Classification of Image Steganography Techniques in Spatial Domain: A Study

Gandharba Swain,
Department of Computer Science and Engineering,
SOA University,
Bhubaneswar 751030, India
gswain1234@gmail.com

Saroj Kumar Lenka,
Department of Computer Science and Engineering,
MITS University,
Lakshmangarh 332311, India
lenka.sarojkumar@gmail.com

Abstract- Steganography is a method of secret communication wherein the very existence of communication is hidden. During the last few decades there have been a tremendous development in digital image steganography and a large number of papers have been published by different researchers. This review paper presents a classification of the spatial domain image steganography techniques. These classifications include, (i) LSB steganography, (ii) RGB based steganography, (iii) pixel value differencing steganography, (iv) mapping based steganography, (v) palette based steganography, (vi) collage based steganography, (vii) spread spectrum steganography, and (viii) code based steganography. In image steganography the different quality measurement parameters are, (i) capacity, (ii) security, (iii) imperceptibility, (iv) temper resistance, and (v) computational complexity. Different researchers have attempted to improve the different quality measurement parameters. At the end of the paper the current promising directions of research are also pointed out.

Keywords- Steganography; data hiding; spatial domain techniques; PSNR; MSE; Correlation

I. INTRODUCTION

Steganography, an art of invisible communication, is achieved by hiding secret data inside a carrier file like image. After hiding the secret data, the carrier file should look innocent so that the very existence of the embedded data is concealed. Mainly it is of three categories, (i) steganography in image, (ii) steganography in audio, and (iii) steganography in video [1]. In recent literature steganography in text has also been proposed [2]. In image steganography the secret message is hidden inside an image in such a way that the change in quality of the image cannot be noticed. In audio steganography the secret message is hidden inside an audio file like a song or music without changing the original quality of it. In video steganography the secret message is hidden inside a video file without disturbing the original quality of the video. In text steganography the secret message is hidden inside a text file without changing its meaning. Image steganography techniques can be classified into two major categories such as spatial domain techniques and frequency domain techniques [1] as shown in Fig.1. In spatial domain techniques the secret message is hidden inside the image by applying some manipulation over the different pixels of the image. In frequency domain techniques the image is transformed to another form by applying a transformation like discrete wavelet transform and then the message is hidden by applying any of the usual embedding techniques. The image in which secret message is hidden is called as the stego-image. There are different categories of methods in spatial domain, (i) LSB steganography, (ii) RGB based steganography, (iii) pixel value differencing steganography, (iv) mapping based steganography, (v) palette based steganography, (vi) collage based steganography, (vii) spread spectrum steganography, (viii) code based steganography, and (ix) others.

In section II the performance measurement parameters of image steganography methods have been illustrated. In section III the different categories of techniques are described. In section IV some promising research directions are identified. Finally in section V the paper is concluded.

II. PERFORMANCE MEASUREMENT PARAMETERS

The performance of various steganographic methods can be rated by three main parameters, (i) capacity, (ii) security, and (iii) imperceptibility [3, 5]. Recently, two more parameters, (iv) temper resistance, and (v) computational complexity are also introduced in literature [4]. The hiding capacity refers to the maximum amount of information that can be hidden in the image. It is represented in bits per byte, or bits per pixel, or in total as number of bytes, or number of kilo bytes. It should be as high as possible. Security means the ability to survive from transformations like cropping, scaling, filtering, addition of noise, and from different attacks. The

different attacks are, (i) steganography-only attack, (ii) known-carrier attack, (iii) chosen steganography attack, and (iv) known steganography attack [6]. In "steganography-only" attack, only the stego-image is available to the intruder for analysis. In "known-carrier attack", both the original image and stego-image are available to the intruder for analysis. In "chosen steganography attack", the steganographic algorithm is available to the intruder along with the known message. In fourth category i.e. the "known steganography attack", the original image, stego-image and the steganography algorithm are available to the intruder for analysis. A good steganographic technique should escape from all these varieties of attacks. Imperceptibility refers to perceptual transparency i.e. no visual artifacts on the stego-image. It should be as high as possible. Temper resistance means the survival of the embedded data in the stego-image when attempt is done to modify it. Finally, computational complexity refers to the computational cost of embedding and extraction. It should be as low as possible.

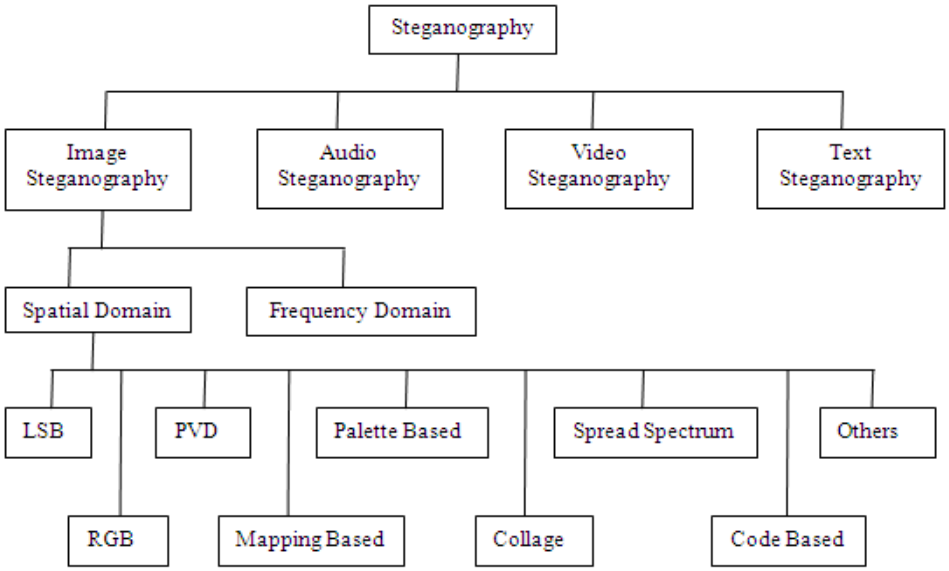

Fig.1. Classification of spatial domain image steganography techniques

The distortion in the stego-image can be measured by the parameters like, mean square error (MSE), peak signal-to-noise ratio (PSNR), and correlation (r) [22]. The lesser distortion means, lesser MSE, but higher PSNR. If p is a M×N grayscale image and q is its stego-image, then the MSE and PSNR values are computed using (1) and (2). The p_{ij} and q_{ij} are the original image pixel value and the stego-image pixel value at i^{th} row and j^{th} column respectively. For color images a pixel comprises of 3 bytes. Each byte can be treated as a pixel and the same equations can be used to calculate the MSE and PSNR.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2 \quad (1)$$

$$PSNR = 10 \times \log_{10} \frac{C_{max}^2}{MSE} \quad (2)$$

The c_{max} represents the actual maximum pixel value in the image [1, 5]. PSNR values falling below 30 dB indicate a fairly low quality stego-image i.e. distortion caused by embedding is severe. However a high quality stego-image should possess the PSNR value more than 40 dB [1]. The correlation, denoted by the letter r, is a measure of the similarity between the original image and the stego-image. It is measured using (3). The $\bar{p}$ and $\bar{q}$ are the average pixel value in original image and stego-image respectively. The MATLAB built in function corr2(p, q) evaluates the correlation between the cover image, p and the stego-image, q. The maximum value of corr2(p, q) can be 1, if p and q are the same images. So if distortion is lesser, then the correlation can be higher.

$$r = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - \bar{p}) \times (q_{ij} - \bar{q})}{\sqrt{\left(\sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - \bar{p})^2\right) \times \left(\sum_{i=1}^{M} \sum_{j=1}^{N} (q_{ij} - \bar{q})^2\right)}} \quad (3)$$

It has been experimentally investigated that stego-images bearing secret message, are statistically natural images [7]. By adding the unnatural message inside a natural image, there is a change in statistics, but this change is so small, and thus does not allow for reliable detection. Every year new steganographic techniques are evolved, at the same time the new types of attacks are also introduced. As per information theory the entropy measure can be an attack [8]. The entropy of the stego-image, S; will be equal to the entropy of the cover image, C; plus the entropy of the embedded data, E.

