capacity, a novel technique has been proposed by Chang et al [6]. This method uses the concept of dynamic programming to identify the optimal bit in LSB for substitution. It uses the concept of “Principle of optimality”. This principle ensures that each sub sequence of a solution must be optimal. By experiment the authors have proved that, the computational time is less compared to the method proposed by Wang et. al. [4] and also quality of the stego image is better.

Chan and Cheng [7] extended the work of Wang et al [4], they experimentally showed that the image quality of the stego-image can be greatly enhanced with low computational complexity. The authors have proved that the worst mean-square-error (WMSE) between the cover image and stego-image can be reduced to half as computed by simple least significant bit method proposed by Wang et al. [4]. Swain and Lenka [8] proposed a technique, RGB channel based steganography with two levels of security. In order to encrypt the plaintext, RSA algorithm has been used. The ciphertext is embedded in any two channels out of the available Red (R), Green (G), and Blue (B) channels. Swain and Lenka [9] proposoed a dynamic steganography, it is a unique and secured technique by combining cryptography and steganography. In order to encrypt the message the block cipher cryptographic algorithm with block length of 128 key has been used. Three LSB bits (6^{th}, 7th, and 8th) are used to hide two bits of cipher text in each pixel of the image. Experimental results reveal that the stego-image quality will be preserved. Gutub et al.[10] proposed a novel technique called pixel indicator technique. The last two LSB bits from any one of the available R, G, and B channel is chosen as indicator to indicate the presence of data. The choice of choosing the indicator bit is done randomly. The indicator is selected on the basis of sequence of R, G, and B channels. If R is indicator in the first pixel then G and B channel are the channel 1 and 2 respectively. Similarly G and B channels are the indicators for second and third pixels.

To increase the capacity, a better technique has been proposed by Parvez and Gutub [11]. The concept behind this method is, embed data bits in low value channel instead of embedding in high value channels. Suppose each of the values of the R, G, and B channels is 255, and then change in any channels will lead to distortion. So the channel which has less value will be appropriate for data embedding rather than higher value channel. As this method inserts different number of bits depending upon the channel values, this can be also called as variable-bits per channel. The security and capacity is increased compared to the earlier proposed pixel indicator technique by Gutub et al. [10].

The pixel indicator technique although increases the security but capacity is not predictable. Furthermore to increase the security and to enhance the capacity, a more randomization technique in selecting the pixel to store data has been proposed by Gutub et al. [12]. This algorithm is called triple – A algorithm. The algorithm uses the similar procedure as used by LSB method but with more randomization. At first the data is encrypted by using AES algorithm to produce ciphertext. By using a pseudorandom number generator (PRNG) which generates two random numbers per each number of iterations, let it be seed1 and seed2. The seed1 random number is used to locate the channel where the ciphertext can be embedded and

seed2 is used to find how many bits can be embedded. This algorithm provides better security and capacity.

In order to compare the parameters such as security and capacity provided by pixel indicator and triple-A algorithm, Tiwari and Shandilya [13] experimentally observed that there is an increase of 14% capacity if we use more number of bits in an image in case of triple-A algorithm. Also high security can be achieved by using pseudorandom number generator (PRNG) in the triple-A algorithm. So as per the result the triple-A algorithm is more efficient in terms of capacity compared to pixel indicator method.

The pixel indicator technique and triple-A algorithm uses the least two LSB bits of any one of the channels used as indicator, by this the capacity of the stego image is limited. To further improve the hiding capacity Kaur et al. [14] introduced a novel technique of embedding data in the 4 LSB bits of an image. One of the three channels is used as indicator. The data is stored in that channel whose color value is small. The indicator is selected depending on specific range. Three range of color values such as {0, 85}, {85, 170}, {170, 255} has been specified. If the color value of a channel falls in the first range {0, 85} then we can store 4 bit of secret data in the channel. Similarly 2 bit and no bit of data can be hidden if the color value is in the second range and third range, which indicates that more number of data bits can be hidden in the channel with lower range. So this method increases the security and capacity of an image.

