VARIABLE LEAST SIGNIFICANT BITS GRAYSCALE IMAGE STEGNOGRAPHY

S. Khan, M. H. Yousaf [*], M. Wahid

University of Engineering and Technology Peshawar, Pakistan
*University of Engineering and Technology Taxila, Pakistan
Corresponding Author: haroon.yousaf@uettaxila.edu.pk,

ABSTRACT: This work presented a leading and more secured least significant bits stegnography technique having variable information hiding capacity and signal to noise ratio (SNR). Hiding capacity was enhanced by sacrificing signal to noise ratio (SNR) and vice versa. A give and take was made between the capacity and SNR depending on the situation it was used in. The presented stegnography technique offered a very large key size, to extract covered information, in addition to basic purpose of stegnography. The key size was directly related to cover image size and the number of bits variation used for information hiding. The key was kept secret and shared with the intended party only.

Keywords: Stegnography, Steganalysis, Image Processing, Key size, Cover media.

(Received 07-01-2014 Accepted 29-08-2015).

INTRODUCTION

Stegnography, literally means "covered writing", is a tool of hiding information in a suitable media i.e. Text, Image i.e. Grayscale, RGB etc., Audio and Video. It is a practical and operational technique of transmitting secret information via innocuous cover carriers making the existence of the hidden information undetectable. The covert information is hidden within the cover data set i.e. text, image, audio, video, etc (Johnson and Jajodia, 1998 and Rabah, 2004) by the stegnography so that its existence is indiscernible (Domitrescu *et al.*, 2002). This technique does not permit any opponent to even notice the presence of covert information (Moon and Kawitkar, 2007).

Greeks used the cover writing mechanism for the first time by covering information/message with wax. Invisible ink was used during World War II to achieve the goal of stegnography (Mehboob and Farooquie, 2008). The Germans used microdots in World War II (Swanson et. al., 1998). In the recent era stegnography uses highly efficient digital media i.e. Digital Images, Audio and Videos as cover (Cedric *et al.*, 2000). The stegnography technique presented in this work uses Grayscale digital images for information hiding. A great care needs to be taken in the assortment of the cover image (Tsai *et al.*, 2011).

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and Stegnography. All these applications of information hiding are quite diverse. In watermarking applications, the message contains information such as owner identification and a digital time stamp, which is usually applied for copyright protection. This adds to copyright information and makes it possible to trace any unauthorized use of the data set (Swanson *et. al.*, 1998).

Many techniques are used to implement stegnography both in spatial domain or transform domain. Discrete Cosine Transform (DCT) is used and data is hidden by exploiting the coefficient of DCT of the cover image. In this technique Image data is divided into square blocks, for example, 8×8 pixels, which are transformed to DCT coefficients. A DCT coefficient matrix $\left[d_{i,j}\right]$ that corresponds to a block of pixel $\left[b_{i,j}\right]$ is calculated. Secret information is embedded by rewriting DCT coefficients $\left[d_{i,j}\right]$following certain rules. If some appropriate rule is used for rewriting of DCT coefficients, the quality of the reconstructed image will be almost the same as that of the original one (Fridrich *et al.*, 2001). Wavelet Transform is also used for data hiding.

The most important technique implemented in spatial domain is 4 Least Significant (4LSB) stegnography. In 4LSB Stenography four least significant bits are used for substitution (Moon and Vasnik, 2007). The 4LSB method is implemented for color bitmap images i.e. 24 bit and 8 bit; where 256 color palette images and wave files as the carrier media.

It would appear that 4 LSB is a good method of stegnography with 50% information capacity, less distortion but not much secure. 4-LSB stegnography can be used to exchange secret messages over the public channel in a safe way, (Habes, 2006 and Morkel *et al.*, 2005) but the security can be increased further to develop more secure mechanism. A broad overview of data embedding and watermarking methods is available as reported by (Ogihara *et al.*, 1996). All algorithms employed have pros and cons and depend upon the environments used. It also depends upon the information to be embedded. Various techniques developed are compared.