III. THE DIFFERENT STEGANOGRAPHY METHODS IN SPATIAL DOMAIN

A. LSB Staganography

The simplest and popular image steganographic method is the least significant bit (LSB) substitution. It embeds messages into cover image by replacing the least significant bits directly. The hiding capacity can be increased by using up to 4 least significant bits in each pixel. It has a common weak point i.e. the sample value changes asymmetrically. When the LSB of cover medium sample value is equal to the message bit, no change is made. Otherwise the value 2n is changed to 2n+1 or 2n+1 is changed to 2n. But the changes from 2n to 2n-1 or 2n+1 to 2n+2 will never happen. This asymmetry can be captured by simple steganalytic programs. There are a lot of improvements and modifications proposed to strengthen this technique. In [9] a steganography approach for data hiding is proposed, wherein the binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. As the image is encrypted and then embedded, the security is enhanced.

Kekre et al. [10] proposed an LSB technique to embed variable number of bits in different pixels based on its value. They divided the pixel values into 4 ranges, such as, R_1={0, 191}, R_2={192, 223}, R_3={224, 239}, and R_4={240, 255}. Then they embedded i bits in a pixel which belongs to range R_i , for i=0,1,2,3. By making the number of bits adaptive, the security is enhanced and by embedding upto 4 bits in some of the pixels the capacity is also increased. Zhang and Tang [11] proposed an enhancement over LSB technique by choosing a set of pixels at a time randomly with the help of a pseudo random number and then embedded n bits in each pixel using addition and modular division operations. The n value is dependent on the length of bit stream of embedded message. Both security and capacity is addressed. Mathkour et al. [12] proposed a spiral based LSB substitution approach for hiding message in image. This approach is based on LSB substitution technique applied on RGB color components of an image. The idea is to divide the image into many segments and apply a different processing on each segment. The approach considers three processes corresponding to three sequences; (i) start from corner, (ii) start from centre and (ii) hybrid. And applies two directions for the sequencing process; (i) counter clock wise direction and (ii) clock wise direction. Only security is enhanced.

Mishra et al. [13] proposed a modified LSB approach, wherein the secret binary message is converted into 8-bit blocks and the image is divided into 8-pixel blocks. Then by using a pseudo random number generator (PRNG), the 8-bit message block is embedded into a chosen 8-pixel image block. This results in distribution of the message over the entire image randomly. Thus, even if LSBs are removed and read, they do not convey any intelligent information. If the integer value of each 8-bit message block is between 0 and 85, the embedding of these 8-bits under consideration takes place in the R plane. Similarly, values ranging between 86 and 170 are embedded in G plane and values between 171 and 255 are embedded in B plane. Only security has been improved. Although this method seems to be better than simple LSB substitution, but the visual steganalysis says that the distortion in the stego-image is noticeable if large amount of data is embedded. The statistical analysis carried out by plotting histograms says that if the amount of data is increased the variation in the histogram is observed.

In [14] a technique based on LSB array is proposed. The LSB array means all the LSB bits are kept together to form an array. In this method a suitable image is chosen from a large number of images for a given data. The secret data is converted to bit stream. Then it is mapped in the LSB array of different images and steganographed at the maximum matching portion of it. This method makes a very less distortion, but the computational cost for searching of a suitable image is high. This method is following simple LSB substitution and vulnerable to RS analysis. In [15] a technique with four LSB arrays is proposed. The four arrays, such as LSB, LSB1, LSB2 and LSB3 are formulated separately by collecting the bits from the 8^{th} (LSB), 7^{th}, 6^{th} and 5^{th} bit locations of the pixels respectively. The cipher text is partitioned into four segments, each is called a block. The first block is mapped over the LSB array and embedded at maximum matching portion of the LSB array. Similarly the second, third and fourth blocks are embedded at maximum matching portion of LSB1, LSB2 and LSB3 arrays respectively. Both the security and capacity has been improved. The capacity can be four times than that of [14]. A LSB array based technique by embedding the different words in maximum matching portion on the LSB array is proposed by Swain and Lenka “in press” [110]. In [16], a different style of LSB substitution is applied. By considering 8-connectivity found the dark places and then embedded in LSBs of these dark places. This method is not direct LSB substitution, so security is obviously improved.

Swain et al. [17] proposed message bit dependent dynamic steganography to embed one bit in 7^{th} bit location of every pixel. Although capacity is only one bit per byte, but security is enhanced. In [18] a LSB steganography is used to embed two bits of message in two bit locations either (6^{th} and 7^{th}) , or (7^{th} and 8^{th}) , or (6^{th} and 8^{th}) bit locations of a pixel depending on the value of an index variable. The capacity is improved (2 bits per byte) and security is strengthened. In [19] dynamic embedding based on an evaluation function is used. Two LSBs are exploited. Some selected pixels are embedded. So capacity is not improved, only security is enhanced. In [20] dynamic embedding based on bit pattern of secret message is used. Three LSBs are exploited in a pixel, but only two bits are embedded. Some selected pixels are embedded. So capacity is not improved, only security is

enhanced. In [21] dynamic embedding based on bit pattern of secret message is used. Three LSBs are exploited in a pixel, but only two bits are embedded. All the pixels are embedded. So capacity is improved (2 bits per byte) and security is also enhanced. A moderate bit substitution (MBS) data hiding technique is proposed by Pharwaha in [22]. As per this technique a pixel in the given image is skipped if all the first three positions of the LSB in it are one. The data bit is embedded at position next to first zero appearing at any of the first three LSB positions in the pixel. This process leads to the random selection of bit position in a pixel. To improve the perceptual quality of stego-image a post pixel adjustment was also followed. Only security is improved.

TABLE 1. Comparison among the different LSB techniques

Ref.	Targeted Parameter		Comments
	Security	Capacity	
[10]	Yes	Yes	Adaptive LSB embedding
[11]	Yes	Yes	LSB embedding based on pseudo random number
[12]	Yes	No	Different image segments are processed separately
[13]	Yes	No	Vulnerable to histogram analysis
[14]	Yes	No	Suffers with high computational cost and RS-analysis
[15]	Yes	Yes	High capacity upto 4 bits per byte
[16]	Yes	No	Capacity is less than 1 bit per byte
[17]	Yes	No	Message bit dependent embedding
[18]	Yes	Yes	Capacity is 2 bits per byte and embedding locations are adaptive
[19]	Yes	No	Message bit dependent embedding
[20]	Yes	No	Message bit dependent embedding
[21]	Yes	Yes	Capacity is 2 bits per byte and message bit dependent embedding
[22]	Yes	No	Moderate bit substitution and capacity is less than 1 bit per byte
[23]	Yes	Yes	Adaptive embedding
[24]	Yes	Yes	Adaptive embedding
[25]	Yes	Yes	Adaptive embedding and capacity is more than 2 bits per byte
[26]	Yes	No	Based on a pseudo random number and broke the PoV
[27]	Yes	No	Capacity is less than 1 bit per byte
[28]	Yes	No	Capacity is approximately 1 bit per byte
[29]	Yes	No	Use of histogram transformation functions
[30]	Yes	No	After LSB substitution optimal pixel adjustment is used
[31]	Yes	Yes	Encrypted message is compressed and then embedded
[32]	Yes	Yes	Capacity is 2 to 3 bits per byte
[33]	Yes	No	A secret key is used in LSB embedding
[34]	Yes	No	Use of histogram transformation functions
[35]	Yes	No	Associated graph coloring problem with an image block

Adaptive embedding refers to the hiding of variable number of bits in different pixels. Based on some statistical analysis one can find the embedding depth, k in a pixel and hide k bits by substituting k LSBs in that pixel [23]. Here both capacity and security has been improved. Jain and Ahirwal proposed an adaptive embedding approach by using a private stego-key [24]. The private stego-key consists of five gray level ranges that are selected randomly in the range from 0 to 255. The selected key shows the five ranges and each range substitute different number of bits in LSBs. By using this adaptive embedding idea we can hide up to 4 bits in some pixels, thus it greatly increases the capacity in addition to security. Meena et al. [25] also proposed an adaptive embedding technique based on the correlation of a pixel with its neighboring pixels. Adaptive techniques are obviously more secured and possess more capacity.

