Advanced Research in Electrical and Electronic Engineering
p-ISSN: 2349-5804; e-ISSN: 2349-5812 Volume 4, Issue 4, July-September, 2017, pp. 183-188
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

A Comparative Study on Text Steganography in Spatial Domain

Deeksha Chalotra

Department of ECE, SMVDU, Katra, India

Abstract—*Digital images primarily consist of a rectangular grid of evenly spaced pixels. Image steganography extensively utilizes well detailed Least Significant Bit (LSB) based techniques. The steganographic process is well integrated and often encounters resampling which attempts to alter pixel characteristics qualitatively and quantitatively. An interesting alternative sustains in the form of Distortion technique to serve the steganographic needs. However, the effectiveness of a scheme under diverse conditions is an aspect yet to be comprehensively explored. The work predominantly focuses on to the need to address the accountability of existing steganography techniques for varying circumstances. Text steganography is adopted for the selected parametric studies in spatial domain involving both techniques. Schemes were extensively tested in under varying conditions and their implications noted to explore the role of key controlling parameters. Aiming enhanced quality and security, a new scheme is proposed based on the adjudging interpolation formula to stretch lossless compression regime under varying disarrays.*

1. INTRODUCTION

Steganography has uprooted to one of the important part of human society. The essence comprises hiding vital information within innocuous canvas carriers in ways that the hidden message is undetectable. The very need covers wide range of practical, engineering and scientific applications. The cover object can be a text, image, audio, video file processed by maintaining the appearance of the resulted object exactly same as the original (figure 1). The main goal of steganography is to hide the fact that the message is present in the transmission medium. The interest in this class of problems is specifically driven by the need to have better understanding of security, transmission and quality. Of various modes, Image Steganography is very popular because of frequency of digital image transmission over the cyberspace.

Image Steganography use redundancy of digital image to hide the secret data. It may be divided into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain, the secret messages are embedded in the image pixels directly. Least Significant Bit (LSB) substitution uses fixed LSBs in each pixel to embed secret message. However, it is easy to reveal a stego-image produced by the LSB insertion method.

Next, is the Distortion technique where some pixel property of cover image is changed according to secret message and then deflection of distorted from original image contains secret information. In the frequency-domain, the secret image is first transformed to frequency-domain, and then the messages are embedded. The secret information is embedded on the significant frequency values while higher frequency part is omitted. Transformations are applied to the image then data is to be hidden by changing the values of the transformation coefficients.

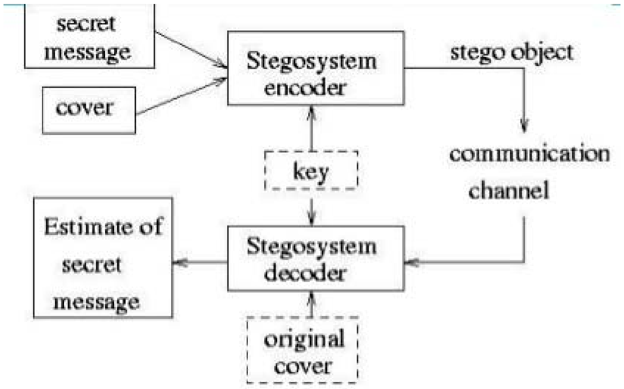


Figure 1: Schematic of steganographic process.

Following the classical work of Duda and Hart (1973) on pattern classification and scene analysis, over the last four decades research works have contributed significantly to the improvement in the understanding of the steganography. The contributions (numerically, analytically, experimentally) have been reported in several reviews like Ziv and Lempel (1977), Simmons (1983), Moerland (Steganalysis), Welch (1984), Kafri and Keren (1987), Zollner et al., (1998), Burges (1998), Westfield and Pfitzmann (1999) and till the end of the century.