To increase the capacity and imperceptibility of the stego image, in [15] the author has proposed an adaptive LSB bit method. The different range of the stego key determines the amount of bits to hide in the LSB plane of an image. The uniqueness of this technique is to verify the integrity of the hidden data by using selected bit key. In addition to that this technique hides 4.15 bits in each pixel of an image. This method achieves better security and higher capacity. Swain and Lenka [37] proposed a new technique based on LSB array. Depending upon the length of the secret message the respective LSB array is chosen. This technique provides two levels of security with acceptable hiding capacity. The comparison among the various LSB techniques has been done in the Table 2.

Table 2. Comparison among the various LSB techniques

Ref No.	Capacity	Security	Distortion	Complexity	Advantage
3	Moderate	Moderate	High	Low	Data can be embedded in moderately significant-bit (MSB). So less chance of loss of data in future.
4	High	Moderate	Moderate	High	Capacity is high.
6	Moderate	Moderate	Low	Low	Quality of stego-images obtained is much better with low computational time than simple LSB-substitution method.
7	Moderate	Moderate	Low	Low	Low computational complexity and high quality of stego-images obtained Compared to method [3] [4].
8	Moderate	High	Low	High	Two levels of security is provided to secret data.
9	Moderate	High	Moderate	Moderate	Additional security can be achieved to secret data.
10	Moderate	Moderate	High	Low	New direction of data embedding.
11	Moderate	High	Low	Low	Security to secret data is high.
12	High	High	Low	Low	More capacity and security compared to pixel indicator technique [11].
14	Moderate	Moderate	Moderate	Moderate	Capacity is increased due to 4 bits LSB embedding.
15	High	High	Moderate	High	High security to hidden data.
37	Moderate	High	Moderate	High	Security is high.

3. PVD Techniques

A new concept called pixel value differencing (PVD) has been proposed by Wu and Tsai [16] 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 [17] noticed that, the original PVD technique proposed by Wu and Tsai [16] is vulnerable to histogram-based steganalysis. That is the stego-image exhibit an abnormal behavior 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 behavior shown by the histogram. Hence the security is an added advantage. Chang et al. [20] found that the capacity of the PVD technique presented by Wu and Tsai [16] 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 [21] 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 derieved, 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[16], a steganographic technique called Tri-Way PVD has been proposed by Chang et al. [22] 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 [23] 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 [24] 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 [21] 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 [25] 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. [21] in terms of security and capacity.

Hong et al [26] 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 [27] 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 [16]. This results of this schema reveals that better stego-image

quality and security compared to original PVD concept proposed by Wu and Tsai [16] also the falling-off boundary problem can be avoided.

In 2012, Lee et al [28] 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 [29] 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 neighboring 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 neighboring 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 [30], 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 [31] suggested a new technique to achieve this. In contrast to Wu and Tsai [16] 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 [5] 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 [32] marked this issue and then proposed revised variants of two, three and four sided side match with higher embedding capacity.

Swain[33] 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 neighbors 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 neighbors differencing method the difference value is calculated by same way as in five neighbor differencing method with one extra pixel as upper-left corner. Similarly for seven neighbors differencing method one extra pixel as bottom left corner and for eight neighbors 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 neighbors differencing and the capacity is higher in eight neighbors differencing.

Pradhan et al [38] proposed a pixel value differencing technique based on PVD called two neighbor method, three neighbor method and four neighbor method. The result reveals that the capacity is good in four neighbor method with acceptable stego-image quality. An adaptive pixel value differencing method using vertical and horizontal edges has been proposed by Swain [39]. 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.

The comparison between various PVD techniques has been done in the Table 3.

Table 3. Comparison between various PVD methods.