One major drawback of LSB embedding is the existence of detectable artifacts in the form of pairs of values (PoVs). The Lee et al.'s scheme [26] broke the regular pattern of PoVs by using a pseudo random number generator and increased the security level. If the secret message is very short then only the LSBS of the darker and brighter pixels can be used to randomize the embedding process. In [27] such an embedding by targeting only three LSBs of darker and brighter pixels is used along with encryption. So, only the security is improved. In [28] also the 4-LSBs of darker and brighter pixels are targeted. Here also only security has been improved.

Approximately 25% of the pixels are defined as darker or brighter category, so no improvement in capacity. Lou and Hu [29] proposed histogram transformation based LSB steganography, which can escape from RS-analysis and Chi-square attack. Security has been improved. Chan and Chang [30] used simple LSB with optimal pixel adjustment to improve the quality of stego-image. To improve both capacity and security Bashardoust et al. [31] used encryption, compression, and then LSB embedding. And by using encryption with LSB steganography only security is improved in [32]. To improve the security with LSB substitution, the embedding has been randomized by using a secret key [33]. Marcal and Pereira [34] applied reversible histogram transformation functions to the image before and after LSB embedding to survive from RS-analysis. Douiri et al. [35] located the optimal positions of the pixels in the cover image using GCP (graph coloring problem) algorithm and then embedded in LSBs to survive from RS-analysis and Chi-square attack. Table 1 represents the status of the parameters being attempted to be improved by the respective authors.

B. RGB Based Steganography

A pixel in a color image possesses three components; (i) red (R), (ii) Green (G), and (iii) blue (B). Each component comprises of 8 bits. These R, G, and B components, called as channels can be treated as independent bytes and LSB substitution can be applied. That means 3 data bits can be hidden in one pixel. But as these three bits together form the pixel, it is not wise to apply direct LSB substitution, some other methods are suggested. So to enhance the security some modified approaches are applied.

A technique called pixel indicator technique is proposed by Gutub et al. [36]. This technique uses the last two LSBs of one of the channels from R, G, or B as indicator for existence of data in other two channels. The indicator channels are chosen in sequence with R being the first. In the first pixel R is indicator, G is channel 1 and B is channel 2. In the second pixel G is indicator, while R is channel 1 and B is channel 2. In the third pixel B is indicator, while R is channel 1 and G is channel 2. The length of the secret message is stored in first 8 bytes of the cover image. The disadvantage of this technique is that the capacity depends upon the indicator bits and based on the cover image, it is not high, may be in an average 3 bits per pixel. Also it uses fixed number of bits per channel (2 bits) to store data. Only security has been enhanced.

Parvez and Gutub [37] proposed a better technique to enhance the security. The idea in this technique is, for insignificant colors, significantly more bits can be changed per channel. For example suppose in a pixel R=255, G=255 and B=255, then a change in the R channel will show a distortion. If in a pixel R=55, G=255 and B=255, a change in the R channel will not show a distortion. The lower color value of a channel has less effect on the overall color of the pixel than the higher value. Therefore more bits can be changed in a channel having ‘low’ value than a channel with a ‘high’ value. Both security and capacity is improved. Even though the pixel indicator scheme proposed by Pervez and Gutub adds some randomization to harden the detection of the secret data, its capacity varies depending on the actual values of the indicator channel. So the actual capacity is unpredictable.

The technique proposed by Gutub et al. [38] tries to add more randomization to the selection of the pixels in which secret data is to be stored, affecting the number of bits used to keep the secret data, and the channels that are used to store the secret data. This technique is called as Triple-A algorithm. The algorithm is having two parts, such as ; (i) encrypting and (ii) hiding. In part 1, the message is encrypted using AES algorithm which will produce the cipher text. In part 2, The RGB image is used as cover media and the cipher text is hidden inside the image using a pseudorandom number generator (PRNG). The PRNG produces two new random numbers per iteration, say seed1 and seed2. The seed1 random number is used to determine the RGB component where cipher text will be hidden and seed2 determines the number of bits that can be hidden in it. As per the observation and conclusion by Tiwari and Shandilya [39] the Triple-A algorithm introduces more randomization by using two different seeds which adds more security to the technique. Triple-A has a capacity ratio of 14% and can be increased if more number of bits are used inside the components. Triple-A has a capacity better than the pixel indicator.

In [40] a pixel indicator technique is proposed in which one of the channels is the indicator and other two channels are the data channels. The embedding is done based on four defined conditions. In this technique the indicator channel is the channel whose sum over all the pixels is the maximum. The capacity is unpredictable and indicator is fixed for the entire image. Only security is enhanced. In [41], a novel approach to RGB channel based steganography technique is proposed. The image is divided into 8 blocks and the encrypted message is divided into 8 blocks. One message block is allocated to be embedded in only one image block by a user defined sub key. One of the three channels in each pixel is used as indicator channel. The indicator channel is the channel whose sum over all the pixels is the maximum. The indicator channel for the different blocks is changed. The other two channels (often called as data channels) are used for hiding cipher text bits in 4 least significant bit (LSB) locations. In a data channel 4 bits of cipher text can be embedded, with a provision that the change in pixel value is less than or equal to 7. The two LSBs of indicator shall indicate whether the cipher text is embedded in only one data channel or in both data channels, so that retrieving can be done accordingly at the

receiver. The message blocks are allocated to the image blocks by the sender, using a key; which provides another level of security. Thus the security is three fold, and capacity is also improved.

Juneja and Sandhu [42] proposed a very interesting method by compressing a 24-bit image to 8-bit image and hiding data in this 8-bit image. A 24-bit bit-map image would be converted to an 8-bit bitmap image while simultaneously encoding the desired hidden information. An algorithm would be created to select representative colors out of the 24-bit image to create the palette for the 8-bit image. This palette would then be optimized to an 8-bit color map that could be applied with minimal changes to the quality of the original image. The process of compressing the image from a 24-bit bit-map to an 8-bit bit-map resulted in minor variations in the image that are scarcely perceptible to the human eye. However, these slight variations aid in hiding the data. Since there would not be an original 8-bit image to compare with the stego-image, it would be impossible to discern that the data are different from the slight variations caused by compression. Only security is improved.

Kaur et al. [43] proposed a dynamic RGB intensity based algorithm in which variable number of bits are hidden in different data channels. The LSBs of one of the three channels is used as indicator. The order of the indicator can be selected randomly. Data is stored in other two channels. The channel, whose color value is lowest among the two channels other than the indicator, is used to store the data in its least significant bit locations. If the channel value lies in the range {0, 85}, then 4 bits data can be hidden. If the channel value lies in the range {86, 170}, then 2 bits can be hidden and if the channel value lies in the range {171, 255}, then no data will be hidden. The advantage in this technique is usage of 4 LSBs in some of the data channels, which increases the hiding capacity. Both security and capacity is enhanced.

The pixel indicator technique proposed by Gutub et al. [36] is again extended by Gutub in [44]. The extension is: the first 8 bytes at the beginning of the image used to store the size of the hidden message, is also used to determine the beginning of the indicator channel sequence. These 8 bytes consumes all the LSBs of the RGB channels, assuming it is enough to store the size of the hidden bits. The visual steganalysis and histogram based steganalysis can not attack this technique. It has been observed that the histograms for R, G and B channels of original image and its corresponding stego-image are completely identical. The disadvantage of this technique is that the capacity depends on the indicator bits and based on the cover image. Also, the algorithm uses fixed number of bits per channel (2 bits) to store data and the image may distort with increase in number of hidden bits per channel.

A new pair wise bit based data hiding method for 24 bit images is proposed by Ghosal [45]. The absolute difference value of number of 1's and 0's in R channel, say it is d is calculated. Then d is divided by the number of channels, n (n is 2 for 24 bit images). Then n number of bits is embedded both in G and B channels. Both security and capacity has been improved.

Juneja and Sandhu [46] identified the smooth and edge regions. They embedded at LSBs of randomly selected pixels in edge and smooth regions. In a RGB image if a pixel is having less resemblance with its neighbors then more number of bits can be embedded [47]. In an average only 50% of the pixels can be targeted to embed. Only security is improved, not capacity. Juneja and Sandhu [48] used a hybrid approach for color images using component based LSB substitution and adaptive LSB substitution to improve the hiding capacity and imperceptibility. They also used AES encryption to increase security. Table 2 represents the status of the parameters being attempted to be improved by the respective authors.