In the last decade, the research works around the world have contributed significantly in development of image steganography as a magnificent mode of data hiding. Kharrazi et al., (2004) effectively reviewed the progress of image steganography with a number of embedding algorithms starting with the LSB technique and concluded that given an image, universal steganalysis techniques seem to be the real solution since they should be able to detect stego images even when a new embedding technique is being employed. Li et al., (2011) worked on developing advanced trends of steganography like adaptively selecting the embedding locations. They advocated the fact that edges and irregular texture areas may be hard to build a statistical model so, selecting locations adaptively for embedding is still a promising solution in steganography reducing embedding distortion and increasing embedding efficiency. Nithyanandam et al., (2011) proposed an image steganography algorithm which brings a better PSNR and MSE. The proposed technique was not robust against any geometrical distortion such as rotation, translation, scaling, cropping etc., induced on the stego image. The embedding capacity of the cover image was noted to be increased. Mali et al., (2012) presented a robust and secured method of embedding high volume of text information in digital cover-images without incurring any perceptual distortion. Image Adaptive Energy Thresholding (AET) was used while selecting the embedding locations in frequency domain. Perceptual quality of images after data hiding was tested using Peak Signal to Noise Ratio (PSNR) whereas statistical variations in selected Image Quality Measures (IQMs) were observed with respect to steganalysis. The proposed algorithm takes care of attacks like image tempering, compression, resizing and the security level of the system is enhanced with increased redundancy increasing robustness but reduced payload. Sharma and Kumar (2013) projected a new steganographic algorithm for hiding text files in images. The work utilized an underlying compression algorithm with maximum compression ratio of 8 bits/ pixel. Results showed no noticeable changes in stego images however worked efficiently only for .bmp images. Reddy and Naik (2013) explored the hiding of text messages into a digital image in spatial domain. In their approach, in each pixel two bits of message part was embedded in such a way that the fourth bit place, second bit plane and also the least significant bits are allowed to modify in order to achieve the embedding process. The proposed model was shown experimentally more robust and useful when compared with LSB-Matching. Sathisha et al., (2015) adopted the concept of replacing mantissa part of cover image by the generated mantissa part of payload for higher capacity and security. The Lifting Wavelet Transform (LWT) was applied on both cover image and payload. The mantissa values of Vertical band (CV), Horizontal band (CH) and Diagonal band (CD) of cover image were removed to convert into real values. The modified odd and even column vector pairs are added element by element to form one resultant vector. It was observed that the performance of the proposed algorithm is better compared to the existing algorithms. However, steganography is not easy as with knowledge of the existing algorithm/methods. The major challenges noted are viz., security, payload size, robustness. There is no technique or algorithm of steganography which provide all the three properties at high level. Almost in most of cases, there is a trade-off between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level. It is unpredictable to attain high robustness to signal modifications and high insertion capacity at the same time. Embedding information in spatial domain may be subjected to the losses if the image undergoes any image processing technique like compression, cropping etc. To address this problem, the present work considers a simple case of hiding text in images with implementation of two distinct techniques in spatial domain and attempts to assess them in terms of key controlling parameters viz., embedding capacity, quality of produced stego-image and robustness to attacks. The difficulty increases with the size of the message and the desired robustness of the scheme. This flaw demands a systematic study is needed to understand mechanisms controlling the encoding and decryption under diverse situations to get better insight for further betterment.

2. STEGANOGRAPHIC TECHNIQUES AND SOLUTION METHODOLOGY

Algorithms based on respective techniques were upraised for the present study. The cases with conventional LSB substitution were further extended to other bits and compared the same with distortion technique.