MATERIALS AND METHODS

A. VLSB Stegnography: The 4LSB stegnography has a limited and fixed data hiding capacity of 50% i.e. to hide a message of size "N", a cover file of double size, i.e. "2xN", is needed. Moreover, the hidden data can easily be retrieved read the four least significant bits of each pixel of the cover image, if detected or suspected. To hide larger data in the cover file in a much secure way, a new technique called Variable Least Significant Bits (VLSB) stegnography was devised. In VLSB stegnography technique, the concept of different amount of data hiding was adopted, instead of fixed data. The cover image was divided in different sectors and different amount of data was hidden in the pixels of each sector, which was quite different from the fixed data hiding of 4LSB stegnography technique, to 4 bits in each pixel of the cover image.

Variable Least Significant Bits stegnography was a data hiding technique that used a variable number of bits of the cover file for data embedding. In the VLSB stegnography technique the cover image was divided in various sections/sectors, and "Bi", number of bits was used for data hiding in each pixel of a particular section. The number of bits "Bi", to be hidden changes from sector to sector. The division of cover image in various sectors was a very critical and important in implementation of VLSB stegnography. The hiding capacity and data security of VLSB stegnography, largely depends on the number of sectors and the number of bits used for data hiding in a sector. A well developed and well equipped algorithm was required to implement the VLSB stegnography. The algorithm should be capable of providing large hiding capacity with least possible distortion. The development of strong algorithm opened a new research area for researchers to devise new and better ways to implement VLSB stegnography.

Hiding capacity: The selection of numbers of sectors, assigning pixels to a specific sectors and amount of bits to be embedded in the pixels of that sector played a vital role in determining the hiding capacity and hiding security of VLSB stegnography. To get a hiding capacity of 50% or more, the number bits to be embedded in each pixel should not be less than four.

If the cover image consists rows "R", and columns "C", then the total number of pixels "N", was:

$$N = R \times C \qquad (1)$$

Let's the image was divided in a number of sectors "Ns", then the number of pixels "Ps", belonging to each sectors were:

$$Ps = \frac{N}{Ns} \qquad (2)$$

As each pixel value in a grayscale image was represented in 8 bits. The total hiding space available in the cover image in terms of bits was:

$$B_{total} = N \times 8 \qquad (3)$$

Similarly the hiding space available in each sector "Ps", was:

$$Bs_{total} = Ps \times 8 \qquad (4)$$

The Variable Least Significant Bits stegnography provided user freedom to hide any number of bits i.e. 1 to 8 bits of the message in each pixel of any sector of the cover image. The total data to be hidden in a section depends on the number of bits substituted in each pixel.

If a number of bits "Bi", were hidden in each pixel of a sector "Si", with a number of pixels "Psi", in it. Then the total amount of data embedded "Di", in sector "Si", was:

$$D_i = Psi \times Bi \qquad (5)$$

And consequently the total amount of data "D$_{total}$", embedded in the cover image was:

$$D_{total} = \sum_{i=1}^{Ns} D_i \qquad (6)$$

$$D_{total} = \sum_{i=1}^{Ns} (Psi \times Bi) \qquad (7)$$

And the total hiding capacity "C", of VLSB stegnography was:

$$C = \frac{D_{total}}{B_{total}} \times 100 \qquad (8)$$

$$C = \frac{\sum_{i=1}^{Ns} (Psi \times Bi)}{N \times 8} \times 100 \qquad (9)$$

Key size: The basic aim of stegnography was unseen hiding of information and most of the techniques proposed targeted the same feature. But, in such techniques the recovery of hidden information was very easy, if its presence was suspected or detected. The VLSB stegnography was secure in this regard and was much immune to steganalysis; because of its built-in encryption.