Ref No	Capacity	Security	Distortion	Complexity	Advantage
16	Moderate	Moderate	Moderate	Low	Provides a new method for hiding secret data.
17	Moderate	High	Low	Low	Avoids the histogram steganalysis occurred in Wu and Tsai [16] method.
20	High	Moderate	Moderate	Moderate	An increase in 84.16% ofcapacity compared to PVD method proposed by Wu and Tsai [16].
21	High	Moderate	Moderate	High	Better stego-image quality and security compared to Wu and Tsai [16].
22	High	High	High	High	Capacity and security is increased compared to Wu and Tsai [16].
24	Moderate	High	Moderate	High	Security to stego-image is better compared to Ref. [17] and Ref. [18].
25	High	High	Moderate	High	Minimum differences in the PVD histograms between the cover and stego-images compared to Wang et al [21].
26	High	High	Low	High	Better embedding performance compared to previous PVD-based methods in terms of payload and image quality.
27	Moderate	High	Low	Moderate	A new direction for data embedding in color images.
28	High	High	Low	High	Capacity and Security are high.
29	High	Moderate	Moderate	Low	Better capacity and security compared to conventional LSBs substitution method.
30	High	Moderate	Moderate	Low	Capacity is more compared to LSB methods.
31	High	Moderate	Moderate	High	More edge areas present compared to Wu and Tsai [16], So more capacity.
32	High	Moderate	Moderate	Moderate	Falling-off boundary problem caused in Ref. [29] is addressed.
33	Moderate	Moderate	Moderate	Moderate	Adds more flexibility in choosing data embedding method.

4. LSB+PVD Techniques

The LSB technique provides the larger capacity and PVD technique offers higher security. In this direction, Wu et al [18] in 2005 has proposed a technique by combining the advantage of LSB and PVD to increase the capacity and stego-image quality. The range value 0 to 255 is partitioned into two parts, one is lower level range if the value is 0 to 15, and the other one is upper level range 16 to 255. The difference value is obtained by using simple PVD strategy[16]. As opposed to Wu and Tsai[16], here the authors have targeted the smooth area to embed more data by using LSB substitution with preserving the stego-image quality. Where as in edge areas simple PVD technique is used. There can be 6 bits hidden in lower level of two consecutive connected pixels by using LSB substitution in smooth areas, which inturn increases the capacity of the proposed method compared to Wu and Tsai [16]. But the suggested method has the demerit that the stego-image can be detected by RS analysis.

The LSB+PVD method proposed by Wu et al [18] is highly identical to LSB technique. An image can have major portion of area having small difference value. So the LSB embedding is used for the major part of the image to hide the bits. It brings a conflict scenario to Wu and Tsai [16] where large number of secret data bits should be hidden in edge area and less number of bits should be embedded in smooth area. Although the use of LSB increases the capacity of the stego-image but is can easily perceivable to Fridrich et al.'s method[5]. In this context Yang et al. [19] proposed an improved LSB+PVD technique which ensures the security of secret data by preserving the same capacity as offered by the LSB+PVD method proposed by Wu et al [18].

Swain [34] proposed a novel steganographic technique to provide better capacity to stego-image. The author combined the PVD method with modified LSB substitution. The image is partitioned into 3×3 pixel blocks. The difference value is determined in each block. According to the author the difference may fall in any of the four levels specified. If the difference value is in lower level then 2 bit LSB substitution is carried out and 3, 4 and 5 bit LSB substitution has been done if the value falls in lower-middle, higher-middle and higher levels. The falling-off boundary value also has been taken care. The experimental result reveals that higher capacity

and less distortion is achieved compared to Wu et al [18]. The comparison between various LSB+PVD techniques has been done in the Table 4.

Table 4. Comparison between various LSB+PVD methods.

Ref No	Capacity	Security	Distortion	Complexity	Advantage
18	High	Low	Low	Low	Better embedding capacity compared to Wu and Tsai [16] method
19	High	Moderate	Moderate	Moderate	Security is increased compared to Wu et al [18].
34	High	Moderate	Moderate	Low	Better capacity, security and less distortion compared to Wu et al [18].