LSB Substitution: In this technique, the hidden data is inserted into the least significant bits of the pixel information. Increase or decrease of value by changing the least significant bit doesn’t change the appearance of the image, such that the resulted stego-image looks exactly same as the cover image. A more sophisticated approach pseudorandom number generator is used to spread the secret message over the cover in a rather random manner. If both communication partners share a stego-key k usable as a seed for a random number generator, they can create a random sequence k_1,…..,k_1(m) and use the elements with indices $J_1 = k_1$, Ji = ji-1 + ki, ≥ 2 for information transfer. Since the receiver has access to the seed k and knowledge of the pseudorandom number generator, he can reconstruct k_i and therefore the entire sequence of element indices j_i. If the message size increases, collisions must be considered. To overcome the problem of collisions, cover bits are tracked of all which have already been used for communication in a set B. If during the embedding process one specific cover-element has not been used prior, its index is added to B and continue to embed. If, however, the index of the cover-element is already contained in B, the element is discarded and another cover element pseudo randomly chosen. At the receiver side, similar technique is followed.

When the LSB of cover medium sample value is equal to the message bit, no change is made. In this work LSB with pseudo random generator is implemented. Matlab inbuilt pseudo-random number generator is used for this purpose and seed to this is taken as key of steganography. First, an array of random numbers, with the length equal to secret bit stream, is generated using key. Then with the help of this array, different pixel positions are calculated. Now secret bits are embedded to LSB of these pixels. On the receiver side, first the pixel positions are calculated in the same way with the use of the same key. Then secret bit-stream is formed by the LSBs of these pixels.

Distortion Technique: Require the knowledge of the original cover in the decoding process. A sequence of modifications is applied to a cover to get a stego-image in such a way that it corresponds to a specific secret message for embedding. Receiver measures the differences with the original cover to reconstruct the sequence of modifications applied by sender, which corresponds to the secret message. The sender first chooses l(m) different cover-pixels he wants to use for information transfer. To encode a 0 in one pixel, the pixel is left unchanged; to encode a 1, a random value x is added to the pixel's color. Although, this approach is like a substitution system, there is one significant difference: the LSB of the selected color values do not necessarily equal secret message bits. No cover modifications are needed when coding a 0. Furthermore, x is chosen in a way that better preserves the cover's statistical properties. The receiver would compare all l(m) selected pixels of the stego-object with the corresponding pixels of the original cover. If the ith pixel differs, the ith message bit is a 1, otherwise a 0. In this work, the value of x is taken as 1 so that minimum deflection from cover image will produced. A middle level of pixel value is defined, such that if the pixel value is greater than this value than x is added to pixel value otherwise x is subtracted from the pixel value. On the receiver side, first the difference between the pixel values of cover image and stego-image is calculated. Then pixel positions are calculated in the same way with the use of the key and pseudo random number generator. If the difference at a location is 0 then secret bit is taken as 0 otherwise it is taken as 1.

MATLAB is used as simulator to implement the techniques of steganography. MATLAB provides highly computing environment and advanced in-built function for image processing. The parameters under which the performance of the Steganography Techniques are as follows: -

1. **Embedding Capacity:** Maximum size of the secret data that can be embed in cover image without deteriorating the integrity of the cover image. Represented in bytes or Bit per Pixel (bpp).
2. **Mean Square Error (MSE):** Square of error between cover image and stego-image. The distortion in the image is measured using MSE.

$$MSE = \left[\frac{1}{M*N}\right]^2 \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X'_{ij})^2 \qquad ……(1)$$

Where,

X_{ij} = Intensity of the pixel in cover image

X'_{ij} = Intensity of the pixel in stego image

M*N = Size of an Image.

3. **Peak Signal Noise Ratio (PSNR):** Ratio of peak square value of pixels by MSE. It is expressed in decibel. It measures the statistical difference between the cover and stego-image.

$$PSNR = 10log_{10}\frac{255^2}{MSE}\ db \qquad …….(2)$$

Higher the PSNR value, the better is noise image constructed to match actual.

3. RESULTS

A comparative study was carried out to study the effectiveness of most widely used steganographic techniques for hiding secret text in images. The objective held is to fundamentally understand the characteristic steganography issues and key controlling parameters. The work was carried out in two phase viz., analysis of existing algorithms with related modifications and effect of controlling variable viz. resizing, message file size, cover images and interpolation schemes. The two techniques are systematically compared with the operations on same base cover image and same set of variables to understand their characteristic behavior under diverse conditions. Prior to the main study, the predictions of the upraised algorithm were validated with the conventional steganographic theories.