Consider a grayscale image having rows "R", and columns "C", with a total of "N", pixels was used as a cover for secret information. As in grayscale image each and every pixel's intensity was represented with 8 bits. Using VLSB stegnography, there was liberty of hiding any number bits, ranging from 1 to 8 bits, in each pixel. Let's a number of bits "Bi", were considered at a time for data hiding then 1≤Bi≤8, but to get a data hiding capacity of more than 50% the "Bi", should be greater than 3 (4≤Bi≤8). If the cover image was divided in "Ns", number of sectors, each with "Psi", number of pixels. There would be a total of "Cpi", possibilities for a pixel to be part of sector “Si”.

$$C_{pi} = C_1^{Ns} \qquad (10)$$

Each sector could be subjected to a “Bi” number of bits substitution for information hiding. So the total possible combinations “Csi”, in a sector “Si”, is represented as:

$$C_{Si} = C_{Bi}^8 \qquad (11)$$

So the total possible keys/combination “K”, for the whole cover image were:

$$K = C_{pi} \times C_{si} \qquad (12)$$

$$K = C_1^{Ns} \times C_{Bi}^8 \qquad (13)$$

If the number of sectors “Ns”, was so large that it became equal to the number of pixels “N”, then each sector would consist of the only one pixel. Then each sector would have “Csi”, different combinations for a single pixel so total possible keys/combinations “K”, for a cover image to hide data was given as below.

$$K = N \times C_{Bi}^8 \qquad (14)$$

Number of possible combinations “K”, was the number of different possibilities to hide data in a cover image. Larger the value of “K”, more difficult it would be for an unauthorized person to extract data from the innocent stego-image even if the existence of hidden information was detected. The unauthorized party would have to try “K”, different combinations to retrieve hidden data. The key size “K” was proportional to cover image size, larger the size of the cover media, it would be more difficult to break stegnpgraphy technique and retrieve the hidden information.

SNR and PSNR: The quality of the stego-image was measured quantitatively by calculating the signal to noise ratio (SNR) and the peak signal to noise ratio (PSNR). For stego image the SNR was calculated in Decibels (dB) as below.

$$SNR = 10 * \log_{10}\left[\frac{\sum_{i=1}^{R}\sum_{j=1}^{C}[Cov(i,j)]^2}{\sum_{i=1}^{R}\sum_{j=1}^{C}[Cov(i,j) - Stego(i,j)]^2}\right] \qquad (15)$$

And PSNR in Decibels (dB) was calculated as

$$PSNR = 10Log\left[\frac{255^2}{\frac{1}{r*c}\sum_{i=0}^{r-1}\sum_{j=0}^{c-1}(\mathrm{cov}(i,j) - (steg(i,j))^2}\right] \qquad (16)$$

A. Implementation of VLSB Grayscale Stegnography: To hide data/information in a more secure manner, Variable Least Significant Bits stegnography was implemented. It is a powerful and influential methodology due to its large key size. It could be implemented by using a proper and well-designed algorithm. The algorithm should provide large data hiding capacity with least possible distortion and should have a large key size. In this paper, VLSB stegnography was implemented by selecting a cover image and a message file (image). The message file was converted into a continuous bits stream. The cover file was processed for data hiding, selecting one pixel at a time. The “Bi”, bits of the message were selected and embedded in that pixel of the cover image by replacing “Bi”, number of least significant bits of the pixel, being processed, with “Bi”, bits of the message. The number of bits “Bi”, varied from pixel to pixel. The processed pixels, with hidden data created a new image i.e. Stego Image.