5. Conclusion and Future Scope

This article reviews the various research papers based on LSB and PVD and compares them with regard to embedding capacity, distortion, attack resistance and computational complexity. Least Significant Bit (LSB) and Pixel Value Differencing (PVD) are the most generally utilized strategies for steganography. The LSB substitution can give higher embedding capacity when extended up to 4 LSB planes. The PVD steganography can provide higher security. A combination of PVD and LSB can offer both higher embedding capacity and better security.

Acknowledgement

This work is supported by the Department of Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, by order number SR/FST/ESI-332/2013. KL University, Vaddeswaram, Andhra Pradesh.

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] Wang RZ, Lin CF, Lin JC. Hiding data in images by optimal moderately significant-bit replacement. *IEE Electron. Lett*. 2000; 36(25): 2069–2070.
[4] Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*. 2001; 3: 671–683.
[5] 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.
[6] Chang CC, Hsiao JY, Chan CS. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*. 2003; 36: 1583 – 1595.
[7] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. *Pattern Recognition*. 2004; 37: 469-474.
[8] Swain G, Lenka SK. A novel approach to RGB channel based image steganography technique. *International Arab Journal of e-Technology*. 2012; 2(4): 181-186.
[9] Swain G, Lenka SK. A technique for secret communication using a new block cipher with dynamic steganography. *International Journal of Security and Its Applications*. 2012; 6(4): 12-24.
[10] Gutub A, Ankeer M, Ghalioun MA, Shaheen A, Alvi A. *Pixel indicator high capacity technique for RGB image based steganography*. in: Fifth IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E. 2008: 56-64.
[11] Parvez MT, Gutub AAA. *RGB intensity based variable-bits image steganography*. in: IEEE Asia pacific Services Computing Conference. 2008: 1322-1327.
[12] Gutub A, Qahtani AA, Tabakh A. Triple-A secure RGB image steganography based on randomization. in: *IEEE/ACS International Conference on Computer Systems and Applications*. 2009: 400-403.
[13] Tiwari N, Shandilya M. Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growt. *International Journal of Security and Its Applications*. 2010; 4(4): 53-62.
[14] Kaur M, Gupta S, Sandhu PS, Kaur J. A dynamic RGB intensity based steganography scheme. *World Academy of Science, Engineering and Technology*. 2010; 67: 833-836.

[15] Jain YK, Ahirwal RR. 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)*. 2010; 4: 39-49.
[16] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*. 2003; 24: 1613-1626.
[17] 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.
[18] 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.
[19] 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.
[20] Chang CC, Chuang JC, Hu YC. Spatial Domain image hiding scheme using pixel-values differencing. *Fundamenta Informaticae*. 2006; 70: 171–184.
[21] 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.
[22] Chang KC, Chang CP, Huang PS, Tu TM. A novel image steganographic method using tri-way pixel-value differencing. *Journal of Multimedia*. 2008; 3(2): 37-44.
[23] Lin CC, Hsueh NL. A lossless data hiding scheme based on three-pixel block differences. *Pattern Recognition*. 2008; 41: 1415 – 1425.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] 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.
[29] Chang CC and Tseng HW. A steganographic method for digital images using side match. *Pattern Recognition Letters*. 2004; 25: 1431-1437.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] Swain G. Digital image steganography using nine-pixel differencing and modified LSB substitution. *Indian Journal of Science and Technology*. 2014; 7(9): 1444–1450.
[35] Subhedar MS, Mankar VH. Current status and key issues in image steganography: A survey. *Computer science review*. 2014: 95-113.
[36] Swain G, Lenka SK. Classification of image steganography techniques in spatial domain: A study. *International Journal of Computer Science & Engineering Technology (IJCSET)*. 2014; 5: 219 232.
[37] Swain G, Lenka SK. A novel steganography technique by mapping words with LSB array. *International Journal of Signal and Imaging Systems Engineering*. 2015; 8(1): 115-122.
[38] 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.
[39] 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.
[40] Wang H, Chen G, Zhang M. Edge steganography for binary image. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(5): 2822-2829.
[41] Li Y, Liu Q. Breaking the digital video steganography. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(3): 1691-1696.