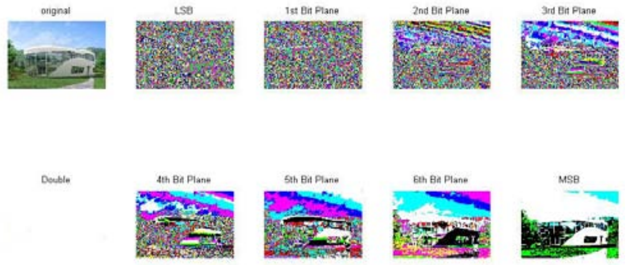


Figure 2. Pictorial view of the 8-bit planes of the reference image.

Figure 2 shows the base image with specification (Jpeg, 436X301, 102KB) an 8-bit image branched into 8 formation planes to note contribution of each plane. As we can note, the contribution of least significant bit plane is minimal which validates the calculations. Furthermore, an experiment was performed by hiding same text message in different bit planes (please see table 1). One can note that, the utilization of pixels is minimal in lease significant bit plane which confirms the conventional LSB substitution.

Table 1. Pixel utilization with varying bit planes.

Bit plane	Pixels utilization
LSB	220
1	440
2	880
3	1760

4	3520
5	7040
6	14080
MSB	28160

The predictions of the upraised algorithm conform well and are expected to give good physical insight into steganography science in spatial domain and related issues with existing techniques. First, we look at the effect of interpolation schemes on text steganography. A secret message file (59 Bytes) was chosen and hidden in bit planes. Basic interpolation schemes were considered viz., nearest neighbor, bilinear, Bicubic. Figure 3 shows effect of interpolation schemes on the text steganography performance with varying bit substitution. Experiments show that the PSNR value follows a non-monotonic trend when text is hidden in different bit planes.

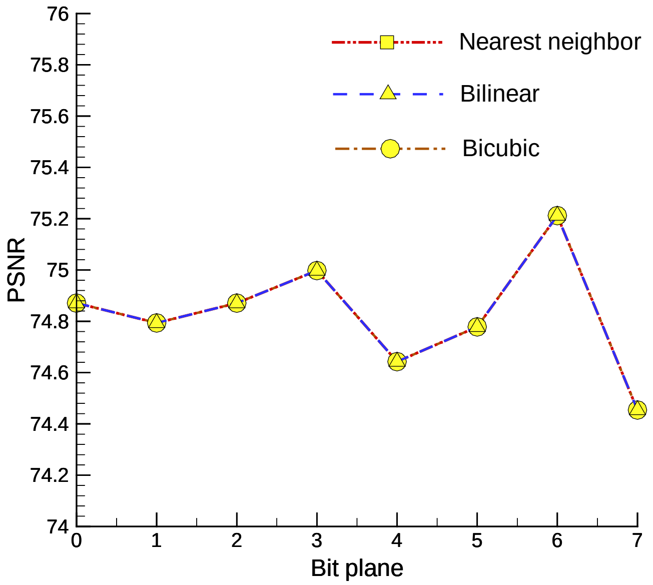
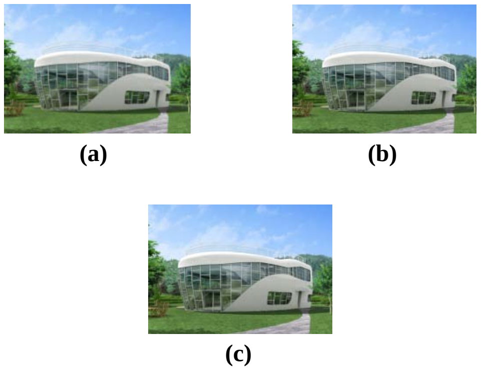


Figure 3. Effect of varying interpolation schemes on text bit extraction text steganography.

It is interesting to note that the PSNR values for different schemes do not change for hiding the selected text in different planes. Interestingly, the maximum value of PSNR coming at 6th plane. Low value of PSNR at MSB indicates the proximity of result. As per conventional theories, it may not be always suitable to use LSB for replacement, even other bits can be useful. To understand the reason for this trend, next we look at the corresponding images. Figure 4 shows the corresponding reference images with text hidden. It can be noted that, the interpolation schemes do not cause significant change in terms of distortion.


(a) (b)

(c)

Figure 4: Pictorial view of embedded image with text hidden at LSB (a) Nearest neighbor (b) Bilinear (c) Bicubic.

Next, the effect of resized cover image utilization in hiding text is compared with both techniques. Figure 5 shows the variation of PSNR when base text file is hidden at different planes with resized cover images. The cover image is resampled both ways viz., up-sampled till **175%** and down-sampled till **25%**. It is important to note that, **100%** represents the original cover image. Looking at the plot, one can note that the PSNR values shows perpetual trend. For a cover image size, the PSNR values in varying bit planes do not change significantly. However, the resizing of cover image is an important parameter in steganography. The up-sampled images show increased PSNR values and down-sampled images depicts reduced PSNR values. It is important to note that, the text was successfully retrieved in all the cases.

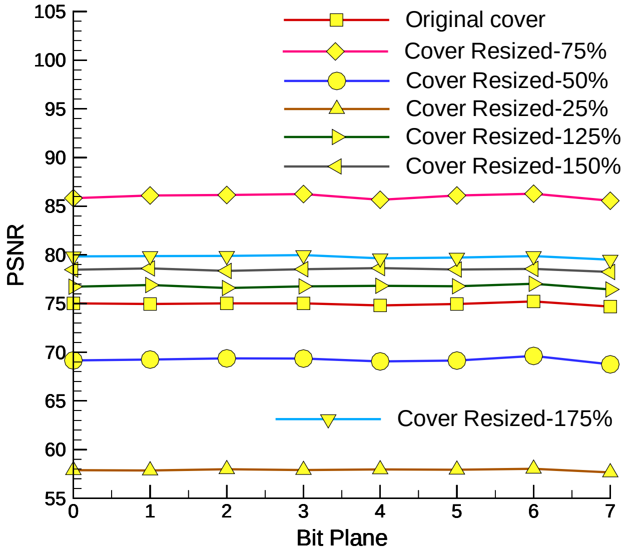


Figure 5. Variation of PSNR of resampled cover images in bit substitution technique.

The results indicate the Upsampling do not affect the text steganography severely however, downsampling may result in distortion. The maximum values of PSNR is obtained with cover image down-sampled **75%**. This offers a critical limit up to which the downsampling can be convenient.

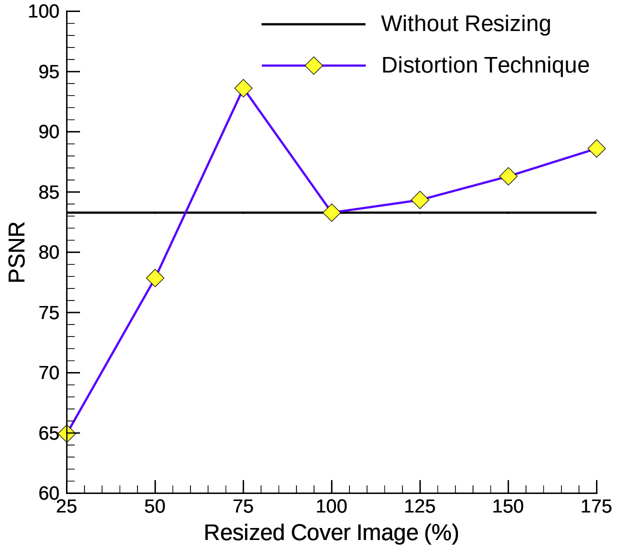


Figure 6. PSNR variation of resampled cover images using distortion technique.

Figure 6 shows the same results with distortion technique. It was thoroughly observed that, the PSNR values were higher for all the resampled cases. Like bit substitution, the maximum values occur at **75%** resized cover image but with higher PSNR value. It indicates that, while considering resizing attacks, it is better to shift to distortion technique for efficient text steganography. Another important parameter is embedding capacity. Figure 7 shows the PSNR variation for cover images with varying message file size hidden at different bit planes.

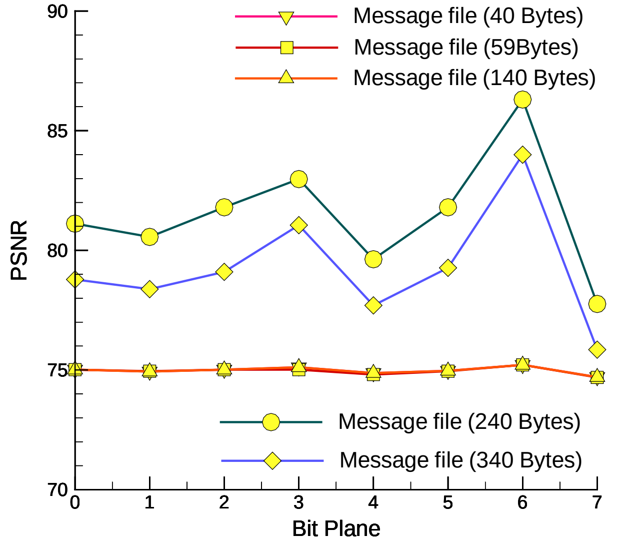


Figure 7. Variation of PSNR of cover images with hidden message file size in bit substitution.

Looking at the plot, one can note that the PSNR value do not change significantly. As the message file size increases, hiding text at different planes shows varying PSNR values. It is interesting to note that, heavier message files show higher PSNR values as compared to lower one. However, beyond a critical limit the PSNR values starts falling. The bit replacement algorithm predicts maximum PSNR at 6th plane which dictates pseudorandom norms. Figure 8 compares the results of message file size variation with distortion technique. It is interesting to note that, as the file size increases, the PSNR values with distortion technique reduces. In the present study, till a file size of 102 KB the distortion technique predicts PSNR higher than bit replacement. However, as the file size increases, the PSNR values with distortion technique reduces than Bit replacement. This indicates that for higher embedding capacity, the bit replacement performs better with output stego image approximately close to actual one.

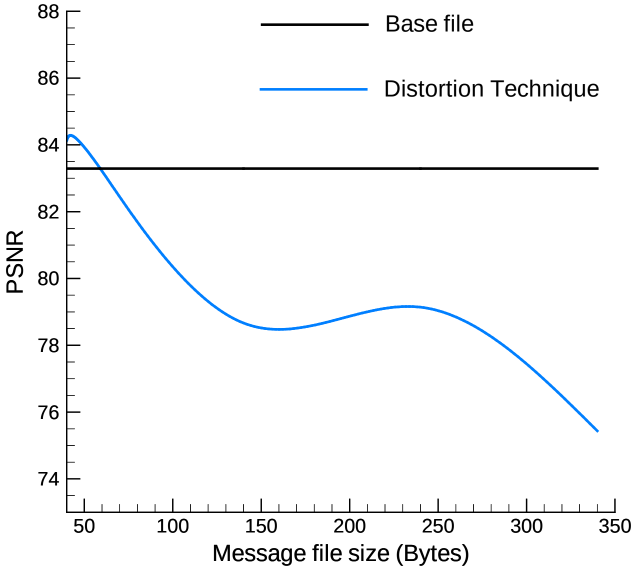


Figure 8. PSNR variation of hidden message file size using distortion technique.

Based on the present study, we noted that the spatial domain techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications. The spatial domain techniques provide high PSNR, high perceptual quality and high embedding capacity but these not provide robustness. Results indicates that the Bit replacement technique in spatial domain offers less chance for degradation of the original image. More information can be stored in cover image i.e. more hiding capacity. Foremost it is simple and less complex. However, it is less robust and the hidden data can be lost with image manipulation. Hidden data can be easily detected by simple attacks. It would require high transmission rate due to large size of stego image. Whereas, the distortion technique would result in less degradation of cover image than the conventional LSB and offers more embedding capacity except for heavy files. However, in many applications, the receiver must have access to the original covers and it is not safe as access to original cover detect the can lead to cover modifications and evidence for a secret communication.

4. CONCLUSIONS

A coding experimental exploration was carried out to compare the spatial domain text steganography using images. Recent advances and available algorithms were deeply analyzed to enhance understanding. Bit replacement and distortion techniques were thoroughly investigated and compared based on key controlling parameters. Appreciable development and modifications are carried out however, there are issues yet to be comprehensively addressed. Based on results obtained following conclusions may be drawn from this study: Hiding of secret text and hiding the images may lead to wavering performance of available techniques in diverse conditions. Interpolation schemes do not significantly affect significant bit replacement and performance. Distortion techniques is an interesting alternative within a critical limit. Resized cover images drastically affect the performance of bit replacement. However, up-sampled cover images are not severely noised. Within a critical size limit of text file, distortion technique performs better however, after that the bit replacement incurs high performance and stability. Both the techniques offer advantages over other however, a complete solution to generalized attack proof text steganography with a particular scheme looks redundant.

Based on the results, for future an option to be tested can be a hybrid scheme which is amalgation of both the techniques in such a way to maximize advantages of each techniques while minimizing the disadvantages for enhanced security, better transmission and capacity.

REFERENCES

[1] Duda and P. Hart, “Pattern classification and scene analysis,” John Wiley and Sons., 1973.

[2] Jacob Ziv, Abraham Lempel: A Universal Algorithm for Sequential Data Compression. IEEE Transactions on Information Theory, May 1977.

[3] G. Simmons, “The prisoners problem and the subliminal channel,” CRYPTO, pp. 51–67, 1983.

[4] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf.

[5] Terry Welch: A Technique for High-Performance Data Compression. IEEE Computer, June 1984.

[6] O. Kafri and E. Keren, Encryption of pictures and shapes by random grids, Optics Letters, vol. 12, no. 6, June 1987, pp. 377-379.

[7] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, “Modeling the security of steganographic systems,” 2nd Information Hiding Workshop, pp. 345–355, April 1998.

[8] C. Burges, “A tutorial on support vector machines for pattern recognition,” Data Mining and Knowledge Discovery., pp. 2:121–167, 1998.

[9] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” 3rd International Workshop on Information Hiding., 1999.

[10] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, “Image Steganography: Concepts and Practice” WSPC/Lecture Notes Series, 2004.

[11] Bin Li, Junhui He, Jiwu Huang and Yun Qing Shi, “A Survey on Image Steganography and Steganalysis” Journal of Information Hiding and Multimedia Signal processing, Volume 2, Number 2, and April 2011.

[12] P. Nithyanandam, T. Ravichandran, N. M. Santron & E. Priyadarshini, “A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding” International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (5): 2011.

[13] Mali S.N., Patil P.M and Jalnekar R.M, “Robust and secure image adaptive data hiding”, Digital signal processing 22(2012) 314-323.

[14] Sharma V and Kumar S, “A New Approach to Hide Text in Images Using Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[15] Reddy M.R.S and Naik S.J.S, “A Novel Method for Steganography in Spatial Domain”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.

[16] Sathisha N, Babu K.S, Raja K.B and Venugopal K.R, “Image Steganography Based on Mantissa Replacement using LWT”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4 Issue 2, February 2015.