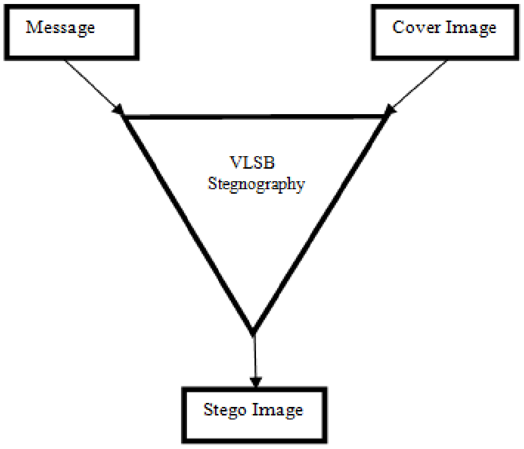


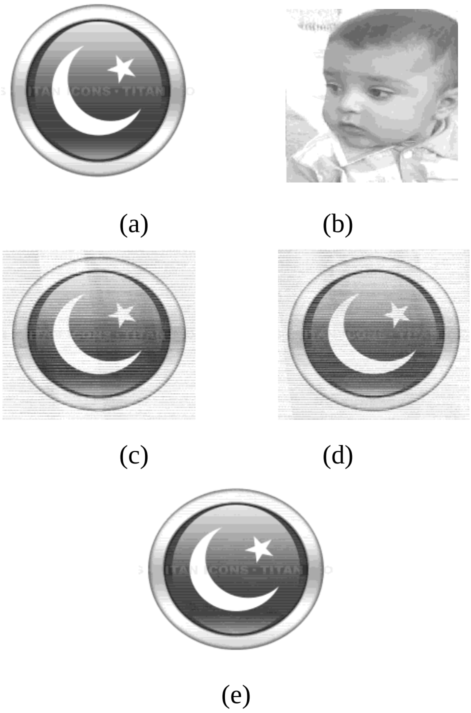
Fig-1: VLSB Stegnography

The VLSB stegnography could be implemented by selecting any number bits “Bi”, of message and hiding it in cover image pixels. The value of “Bi” was selected from a ranges from 1 to 8 bits, depending on the application, hiding capacity required and affordable distortion in the stego-image.

RESULTS AND DISCUSSIONS

The VLSB stegnography was implemented by embedding “Bi”, bits of message in the pixels of cover file. To get more fair results with less distortion all possible values of “Bi”, were utilized. The “Bi”, varied from 1 to 8 ($1 \le Bi \le 8$) and any value in this range was selected for data hiding. The VLSB stegnography was implemented for different combinations $j \le Bi \le 8$ of “Bi”, where $1 \le j \le 8$ showed the position of a specific bit. This combination of “j” hides data in the most significant bits of cover image pixels and results were obtained. The results obtained for 1≤j≤8 and 2≤j≤8, were of high quality and of significant hiding capacity of 56% and 63% respectively. The stego images for 1≤Bi≤8 and 2≤Bi≤8 are shown in Fig-2 (c and d).

But the results obtained for 3≤j≤8, 4≤j≤8, and higher values of "j", created significant distortion and stego images were shown in the paper. The statistical results obtained of capacity, SNR and PSNR for data hiding in most significant bits of cover image pixels are listed in the Table 1.


(a) (b)

(c) (d)

(e)

Fig-2: (a) cover image, (b) message, (c) Stego Image for (1≤Bi≤8), (d) Stego Image for (2≤Bi≤8), (e) Stego Image of 4LSB Stegnography, of VLSB Stegnography

4 Least Significant Bits (4LSB) stegnography was also applied on the same cover image and the same message. The stego image obtained is shown Fig-2 (e).

Table. 1. Hiding Capacity, SNR and PSNR verses different no. of Most Significant Bits

Bits	Hiding Capacity	SNR (dB)	PSNR (dB)
8MSBs	56.050%	-6.258	27.7195
7MSBs	48.50%	-5.8594	27.1159
6MSBs	43.650%	-5.0475	25.6393
5MSBs	37.500%	-4.253db	23.8465
4MSBs	31.250%	-3.312db	21.9560
3MSBs	24.975%	-3.2715db	19.9651
2MSBs	18.750%	-3.2575db	18.1189

It was apparent from Table 1, that as the range of "Bi" decreased and shift towards most significant bits the hiding capacity also decreased and consequently, the SNR and PSNR decreased. The decreasing trend of capacity, SNR and PSNR is shown in Figures 3, 4 and 5. On comparison with 4LSB stegnography, the hiding capacity and SNR of VLSB stegnography was higher than 4LSB stegnography, while the PSNR was smaller than that of 4LSB technique. The VLSB technique implemented by using "Bi", in the range from 1 to 8 was having the capacity of 56% and was most secure due to largest key size.

To decrease distortion in stego images, the capacity decreased; the least significant bits of cover image were used instead of the most significant bits. The number of bits "Bi", substituted was shifted towards least significant bits, i.e. the minimum value of "j", was kept fixed at 1, but the upper limit was changed from 1 to 8 (1≤Bi≤j and 1≤j≤8). For example j=2 and j=3 means that two and three least significant bits were used for data hiding, respectively. The VLSB stegnography was implemented to hide data using different number of least significant bits and stego images were obtained. The stego images obtained for j=8, 7, 6, 5, 4 and 3 is shown in Fig-6 (a, b, c, d and e) respectively. The stego image for j=2 and 1, were very fine and almost same as the cover image, they are not shown.

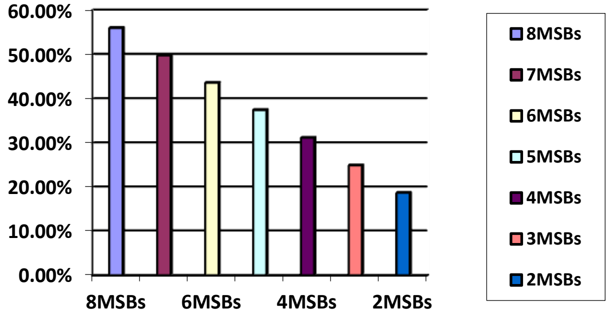


Fig-3: Capacity versus No. of MSBs

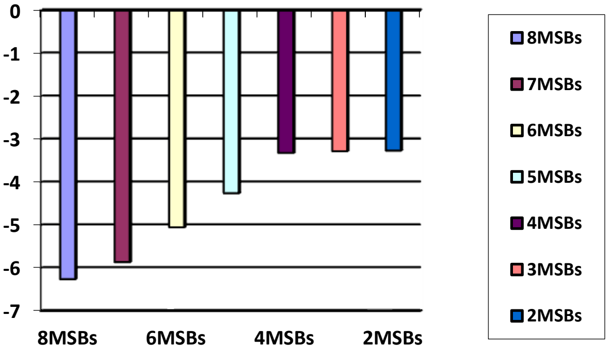


Fig-4: SNR versus No. of MSBs

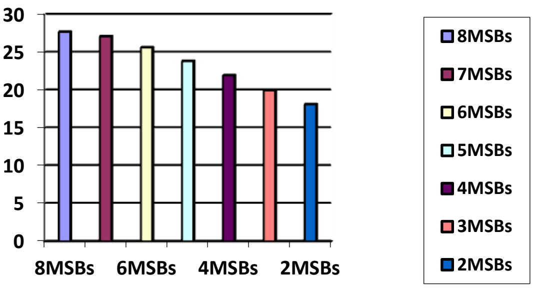
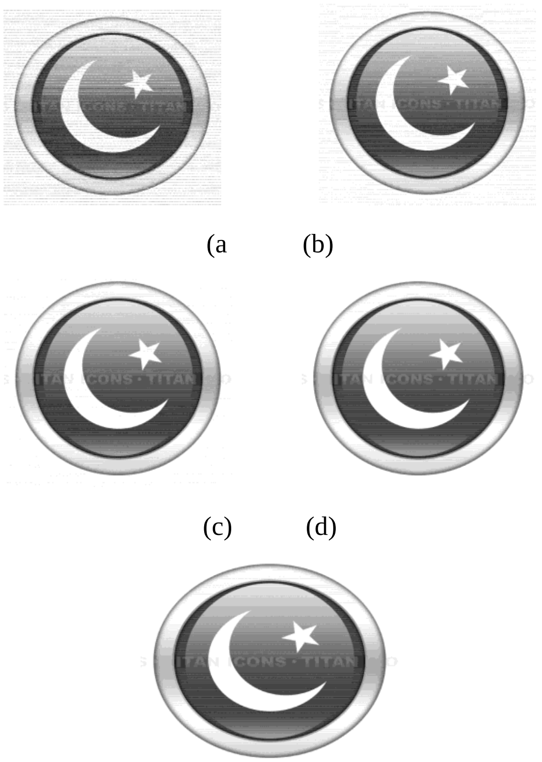


Fig-5: PSNR versus No. of MSBs



(a (b)

(c) (d)

(e)

Fig-6: (a) Stego Image for (1≤Bi≤7), (b) Stego Image for (1≤Bi≤6), (c) Stego Image for (1≤Bi≤5), (d) Stego Image for (1≤Bi≤4), (e) Stego Image for (1≤Bi≤3), of VLSB Stegnography

While comparing the statistics, given in Table 2, with the statistical results of 4LSB stegnography, it was quite apparent that by increasing the number of bits “Bi”, the capacity and SNR gradually increased and remained smaller than that of 4LSB technique for “j”, smaller or equal to 7. The stego images were very close to the original cover image and the key size was also significantly large which made the use of these combinations of “Bi”, very suitable for VLSB stegnography due to high quality and fair results of the stego image and strong key size. VLSB stegnography using all possible values of “Bi”, were much efficient, having a largest possible key size and good enough hiding capacity although a bit distortion was added to the stego image, but that was affordable due to increase in capacity and key size. In addition to these, few more findings were obtained as is evident from the Fig-7, Fig-8 and Fig-9. The capacity was directly proportional to the LSB’s used. To increase the storage capacity, more LSB were required. But higher capacity pay back in terms of SNR and PSNR, as SNR and PSNR was inversely proportional to the LSB’s. As far as the number of LSB’s used for data hiding were increased, the SNR and PSNR were decreased to a huge extent. That’s why a rational can be there to incorporate capacity as well as SNR and PSNR for well-balanced stegnography.

Table 2. Hiding Capacity, SNR and PSNR verses different no. of LSBs

Sr. No	Bi	Hiding Capacity	SNR (dB)	PSNR (dB)
1	8LSBs	56.050%	-6.258	27.7195
2	7LSBs	49.850%	2.8008	31.7556
3	6LSBs	43.650%	8.8042	36.2005
4	5LSBs	37.500%	11.5100	41.9901
5	4LSBs	31.250%	16.6802	48.0859
6	3LSBs	24.975%	21.1072	51.7248
7	2LSBs	18.750%	26.1552	56.5390
8	1LSBs	12.500%	30.563	61.1257

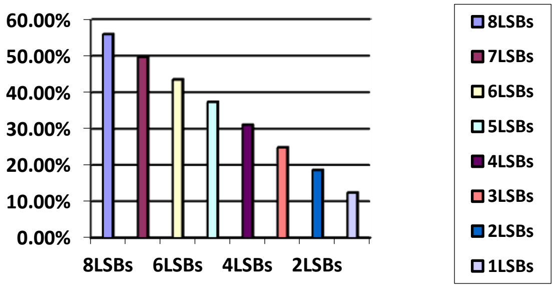


Fig-7: Capacity verses No. of LSBs

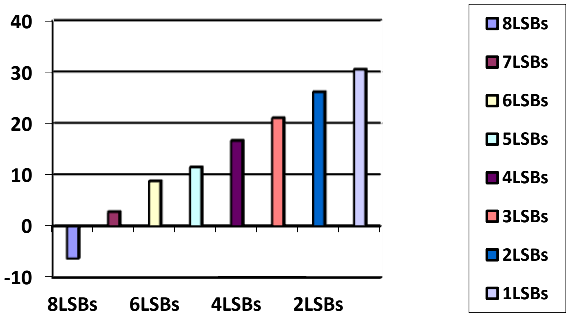


Fig-8: SNR verses No. of LSBs

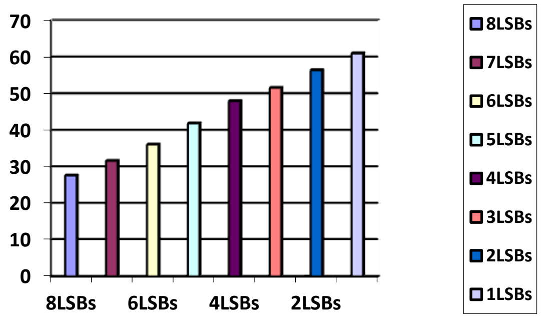


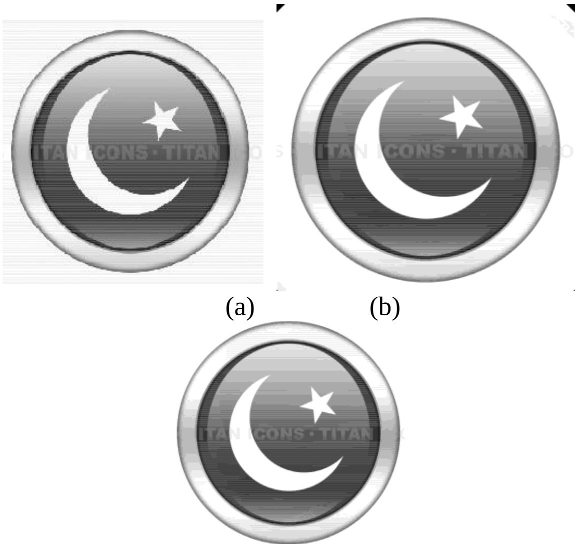
Fig-9: PSNR verses No. of LSBs

To compare the presented data hiding method with Modular Distance Technique (MDT) (Khan, and Yousaf. 2013) and Decreasing Distance Decreasing Bits Algorithm (Khan, S., *et al.* 2011), all the three data hiding techniques were applied one by one on the same cover, to hide secret message in the same cover. The resulted stego images obtained also showed that VLSB gray scale image Steganography was better than other two techniques as shown in Fig-10. The stego images of MDT and DDDB Algorithm were more distorted as compared to the proposed technique.

While comparing the proposed data hiding method Modular Distance Technique (MDT) (Khan and Yousaf. 2013) and Decreasing Distance Decreasing Bits Algorithm (Khan, S., *et al.*, 2011), the SNR and PSNR were calculated using three different cover images for hiding the same secret message. As the proposed method, MDT and DDDB Algorithm were designed for variable data hiding capacity and the SNR and PSNR varied with the variation of hiding capacity so SNR and PSNR were calculated at the fixed hiding capacity level of 48%. The statistical results obtained are listed in Table 3. The results showed that the proposed technique gave high SNR and PSNR for all the three cover images and generated much fine and clear results as compared to MDT and DDDB Algorithm. Fig-10 showed the stego images produced by MDT, DDDBA and VLSB grayscale image stegnography. The images produced clearly showed that VLSB grayscale image stegnography gave high quality stego image as compared to the other two methods.

Table. 3 Hiding Capacity, SNR and PSNR verses different no. of LSBs

Stegnograhy Technique	Hiding Capacity (%)	SNR (dB)			PSNR (dB)		
		Image 1	Image 2	Image 3	Image 1	Image 2	Image 3
MDT	48.8734	-34.2706	-33.7629	-17.7321	25.025	19.7287	33.5100
DDDBA	48.368	-17.0191	-19.8706	-10.2595	26.8401	23.8313	38.6439
Gray scale Image Stegnography	48.500	-5.8594	-6.8884	-5.6604	27.1159	26.8710	49.1779



(a) (b)

(c)

Fig-10. (a) Stego Image of MDT, (b) Stego Image of DDDB Algorithm, (c) Stego Image of VLSB gray scale image steganography

Conclusion: The stegnographic technique presented was much secure data hiding technique with variable data hiding capacity. The hiding capacity and SNR were inversely related to each other. A tradeoff was made to get the desired parameters by implementing VLSB stegnography. If the capacity was increased the distortion was increased and vice versa. Key size was proportional to number possible values of bits substituted "Bi". Minimizing the numbers of bits "Bi", used for data hiding, decreased the key size of the proposed method. VLSB methodology provided the users with full liberty to get the desired values of these parameters according to requirements.

REFERENCES

Cedric, T. M., Adi, R. W., and Mcloughlin, A. I. (2000). Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion. In IEEE Proceedings, *TENCON 2000*, Kuala Lumpur, Malaysia Vol. 1, pp. 275-278. DOI: 10.1109/TENCON.2000.893586

Dumitrescu, S., X. Wu and N. Memon (2002, June). On steganalysis of random LSB embedding in continuous-tone images. In International Conference on Image Processing. 2002. Proceedings, Rochester, NY ,Vol. 3, pp. 641-644. DOI: 10.1109/ICIP.2002.1039052

Fridrich, J., M. Goljan and R. Du (2001). Detecting LSB Stegnography in Color and Gray –Scale Images. Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, Vol. 8(4), pp.22-28. DOI: 10.1109/93.959097

Habes, A. (2006). Information transmissions in computer network. Information hiding in bmp image Implementation analysis and evaluation. Information Transmissions In Computer Networks, vol.6(1), pp.1-10.

Johnson, N. F. and S. Jajodia (1998). Steganalysis: The Investigation of Hidden Information. , IEEE Information Technology Conference, pp.113-116. DOI: 10.1109/IT.1998.713394

Khan, S., M. H. Yousaf, and M. J. Akram (2011). Implementation of Variable Least Significant Bits Stegnography using Decreasing Distance Decreasing Bits Algorithm. International Journal of Computer Science, Vol. 8 (6), pp: 292-296.

Khan, S., and M. H. Yousaf (2013). Implementation of VLSB Stegnography Using Modular Distance Technique. In Innovations and Advances in Computer, Information, Systems Sciences, and Engineering, Springer, New York, pp:511-525.

Mehboob, B., and R. A. Faruqui (2008, April). A stegnography implementation. In IEEE International Symposium on Biometrics and Security Technologies, 2008. ISBAST 2008, pp: 1-5. DOI: 10.1109/ISBAST.2008.4547669

Moon, S. K. and V. N. Vasnik (2007). Application of steganography on image file. National conference on Recent trends in Electronics, pp:179-185.

Moon, S. K. and R. S. Kawitkar (2007). Data Security using Data Hiding. International Conference on Computational Intelligence and Multimedia Applications, pp:247-251.

Morkel, T., J. H. P. Eloff and M.S. Olivier (2005). An Overview of Image Steganography. In Proceedings of the Fifth Annual Information Security, Conference (ISSA2005), Sandton, South Africa, pp: 1-11.

Ogihara, T., D. Nakamura and N. Yokoya (1996, August). Data embedding into pictorial images with less distortion using discrete cosine transform. In Proceedings of the 13th International Conference on Pattern Recognition, Vol. 2, pp. 675-679.

Rabah, K. (2004). Steganography - The Art of Hiding Data. Information technology Journal, Vol. 3 (3), pp: 245-269.

Swanson, M. D., M. Kobayashi and A. H. Tewfii (1998). Multimedia Data Embedding and Watermarking Technologies. Proc. of the IEEE, vol. 86(6), pp:1064-1087. DOI: 10.1109/5.687830

Tsai, C. T., C. Liaw, