Comparison of LSB and PVD Steganography Methods

Khandagale P.M
PG student, SVERI COE
Pandharpur

Mukane S.M, PhD
Professor
SVERI COE, Pandharpur

Sadekar D.G
PG student, SVERI COE
Pandharpur

ABSTRACT
Now a day's as the internet is widely in-use hence the information is transferred with a single click. Information is transferred usingviz; images, videos, texts but the most popular format is the images. In order to transfer the information in a secure way, methods like cryptography, watermarking and Steganography have come into practice. But amongst all above methods Steganography is more reliable and apt because itsan art that involves communication of secret data with an appropriate carrier. Many Steganography methods have been design depending upon requirements such as data hiding capacity, robustness, image quality and each having its pros and cons. This paper aims to give thorough understanding and evolution of different existing 'Digital Image Steganography Techniques' of data hiding in spatial and transform domain. It also covers and integrates comparison of Least Significant bit (LSB) method as well as Pixel Value Difference Method (PVD).

Keywords
LSB, PVD.

1. INTRODUCTION
In the recent years, enormous research efforts have been invested in the development of digital image Steganography techniques. The major goal of Steganography is to enhance the communication security by inserting secret message into the digital image as well as modifying the nonessential pixels of the image. The image after the embedding of the secret message, so-called stego-image, is then sent to the receiver through a public channel. For the past decade, many Steganography techniques for still images have been presented. A simple and well known approach is, directly hiding secret data into the least-significant bit (LSB) of each pixel in an image[1]. This method embeds fixed-length secret bits into the least significant bits of pixels by directly replacing the LSBs of cover image with the secret message bits. Another approach is the 'Pixel Value Differencing' (PVD) method that computes the difference value between two neighboring pixels to determine how many secret bits should be embedded into a cover pixel[2].

2. STEGANOGRAPHY PRINCIPLE
2.1 The Encoder
The stego-system encoder is the heart of the Steganographic system. It makes it possible to embed a secret message within some cover medium. In the case of image Steganography, the encoder will read in a cover image c m:n (where m and n refer to the height and width dimensions of c), and will embed a message m by tweaking carefully selected values of the cover image ci. Exactly which ci values are tweaked depends on the specific embedding algorithm, and it is this decision process that makes each stego-system unique. The regions that are typically chosen to hide the message are often selected because they are believed to hold redundant data. That is to say that replacing the image data with the message data has no direct impact on the overall perceptibility of the image, therefore meaning the message is hard to detect at least with the naked eye.

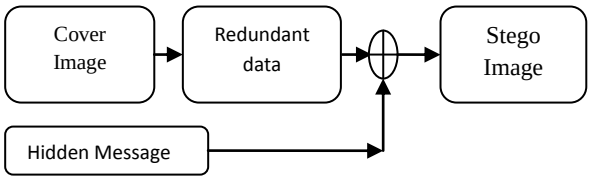

Figure 1.shows a graphical representation of the elements and processes typically associated with a stego-system encoder.

2.2 The Decoder
The stego-system decoder allows the receiver of the stegogramme to obtain an estimate of the secret message m. Thenreferring the output message as an estimate, each mi is derived from the locations of the stegogramme according to the shared key k. This means that it is not the exact same message that was an input into the encoder, so it can't be said 100% identical; indeed, some of the values may be slightly off. However, a good stego-system ensures that the estimate will be as close to the original message m as possible.

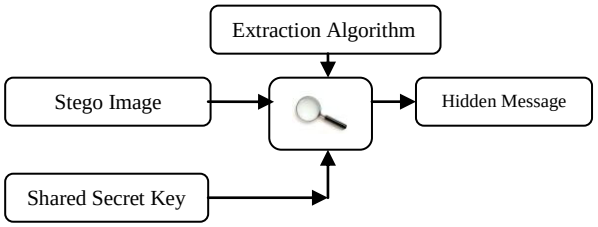

Figure 2. Shows graphical representation of Stego decoder system

3. STEGANOGRAPHY METHODS
There are various methods which can be classified such as spatial domain and transform domain. In this paper much emphasis is given on two methodsi.e,Least Significant Bit (LSB) and Pixel value difference (PVD) which as follows:

3.1 Least Significant Bit(LSB) Method
Now a day's LSB insertion has become rampant method to embed the information in a cover image [3]. The Lest Significant bit that is the 8th bit of some of the bytes inside an image is converted to a bit of the secrete message [1]. A bit of each red, green and blue color components are commonly used in a 24-bit image. As each color represents a byte hence each pixel can store three bits. For instance, an 800x600 pixel image can store a total amount of 1,440,000 bits or 180,000 bytes of the embedded data. To clarify the above fact let us focus on a grid of a three pixels of a 24-bit image, as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

As per the embedded message only three underlined bits were to changed but on the contrary the number was embedded into the first 8-byte of the grids. So from the average point of view only half of the bits in a image were to be modified to hide a secrete message using the optimum cover size [4]. Each primary color has 256 possible color intensities so while changing LSB of a pixel surely results in slight changes in the intensity of the various colors. Eventually the human eye is unable to notice these small changes and the message is successfully concealed. If cover image is well chosen one can also hide the message in the least as well as second to least significant bit and the difference created is invisible.

In the aforesaid citation, consecutive bytes of the image data – from the first byte to the end of the message are used to embed the information. As this method is very easy to trace [5]. Sharing a secret key that highlights only certain pixels to be changed is rather more secure system, for both, sender and receiver.

3.2 Pixel Value Difference (PVD) method

3.2.1 Embedding Stage

In the PVD method, the cover image is are to be 256 gray-valued ones [2]. A difference value d is computed from every non overlapping block of two consecutive pixels, say $p_i$and p_{i+1} of a given cover image in the embedding phase.The cover image is partitioned into two pixel blocks which runs through all the rows of each image in a zig zag format. Just assume that g_i and g_{i+1} are the gray values for p_i and p_{i+1} respectively.Then d is computed as a g_{i+1}-g_i which may be in the range from -255 to 255. A block with d close to 0 is considered to be an extremely smooth block. Whereas a block with d closed to -255 or 255 is considered as a sharply edged block. Only absolute values of d (0-255) are considered in this method and classifies them into a number of contiguous ranges such as R_k, where k=1,2,…,q. These ranges are assigned indices 1 though n. The lower and upper bound values of Rk are denoted by l_k and u_k, respectively. The width of Rk is u_k-l_{k+1}. In PVD method the width of each range is taken to be a power of 2, every bit in the bit stream should be embedded into the two pixel blocks of the cover image. Given a two pixel block B with gray value difference d belonging to kth range, then the number of bits, say n, which can be embedded in this block, is calculated by n=log(uk-lk+1) which is an integer. A sub stream S with n bits is selected from the secret message for embedding in B. A new difference d then is computed with equation 1.

$$d' = \begin{cases} lk + b & d \geq 0 \\ -(lk + b) & d < 0 \end{cases} \quad (1)$$

Where *b* is the value of the sub stream *S*. Because the value *b* is in the range [0, uk-lk], the value of *d'* is in the range from *lk*to *uk*. If we replace *d* with *d*', the resulting changes arepresumably unnoticeable to the observer. Then *b* can beembedded by performing an inverse calculation from *d'* toyield the new gray values (gi', gi+1') for the pixels in thecorresponding two-pixel block (pi, pi+1) of the stego-image.The inverse calculation for computing (gi', gi+1') from theoriginal gray values (gi, gi+1) of the pixel pair is based on a function given in equation 2.

$$(g_i', g_{i+1}') = \begin{cases} \left(gi - \left(\frac{m}{2}\right),\ g_{i+1}'\left(\frac{m}{2}\right)\right) if\ d\ is\ even \\ \left(gi - \left(\frac{m}{2}\right),\ g_{i+1}'\left(\frac{m}{2}\right)\right) if\ d\ is\ odd \end{cases} \quad (2)$$

Where *m* is *d'-d* .the embedding is only done for pixels which their new values would fall in the range of [0,255].

3.2.2 Retrieving Stage

The basic range table is mandatory in the extracting phase, and is used for stego image partitioning adopting same method utilized for cover image. After calculating the difference value d*(pi,pi+1) for each block of two successive pixels find the max Riof the d* same as in the concealed phase. Hence b0 is obtained after subtracting li from d*(pi,pi+1). The decimal number containing secrete data is represented by b0 value. Now transform b0 into binary with t bits, where t=[log2wi]. The t bits can stand for the original secret data for hiding [6].

4. RESULTS AND DISCUSSION

In this section after the analytical study of LSB and PVD method with some performance measures following is the inference:

4.1 Performance Measures

Steganography methods can be analyzed by using various parameters such as Robustness, data hiding capacity, image quality, PSNR, MSE.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}(I1(m,n) - I2(m,n))^2}{M * N}$$

$$PSNR = 10 log_{10}\left[\frac{R^2}{MSE}\right]$$

4.2 Result of LSB method

Following table shows performance of LSB method.

Table 1. Result of LSB method

	LSB Encoding		LSB Decoding	
	PSNR	MSE	PSNR	MSE
Lenna	44.17	2.48	44.16	2.47
Cameraman	44.15	2.497	44.14	2.49
Babun	44.18	2.499	44.17	2.48

4.3 Result of PVD method

Following table shows performance of PVD method

Table 2. Result of PVD method

	PVD Encoding		PVD Decoding	
	PSNR	MSE	PSNR	MSE
Lenna	48.69	0.87	46.10	1.59
Cameraman	48.31	0.9	46.30	1.44
Babun	48.52	0.88	47.01	1.48

5. COMPARISON OF LSB AND PVD

In an LSB method very less number of bits are stored as only a least bit of each pixel is changed. LSB can be performed up to four bits but result may degrade. As compared to LSB method more number of bits is stored in cover image with less distortion. So, more number of message bits is stored in PVD method than LSB method. Image quality after decoding is better in LSB than PVD. A large number of data bits are stored in PVD method without compromising quality of the image while a large number of data can be stored in LSB method but image quality degrades.

6. CONCLUSION

Depending upon needthe of the user Steganography method is selected. While selecting the method, performance-parameters should be considered. PVD method is having capacity to hide more data bits than LSB method. The LSB method is easily detectable and can be retrieved smoothly as compared to PVD. While embedding more data bits, the image quality may degrade.

So, to conclude PVD method is giving better result than LSB as it hides more data bits, with good image quality and is not be easily detectable and hence communication becomes more secure.

7. REFERENCES

[1] C. K. Chan and L. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, 2004, pp. 469–474.

[2] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[3] Johnson, N.F. &Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*,February 1998.

[4] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf.

[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,47:10, October 2004.

[6] H.B.Kekre, ArchanaAthawale, and PallaviN.Halarnkar, "Increased Capacity of Information Hiding in LSB's Method for Text and Image", International Journal of Electrical and Electronics Engineering 2:4 2008.