TABLE 2. Comparison among the different RGB techniques

Ref.	Targeted Parameter		Comments
	Security	Capacity	
[36]	Yes	No	The first pixel indicator technique
[37]	Yes	Yes	More bits are embedded in a channel with low value
[38]	Yes	Yes	Based on generation of random number
[40]	Yes	No	Capacity is very less
[41]	Yes	Yes	Both image and message are divided into 8 blocks
[42]	Yes	No	24-bit bit-map image is converted to 8-bit bit-map image
[43]	Yes	Yes	Adaptive embedding
[44]	Yes	No	Pixel indicator technique
[45]	Yes	Yes	Capacity depends on the number of 1's and 0's in the indicator channel
[46]	Yes	Yes	Image is divided into smooth and edge areas
[47]	Yes	No	Variable number of bits are embedded in color components
[48]	Yes	Yes	A hybrid approach

C. Pixel Value Differencing Steganography

A new track in image steganography called pixel value differencing is proposed by Wu and Tsai [49] in 2003 for gray images. A difference value d is calculated from every non-overlapping block of two consecutive pixels, say p_i and p_{i+1}, of a given cover image. The way of partitioning into two-pixel blocks is by scanning all the rows in a zig-zag manner. The difference value d is mapped into a range table. The range table is divided into different ranges of specific widths. The width of a range indicates the number of bits that can be hidden in a block. This difference value d is replaced by a new difference value d' after data is embedded in the block. This technique possesses moderate capacity, high security and better imperceptibility. Zhang and Wang [50] observed that this PVD steganography is vulnerable to histogram analysis attacks and proposed to take different ranges corresponding to different blocks instead of fixed ranges as in the original PVD method.

Wang et al. [51] proposed a steganography method with pixel value differencing and modulus function. As per this method, in first step we have to derive a difference value from two consecutive pixels by utilizing the PVD technique. The hiding capacity of the two pixels depends upon the difference value. In second step the remainder of the two consecutive pixels can be computed by modulo operation, and then the secret data can be embedded into the two pixels by modifying their remainder. In this scheme there is an optimal approach to alter the remainder so as to greatly reduce the image distortion caused by hiding the secret data. The values of the two consecutive pixels are scarcely changed after the embedding of the secret message by the proposed optimal alteration algorithm. Experimental results reveal that this algorithm is not vulnerable to RS-analysis.

To increase the hiding capacity Chang et al. [52] proposed tri-way pixel value differencing using four pixel blocks. As per this technique the image is divided into 2×2 non-overlapping blocks as shown in Fig. 2. Each 2×2 block includes four pixels: $p_{(x,y)}$, $p_{(x,y+1)}$, $p_{(x+1,y)}$, and $p_{(x+1,y+1)}$, where x and y represent the pixel location in the image. Let $p_{(x,y)}$ be the first point and then the pixel pairs can be found by grouping $p_{(x,y)}$ with the right, the lower and lower-right neighboring pixels. These three pairs are named as p_0, p_1, and p_2, where $p_0 = (p_{(x,y)}, p_{(x,y+1)})$, $p_1 = (p_{(x,y)}, p_{(x+1,y)})$, and $p_2 = (p_{(x,y)}, p_{(x+1,y+1)})$. When using this method for embedding secret data, each pair has its modified P_i' and a new difference d_i' for i = 0, 1, 2. Now the new pixel values in each pair are different from their original ones. That is we have three different values for starting point $p_{(x,y)}$ named as $P'_{0(x,y)}$, $P'_{1(x,y)}$, and $P'_{2(x,y)}$, from p_0, p_1, and p_2 respectively. However, only one value $P'_{i(x,y)}$ should exist. Therefore one of $P'_{i(x,y)}$ is selected as the reference point to offset the other two pixel values i.e. one pair is used to adjust the other two pairs and construct a new 2×2 block. The capacity is increased.

$p_{(x,y)}$	$p_{(x,y+1)}$
$p_{(x+1,y)}$	$p_{(x+1,y+1)}$

Fig.2. Example of four pixel block

Like these pixel-block techniques, other techniques based on correlation of a pixel with its neighbor pixels have also been evolved. Chang and Tseng [53] proposed two sided, three sided and four sided side match methods in which the correlation of a target pixel with its neighboring pixels is exploited to take embedding decision in the target pixel. The two sided side match method uses the side information of upper neighboring pixel P_U and left neighboring pixel P_L to take embedding decision. The pixels are scanned in raster scan order. Given an input pixel P_X with gray value, g_x; let g_u and g_l be the gray values of its upper neighboring pixel P_U and left neighboring pixel P_L respectively. Then a difference value $d = (g_u + g_l)/2 - g_x$ is computed. A small difference value indicates that the pixel is in a smooth area, whereas a large difference value indicates that the pixel is in an edge area. If d has a value -1, 0 or 1, then one bit secret data is embedded into LSB of pixel P_X using the conventional LSB substitution method. Otherwise if $|d| > 1$, then n number of bits that can be embedded in the pixel is calculated as, $n=\log_2 |d|$. A sub-stream of n bits from the secret data is taken and is converted to integer b. Then the new difference value, d' is calculated as $d' = 2^n + b$, if d >1, otherwise $d' = -(2^n + b)$, if d < 1. Finally the new value of the pixel P_X is defined as, $g'_x = (g_u + g_l)/ 2 - d'$. Sometimes the new value of the pixel P_X may fall off the boundary of the range {0, 255}. If a pixel suffers with fall off boundary problem (FOBP), then it is escaped from embedding.

The three sided side match method is three types: Type 1, Type 2 and Type3. In Type 1 three neighboring pixels upper, left and right are exploited. In Type 2 the three neighboring pixels upper, left and bottom are exploited. In Type 3 the four corner neighboring pixels left-upper, right-upper, left-bottom and right-bottom are exploited. The four sided side match method uses the four neighboring pixels upper, left, right and bottom to take embedding decision. It has been observed from the experimental results that the two sided side match steganography has larger embedding capacity, whereas the four sided side match steganography has less distortion. This side match method suffers with a problem known as fall in error problem (FIEP). Swain and Lenka [64] addressed this problem and then proposed improved versions of two, three and four sided side match

with higher capacity. Subsequently it is extended to five, six, seven and eight neighbor pixels "unpublished"[67]. The hiding capacity of the 2-pixel block PVD scheme is further improved by using the range table based on perfect square number [65]. In [54], Kim et al. proposed a similar technique like that of side match by using three neighboring pixels upper, left and bottom. In this technique the fall off boundary condition does not arise. The number of bits to be embedded is calculated in a slightly different way. However it does not help in increasing the capacity.

Zhang et al. [55] proposed a pixel value differencing steganography by considering the largest difference among the three neighboring pixels. The three neighboring pixels upper, left and upper-left corner are used for estimating the number of bits to be embedded in the target pixel. This method can hide more amount of data compared to the three sided method proposed in [53]. But this technique is not robust. In [63] also a similar method using maximum difference from two, three and four neighbor pixels is proposed. Subsequently it is extended to five, six, seven and eight neighbors in [66]. In [56] four neighbor and eight neighbor methods similar to that of side match methods have been proposed. The four neighbor method is two types. Type 1 is by considering the left, right, upper and bottom neighbors to take embedding decision. The type 2 is by considering the upper-left, upper-right, bottom-left and bottom-right neighbors to take embedding decision. In eight neighbor method all the eight neighbors left, right, upper, bottom, upper-left, upper- right, bottom-left and bottom-right are considered to take embedding decision. All these methods embed variable number of bits in different pixels making the attack difficult. Capacity is also increased.

LSB methods give high capacity, whereas PVD methods give high security. The LSB and PVD approaches can be combined together to get both high capacity and high security. Wu et al. [57] proposed a LSB+PVD technique using two pixel blocks. If the difference is less than or equal to 15, they applied 3-bit LSB substitution. If the difference is more than 15, they applied PVD method. After 3-LSB bit substitution if the new difference becomes greater than 15, then some adjustment was planned. Yang et al. [58] found that Wu et al.'s LSB+PVD approach is conformable to the LSB approach. They studied that in 90% of the blocks the difference is less than or equal to 15. Secondly the LSB+PVD approach embedded more number of bits in smooth areas than edge areas, which contradicts to the principle that in "edge areas more number of bits can be hidden". Furthermore they proposed a modified method of LSB+PVD steganography with enhanced security.

In [59], Liao et al. proposed four pixel differencing and modified LSB substitution technique by conforming to the issue that more number of bits can be hidden in edge areas and less number of bits can be hidden in smooth areas. They calculated the average difference value and partitioned the range into low level and high level. Pixels located in a block are embedded with k-bits of data using modified LSB substitution method, where k is decided depending upon the average difference value in that block. This technique does not use the PVD concept used in [49]. In order to increase the embedding capacity Yang et al. [60] proposed a pixel value differencing technique by processing two pair of pixels in a block at a time instead of a pair of pixels at a time as done by Wu and Tsai [49]. The four pixels can be grouped in three different ways such as two horizontal pairs, two vertical pairs and two diagonal pairs. After embedding in two pairs at a time, they proposed a shifting scheme to avoid fall off boundaries of the range {0,255}. In this method the capacity is not only improved, but also the security is enhanced.

In [61], Hong et al. proposed a steganography technique using PVD and diamond encoding with multiple-base notational system. Lee et al. [62] proposed a high-payload steganography to hide a large image inside a smaller cover image. The secret image is compressed by JPEG2000 and then embedded in the cover image using tri-way pixel-value differencing. Ioannidou [68] used hybrid edge detection technique to identify the edge areas. They combined fuzzy edge detector and canny edge detector to find a larger set of edges and achieved high embedding capacity. Kaur and Jindal [69] combined 3×3 scanning method using different orientation with sobel operator to detect edges in RGB images and hided in blue components. Mandal and Das [70] extended the PVD technique to RGB images by treating each R, G, and B components as a pixel. Table 3 represents the status of the parameters being attempted to be improved by the respective authors.

TABLE 3. Comparison among the different PVD techniques

Ref.	Targeted Parameter		Comments
	Security	Capacity	
[49]	Yes	No	The first PVD technique, possesses moderate capacity
[50]	Yes	No	Ranges in the range table are changed from pixel to pixel
[51]	Yes	No	Distortion is minimized
[52]	Yes	Yes	Used tri-way PVD
[53]	Yes	Yes	Suffers with FIEP problem
[54]	Yes	Yes	Calculation of n value (no. of bits to be embedded) is slightly different
[55]	No	Yes	Capacity is larger than the side match method
[56]	Yes	Yes	Similar to side match
[57]	No	Yes	LSB + PVD approach
[58]	Yes	Yes	LSB + PVD approach
[59]	No	Yes	Modified LSB substitution
[60]	Yes	Yes	Processed a pair of pixel blocks at a time
[61]	Yes	Yes	PVD with diamond encoding
[62]	Yes	Yes	Used tri-way PVD
[63]	No	Yes	Capacity is larger than the side match
[64]	Yes	Yes	FIEP addressed
[65]	Yes	Yes	The range table is based on perfect square, capacity increased
[66]	No	Yes	Capacity is larger than side match
[67]	Yes	Yes	Extension of [64] to five, six, seven, and eight neighbors
[68]	Yes	Yes	Used fuzzy edge detector and canny edge detector to identify edges
[69]	Yes	Yes	Used sobel operator to detect edges
[70]	Yes	No	Extended the original PVD to color images

D. Mapping Based Steganography

Wang and Chen [71] introduced a two-way block matching method by dividing the secret image into blocks and then mapped these blocks on to the cover image. Kumar and Roopa [72] also proposed a method similar to block matching method with improved security. Al-Husainy [73] proposed a new kind of steganography by mapping the pixels of the image to the characters in a message. As per this method the 26 alphabets from a to z, comma, blank space, full stop, single cote, starting parenthesis and closing parenthesis (total 32 characters) can be used to make a message. These 32 characters can be represented in 5 bits. By adding bits 00, 01, 10, 11 on the left of the five bits we can make the character into 7 bits and 4 in numbers. That means a character of the message is having four representations in 7-bit format. The cover image should be 8-bit image, where each pixel is represented by 8 bits. Now the 8 most significant bits of the pixels of the cover image are mapped to the 7-bit character values, if match occurs, then the LSB of that pixel is set to 1. If the index of this pixel is i, then the LSB of $(i-1)^{th}$ pixel is set to 1, LSB of (i-2)th pixel is set to 0, LSB of $(i+1)^{th}$ pixel is set to 1 and LSB of $(i+2)^{th}$ pixel is set to 0, These five pixels are no more available for mapping further. In this way all the characters of the message are mapped and for each match a LSB bit pattern 01110 centered at the matched pixel is formed to extract the character at the receiver.

The method looks to be interesting. But the capacity is very less. If we take a very large message it may not be possible to embed in an image. The experimental results are observed for short messages up to 2000 characters only.

E. Palette Based Steganography

A palette is a set of discrete colors. Palette is used mainly for two purposes. Firstly it allows you to paint with a selected set of colors, in the way an oil painter works with colors from a limited number of tubes. Secondly, it forms the color maps of indexed images. An indexed image is able to use a maximum of 256 different colors, but these can be any colors. The color map of an indexed image is called as an "indexed palette".

Fridrich [74] proposed a steganography method for hiding message bits into the parity bit of close colors. For each pixel with a color palette index i in image f, one data bit (0 or 1) is embedded after determining the closest entry with a different parity. Fridrich and Du [75] also proposed a modified approach to improve the security in

palette based steganography. Wu et al. [76] proposed some modification to Fridrich's method by adding some preprocessing. The root mean square (RMS) error is minimized by iteratively updating a color in a palette before embedding process is applied. It can also be regarded as a replacement operation to remove a specified entry from the palette and replace it with a new color.

A palette-based image steganographic method has also been proposed by Wang [77]. In this method data embedding is done by quantizing similar colors in the palette. Unlike previous methods, this method's rate-distortion behavior is independent from the embedding message, so that given the length of the embedding message, the distortion on the host image can be determined before embedding. This method gives better PSNR value. Assuming that the length of the palette is n, then sum of all pair colors distance is denoted as $D = \sum_{i=0}^{n-2} |p_i - p_{i+1}|$. Where p_i is the pixel value with index i. The absolute value of pair of pixels refers to their distance; it can be defined as every color components scale value difference sum. Besides this the maximum pair color distance, $d = \text{Max} \mid p_i - p_{i+1} \mid$, i =0, 1… n-2, is used as a measure of security. If the distance between two colors is greater than human visual threshold (HVT), the artifacts can be noticeable. So d should be less than HVT. If value of D is less then, the security is more. To decrease the value of D further Zhou et al. [78] proposed direct color pair sort (DCPS) algorithm. This DCPS algorithm has same complexity but can be executed faster.

Zhang et al. [79] proposed a multi-bit assignment steganography in palette images wherein each color that possess close neighboring colors in the palette are exploited to represent several secret bits. If a color possesses atleast one neighbor color it can be called as gregarious color, and a set containing a gregarious color and its all neighbors are called as a neighborhood set. For any pixel with a gregarious color, one can always find a suitable color in the original color's neighborhood set and replace the original color with it to hide atleast one secret bit. Kim et al. [80] also proposed a palette based steganography scheme. This scheme first divides the secret data into several parts based on the number of colors in the cover image and then embeds secret data into the cover image part by part by expanding palettes and modifying indices. Saleh et al. [81] proposed a steganography technique for palette images based on histogram analysis. This technique gives better hiding capacity.

F. Collage Steganography

A new kind of steganography known as collage steganography has been proposed by Shahreza and Shahreza [82], wherein the information is hidden inside the image by changing the appearance instead of its features. In this method images of a number of objects are put on a scene together to form a new image. Then by changing the place and type of each object, information is hidden in the image. Based on the secret information bits the place of the object is changed. Although this method has a lot of advantages, the simple attacks like adding noise, could break the method. So an improved collage steganography method is proposed again in [83]. Although the basic principle is same as that of collage steganography, the implementation is different. This method is robust against attacks such as JPEG compression, blurring and addition of noise. It is well known that image capturing devices add some noise to the captured image. This noise is due to different components of the image capturing device. Using this trick and the fact that consecutive images captured from the same scene will be different due to device noise, a new embedding technique called PSteg: steganograohy by patching is proposed by Petrowski et al. [84]. PSteg creates stego-images by patches obtained from multiple captured copies of the selected cover image. Such an approach reduces the embedding distortion to the image capturing device noise which is less prone to perceptual and statistical detection.

G. Spread Spectrum Steganography

Various kinds of steganography techniques have been developed over the past two decades. One of the popular techniques is spread spectrum image steganography (SSIS). In this direction Smith and Comiskey [85] described three schemes, namely direct sequences, frequency hopping, and chirp. Tsai et al. [86] proposed two methods namely, block spread spectrum and duplicate spreading.

Techniques of error-control coding, image restoration, and those similar to spread spectrum can be combined with SSIS [87]. The fundamental concept is the embedding of hidden information within noise, which is then added to a digital cover image. This noise is typical of the noise inherent to the image acquisition process and if kept at low levels, is not perceptible to human eye or by computer analysis without access to the original image. To successfully decode the message, image restoration techniques and error-control coding are employed. Image restoration is used to obtain an approximate estimate of the original cover image from the stego-image and within the system the message is optionally encrypted. Satish et al. [88] enhanced the above SSIS technique, using chaotic encryption of the message and chaotic modulation of the enciphered message. Widadi et al. [89] also proposed a similar technique called hybrid direct sequence/frequency hopping technique.

H. Code Based Steganography

Code based steganography techniques are also equally interesting techniques. The predictive code based steganography was proposed by Yu et al. [90] in 2005. This technique hides secret data into an image by modifying the prediction errors. Due to the use of uniform quantization embedding rule, the prediction errors

distribution caused by data hiding provides enough evidence to make steganalysis. To enhance security a modified method have been proposed in [91], which preserves the prediction errors' distribution by choosing the optimum adjustment parameter.

In image steganography, a pixel is capable to carry secret bits either by adding or subtracting one to or from the gray value. In image steganography, a pixel can carry secret bits by adding/subtracting, one to/from the gray value. This kind of steganography can hide a longer message than simple LSB embedding. A double layered embedding method is proposed by Zhang et al. [92], in which binary covering codes and wet paper codes are used to hide messages in the LSB plane and second LSB plane respectively. Syndrome coding also called matrix embedding is a steganography method which requires the sender and the receiver to agree in advance on a parity check matrix H. This syndrome coding uses linear codes as an ingredient. Khatirinejad and Lisonek [93] studied that by using this code a large amount of data can be hidden in an image. Hamming code can also be used in steganography to hide data in images [94], which provides better performance compared to LSB steganography. Wet paper coding first proposed by Fridrich et al. [95] is a technique which hides more amount of payload, the stego-image is imperceptible and the technique is robust.

Chang et al. [96] proposed a new data hiding scheme which uses wet paper coding mechanism in combination with fuzzy edge detector and an n-indicator. The n-indicator is to increase the robustness of the proposed system to guard against being detected. The fuzzy edge detector is to improve the payload. Filler et al. [97] proposed a steganography method for minimizing additive distortion. This method uses conventional codes with trellis quantizer. These codes are called as syndrome-trellis codes. These codes can improve the payload with same distortion or can reduce the distortion with same payload.

Li et al. [98] proposed a scheme called tree based parity check (TBPC) to reduce distortion on a cover image based on tree structure. The tree based parity check (TBPC) method can be formulated as a matrix method, but is more efficient than those based on linear codes. Because of its simplicity, the TBPC method provides very efficient embedding and extraction algorithm. A novel method called "majority vote strategy" has been proposed by Hou et al. [99] which provide least distortion in the stego-image and it is based on this TBPC.

Wang and Wang [100] proposed two steganography schemes based on point sampled geometry. Both the schemes employ a principal component analysis (PCA) to translate the points' coordinates to the fresh coordinate system, that resulting in a blind approach. In the first approach they established a list of intervals for each axis according to the secret key and then embedded a bit into each interval by changing the points' position. In the second scheme they located a list of macro embedding primitives (MEPs), and then embedded c bits ($2 \leq c \leq 6$) at each MEP, instead of a single bit as in the first approach.

IV. PROMISING DIRECTIONS IN SPATIAL DOMAIN

The first promising track is the combination of LSB and PVD methods. The LSB and PVD approach can be combined to get both high capacity and high security. LSB+PVD approaches have been proposed in [57, 58]. LSB+PVD approach is in its infancy stage, some more promising work can be done in this direction. The second important promising track is the reversible steganographic scheme [101-106] which involves embedding secret data into the host image to create the stego-image in such a way that it can produce a lossless recovery of the host image when the secret data is extracted.

The third direction is combination of encryption, compression and steganography [31]. In the literature there is a very few contribution in this direction. The fourth direction is the use of the color models YCbCr (yellow, chromatic-blue and chromatic-red) and HSV (hue, saturation and value). There are many color spaces like RGB, YCbCr, HSV etc. Mainly HSV and YCbCr are used in biometric applications. In RGB model a lot of papers are seen in literature, but in YCbCr, and HSV models a few papers are seen [107, 108, 109]. So some good amount of work can be done in this direction.

V. CONCLUSION

In this paper the different spatial domain image steganography techniques are classified into different categories. The promising directions of research are also pointed out. The LSB, RGB and PVD techniques are given more importance. In the LSB techniques, substitution can be done up to 4 least significant bits. The color images can be embedded with direct LSB substitution. But if they are handled differently the quality parameters can be improved. The LSB techniques give high capacity, where as PVD techniques give high security. The LSB and PVD techniques can be combined together to get both high capacity and high security. Every year new steganographic techniques are being proposed and new steganalysis techniques are also found. Steganography is very much useful to have a secret communication in the internet.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P.M. Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, vol. 90, pp.727-752, 2010.

[2] Kamaldeep, "Image steganography techniques in spatial domain, their parameters and analytical techniques: a review article" , IJAIR, vol.2, no.5, pp.85-92, 2013.

[3] B. Li, J. He, J. Huang, and Y.Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal processing, vol.2, no.2, pp.142-172, 2011.

[4] M. Hussain, and M. Hussain, "A survey of image steganography techniques", International Journal of Advanced Science and Technology, vol. 54, pp.113-123, 2013.

[5] N. Hamid, A. Yahya, R.B. Ahmad, D. Nejim, and L. Kannon, "Steganography in image files: a survey", Australian Journal of Basic and Applied Sciences, vol.7, no.1, pp.35-55, 2013.

[6] A. Bhatacharya, I. Banerjee, and G. Sanyal, "A survey of steganography and steganalysis techniques in image, text, audio and video cover carrier", Journal of Global Research in Computer Science, vol.2, no.4, pp.1-16, 2011.

[7] A. Martin, G. Sapiro, and G. Seroussi, "Is image steganography natural", IEEE Transactions on Image Processing, vol.14, no.12, pp.2040-2050, 2005.

[8] R. J. Anderson, and F. A. P. Petitcolas, "On the limits of steganography", IEEE Journal of Selected Areas in Communications, vol.16, no.4, pp.474-481, 1998.

[9] M. A. B. Younes, and A. Jantan, "A new steganography approach for image encryption exchange by using least significant bit insertion", International Journal of Computer Science and Network Security, vol.8, no.6, pp.247-254, 2008.

[10] H. B. Kekre, A. A. Athawale, and P. N. Halarnkar, "Increased capacity of information hiding in LSB's method for text in image", International Journal of Electrical, Computer and System Engineering, vol.2, no.4, pp.246-249, 2008.

[11] H. J. Zhang, and H. J. Tang, "A novel image steganography algorithm against statistical analysis", in Proceedings of Sixth International Conference on Machine Learning and Cybernetics, 2007, pp.3884-3888.

[12] H. Mathkour, G. M. R. Assassa, A. A. Muharib, and I. Kiady, "A novel approach for hiding messages in images", in Proceedings of International Conference on Signal Acquisition and Processing, 2009, pp.89-93.

[13] A. Mishra, A. Gupta, and D. K. Vishwakarma, "Proposal of a new steganography approach", in Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009, pp.175-178.

[14] M. Juneja, and P.S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption", in Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp.302-305.

[15] G. Swain, and S. K. Lenka, "LSB array based image steganography technique by exploring the four least significant bits", CCIS, vol. 270, part II, 2012, pp.479-488.

[16] H. Motameni, M. Norouzi, and A. Hatami, "Labeling method in steganography", World Academy of Science, Engineering and Technology, vol. 24, pp.349-354, 2007.

[17] G. Swain, D. R. Kumar, A. Pradhan, and S. K. Lenka, "A technique for secure communication using message dependent steganography", International Journal of Computer and Communication Technology, vol.2, no. 2- 4, pp.177-181, 2010.

[18] G. Swain, and S. K. Lenka, "Steganography using the twelve square substitution cipher and an index variable", in Proceedings of ICECT, 2011, vol.3, pp.84-88.

[19] G. Swain, and S. K. Lenka, "A robust image steganography technique using dynamic embedding with two least significant bits", Advanced Materials Research, vols. 403-408, pp.835-841, 2012.

[20] G. Swain, and S. K. Lenka, "A dynamic approach to image steganography using the three least significant bits and extended hill cipher", Advanced Materials Research, vols. 403-408 pp.842-849, 2012.

[21] G. Swain, and S. K. Lenka, "A technique for secret communication by using a new block cipher with dynamic steganography", International Journal of Security and Its Applications, vol.6, no.2, pp.1-12, 2012.

[22] A. P. S. Pharwaha, "Secure data communication using moderate bit substitution for data hiding with three layer security", IE(I) Journal-ET, vol.91, pp.45-50, 2010.

[23] J. He, S. Tang, and T. Wu, "An adaptive steganography based on depth-varying embedding", in Proceedings of 2008 Congress on Image and Signal Processing, 2008, pp.660-663.

[24] Y. K. Jain, and R. R. Ahirwal, "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, vol.4, no.1, pp.40-49, 2010.

[25] M. K. Meena, S. Kumar, and N. Gupta, "Image steganography tool using adaptive encoding approach to maximize image hiding capacity", International Journal of Soft Computing and Engineering, vol.1, no.2, pp.7-11, 2011.

[26] Y. K. Lee, G. Bell, S.Y. Huang, R.Z. Wang, and S.J. Shyu, "An advanced least-significant-bit embedding scheme for steganographic encoding", LNCS, vol.5414, 2009, pp.349-360.

[27] G. Swain, and S. K. Lenka, "A hybrid approach to steganography- embedding at darkest and brightest pixels", in Proceedings of International Conference on Communication and Computational Intelligence, 2010, pp.529-534.

[28] G. Swain, and S. K. Lenka, "Application of a large key cipher in image steganography by exploring the darkest and brightest pixels", International Journal of Computer Science and Communication, vol. 3, no.1, pp.49-53, 2012.

[29] D. C. Lou, and C. H. Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis", Information Sciences, vol.188, pp.346-358, 2012.

[30] C. K. Chan, and L. M. Chang, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol.37, pp.469-474, 2004.

[31] M. Bashardoust, G. B. Sulong, and P. Gerami, "Enhanced LSB image steganography method by using knight tour algorithm, vignere encryption and LZW compression", International Journal of Computer Science Issues, vol.10, no.2, pp.221-227, 2013.

[32] R. S. Gutta, Y. D. Chincholkar, and P. U. Lahane, "Steganography for two and three LSBs using extended substitution algorithm", ICTAT Journal on Communication Technology, vol.4, no.1, pp.685-690, 2013.

[33] A. Gangwar, and V. Srivastava, "Improved RGB-LSB steganography using secret key", International Journal of Computer Trends and Technology, vol.4, no.2, pp.85-89, 2013.

[34] A. R. S. Marcal, and P.R. Pereira, "A steganographic method for digital images robust to RS steganalysis", LNCS, vol.3656, 2005, pp.1192-1199.

[35] S. M. Douiri, M. B. O. Medeni, S. Elbernoussi, and E. M. Souidi, "A new steganographic method for gray scale image using graph coloring problem", Applied Mathematics & Information Sciences, vol.7, no.2, pp.521-527, 2013.

[36] A. Gutub, M. Ankeer, M. Abu-Ghalioun, A. Shaheen, and A. Alvi, "Pixel indicator high capacity technique for RGB image based steganography", in Proceedings of Fifth IEEE International Workshop on Signal Processing and its Applications, 2008, University of Sharjah, U.A.E.

[37] M. T. Parvez, and A. A. Gutub, "RGB intensity based variable-bits image steganography", in Proceedings of IEEE Asia-pacific Services Computing Conference, 2008, pp.1322-1327.

[38] A. Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A secure RGB image steganography based on randomization", in Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp.400-403.
[39] N. Tiwari, and M. Shandilya, "Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growth", International Journal of Security and Its Applications, vol.4, no.4, pp.53-62, 2010.
[40] G. Swain, and S. K. Lenka, "A better RGB channel based image steganography technique", CCIS, vol.270, part II, 2012, pp.470-478.
[41] G. Swain, and S. K. Lenka, "A novel approach to RGB channel based image steganography technique", International Arab Journal of e-Technology, vol.2, no.4, pp.181-186, 2012.
[42] M. Juneja, and P. S. Sandhu, "Implementation of improved steganographic technique for 24-bit bitmap images in communication", Journal of American Sciences, vol.5, no.2, pp.35-42, 2009.
[43] M. Kaur, S. Gupta, P. S. Sandhu, and J. Kaur, "A dynamic RGB intensity based steganography scheme", World Academy of Science, Engineering and Technology, vol.67, pp.833-836, 2010.
[44] A. A. Gutub, "Pixel indicator technique for RGB image steganography", Journal of Emerging Technologies in Web Intelligence, vol.2, no.1, pp.56-64, 2010.
[45] S. K. Ghosal, "A new pair wise bit based data hiding approach on 24 bit color image using steganographic technique", in Proceedings of International Conference IEMCON, 2011, pp.123-129.
[46] M. Juneja, and P.S. Sandhu, "An improved LSB based steganography technique for RGB color images", in Proceedings of Second International Conference on Latest Computational Technologies, 2013, pp.10-14.
[47] A. M. Abdalla, "Variable rate steganography using RGB stego-images", European Scientific Journal, vol.9, no.15, pp.62-67, 2013.
[48] M. Juneja, and P. S. Sandhu, "A new approach for information security using an improved steganography technique", J. Inf. Process Syst, vol.9, no.3, pp.405-424, 2013.
[49] D. C. Wu, and W. H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol.24, pp.1613-1626, 2003.
[50] X. Zhang, and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, vol.25, pp.331-339, 2004.
[51] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software, 2007, doi:10.1016/j.jss.2007.01.049.
[52] K. C. Chang, C.P. Chang, P. S. Huang, and T. M. Tu, "A novel image steganographic method using tri-way pixel-value differencing", Journal of Multimedia, vol.3, no.2, pp.37-44, 2008.
[53] C. C. Chang, and H. W. Tseng, "A steganographic method for digital images using side match", Pattern Recognition Letters, vol.25, pp.1431-1437, 2004.
[54] K. J. Kim, K. H. Jung., and K. Y. Yoo, "Image steganographic method with variable embedding length", in Proceedings of International Symposium on Ubiquitous Computing, 2008, pp.210-213.
[55] H. L. Zhang, G. Z. Geng, and C. Q. Xiong, "Image steganography using pixel-value differencing", in Proceedings of Second International Conference on Electronic Commerce and Security, 2009, pp.109-112.
[56] M. Hossain, S. A. Haque, and F. Sharmin, "Variable rate steganography in gray scale digital images using neighborhood pixel information", The International Arab Journal of Information Technology, vol.7, no.1, pp.34-38, 2010.
[57] H. C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Proceedings Vision, Image and Signal Processing, vol.152, no.5, pp.611-615, 2005.
[58] C. H. Yang, C.Y. Weng, S. J. Wang, and H. M. Sun, "Varied PVD+LSB evading programs to spatial domain in data embedding systems", The Journal of Systems and Software, vol.83, pp.1635-1643, 2010.
[59] X. Liao, Q. Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", J. Vis. Commun. Image.R., vol.22, pp.1-8, 2011.
[60] C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images", The Journal of Systems and Software, vol.84, pp.669-678, 2011.
[61] W. Hong, T. S. Chen, and C. W. Luo, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system", The Journal of Systems and Software, vol.85, pp.1166-1175, 2012.
[62] Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, and C.P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing", Information Sciences, vol.191, pp.214-225, 2012.
[63] A. Pradhan, D.S. Sharma, and G. Swain, "Variable rate steganography in digital images using two, three and four neighbor pixels", Indian Journal of Computer Science and Engineering, vol.3. no.3, pp.457-463, 2012.
[64] G. Swain, and S.K. Lenka, "Steganography using two sided, three sided, and four sided side match methods", CSI Transactions on ICT, vol.1, no.2, pp.127-133, 2013.
[65] H.W. Tseng, and H.S. Leng, "A steganographic method based on pixel–value differencing and the perfect square number", Journal of Applied Sciences, 2013, http://dx.doi.org/10.1155/2013/189706
[66] G. Swain, "Steganography in digital images using maximum difference of neighboring pixel values", International Journal of Security and Its Applications, vol.7, no.6, pp.285-294, 2013.
[67] G. Swain, and S.K. Lenka, "Pixel value differencing steganography using correlation of target pixel with neighboring pixels", unpublished.
[68] A. Ioannidou, S. T. Halkidis, and G. Stephanidis, "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, vol.39, pp.11517-11524, 2012
[69] S. Kaur, and S. Jindal, "Image steganography using hybrid edge detection and first component alteration technique", International Journal of Hybrid Information Technology, vol.6, no.5, pp.59-66, 2013.
[70] J. K. Mandal, and D. Das, "Color image steganography based on pixel value differencing in spatial domain", International Journal of Information Sciences and Techniques, vol.2, no.4, pp.83-93, 2012.
[71] R. Z. Wang, and Y. S. Chen, "High-payload image steganography using two-way block matching", IEEE Signal Processing Letters, vol.13, no.3, pp.161-164, 2006.
[72] P. M. Kumar, and D. Roopa, "An image steganography framework with improved tamper proofing", Asian Journal of Information Technology, vol.6, no.10, pp.1023-1029, 2007.
[73] M. A. F. Al-Husainy, "Image steganography by mapping pixels to letters", Journal of Computer Science, vol.5, no.1, pp.33-38, 2009.
[74] J. Fridrich, "A new steganographic method for palette based images", in Proceedings of IS&T PICS, 1999, pp.285-289.
[75] J. Fridrich, and J. Du, "Secure steganographic methods for palette images", LNCS, vol.1768, 2000, pp.47-60.
[76] M. Y. Wu, Y. K. Ho, and J. H. Lee, "An iterative method of palette-based image steganography", Pattern Recognition Letters, vol.25, pp.301-309, 2004.
[77] X. Wang, "A palette-based image steganographic method using color quantization", in Proceedings of IEEE International Conference on Image Processing, vol.2, 2005, pp.1090-1093.

[78] Z. R. Zhou, Z. C. Ji, Y. Z. Wang, and J. J. Lin, "A new algorithm of steganography based on palette image", in Proceedings of First IEEE Conference on Industrial Electronics and Applications, 2006, pp.1-4.
[79] X. Zhang, S. Wang, and Z. Zhou, "Multi-bit assignment steganography in palette images", IEEE Signal Processing Letters, vol.15, pp.553-556, 2008.
[80] S. M. Kim, Z. Cheng, and K. Y. Yoo, "A new steganography scheme based on index color image", in proceedings of Sixth International Conference on Information Technology: New Generation, 2009, pp.376-381.
[81] N. A. Saleh, H. N. Boghdady, S. I. Shaheen, and A. M. Darwish, "High capacity lossless data embedding technique for palette images based on histogram analysis", Digital Signal Processing, vol.20, pp.1629-1636, 2010.
[82] M. S. Shahreza, and S. S. Shahreza, "Collage steganography", in Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Sciences, 2006, pp.316-321.
[83] S. S. Shahreza, and M. S. Shahreza, "Improved collage steganography", in Proceedings of International Conference on Emerging Technologies, 2008, pp.223-227.
[84] K. Petrowski, M. Kharrazi, H.T. Sencar, and N. Memon, "Psteg: steganographic embedding through patching", in Proceedings of ICASSP, 2005, pp.II-537-540.
[85] J. R. Smith, and B. O. Comiskey, "Modulation and information hiding in images", LNCS, vol.1174, 1996.
[86] C. L. Tsai, K. C. Fan, and C. D. Chung, "Secure information by using digital data embedding and spread spectrum techniques", in Proceedings of IEEE 35th International Carnahan Conference on Security Technology, 2001, pp.156-162.
[87] L. M. Marvel, "Spread spectrum image steganography", IEEE Transactions on Image Processing, vol.8, no.8, pp.1075-1083, 1999.
[88] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image steganography", IEEE Transactions on Consumer Electronics, vol.50, no.2, pp.587-590, 2004.
[89] K. C. Widadi, P. H. Ainianta, and C. C. Wah, "Blind steganography using direct sequence/frequency hopping spread spectrum technique", in Proceedings of Fifth International Conference on Information, Communication and Signal Processing, pp.1125-1129, 2005.
[90] Y. H. Yu, C. C. Chang, and Y. C. Hu, "Hiding secret data in images via predicting coding", Pattern Recognition, vol.38, no.5, pp.691-705, 2005.
[91] G. Liu, Y. Dai, and Z. Wang, "Breaking predictive-coding- based steganography and modification for enhanced security", International Journal of Computer Science and Network Security, vol.6, no.3B, pp.144-149, 2006.
[92] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme", IEEE Signal Processing Letters, vol.14, no.11, pp.848-851, 2007.
[93] M. Khatirinejad, and P. Lisonek, "Linear codes for high payload steganography", Discrete Applied Mathematics, vol.157, no.5, pp.971-981, 2009.
[94] H. R. Pous, and J. Rifa, "Product perfect codes and steganography", Digital Signal Processing, vol.19, pp.764-769, 2009.
[95] J. Fridrich, M. Goljian, P. Lisonek, and D. Soukal, "Writing on wet paper", IEEE Transactions on Signal Processing, vol.53, pp.3923-3935, 2005.
[96] C. C. Chang, J. S. Lee, and T. H. N. Lee, "Hybrid wet paper coding mechanism for steganography employing n-indicator fuzzy edge detector", Digital Signal Processing, doi:10.1016/j.dsp.2009.11.005, 2009.
[97] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis code", IEEE Transactions on Information Forensics and Security, vol.6, no.3, pp.920-935, 2011.
[98] R. Y. M. Li, O. C. Au, K. K. Lai, C. K. Yuk, and S. Y. Lam, "Data hiding with tree based parity check", in proceedings of IEEE International Conference on Multimedia and Expo, 2007, pp.635-638.
[99] C. L. Hou, C. C. Lu, S. C. Tsai, and W. G. Tzeng, "An optimal data hiding scheme with tree-based parity check", IEEE Transactions on Image Processing, vol.20, no.3, pp.880-886, 2011.
[100] C. M. Wang, and P. C. Wang, "Steganography on point sampled geometry", computers & graphics, vol.30, pp.244-254, 2006.
[101] S. Weng, Y. Zhao, J. S. Pan, and R. Ni, "Reversible data hiding using companding technique and improved method", Circuits Systems and Signal Processing, vol.27, pp.229-245, 2008.
[102] H. C. Wu, H. C. Wang, C. S. Tsai, and C. M. Wang, "Reversible image steganographic scheme via predictive coding", Displays, vol.31, pp.35-43, 2010.
[103] W. Hong, and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", J. Vis. Commun. Image R., vol.22, no.2, pp.131-140, 2011.
[104] G. Feng, and L. Fan, "Reversible data hiding of high payload using local edge sensing prediction", The Journal of Systems and Software, vol.85, pp.392-399, 2012.
[105] Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery", International Journal of Electronics and Communications, vol.65, pp.814-826, 2011.
[106] C. T. Wang, and H. F. Yu, "A markov based reversible data hiding method based on histogram shifting", J. Vis. Commun. Image R., vol.23, pp.789-811, 2012.
[107] K. Sobottka, and I. Pitas, "Extraction of facial regions and features using color and shape information", in Proceedings of IEEE International Conference on Image Processing, 1996, pp.483-486.
[108] B. H. Lee, K. H. Kim, Y. Won, and J. Nam, "Efficient and automatic faces detection based on skin-tone and neural network model", in Proceedings of 15th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, LNCS, vol.2352, 2002.
[109] R. Hsu, M. A. Mottaleb, and A. Jain, "Face detection in color images", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.24, no.5, pp.696-706, 2002.
[110] G. Swain, and S. K. Lenka, "A novel steganography technique by mapping words with LSB array", International Journal of Signal and Imaging Systems Engineering, in press.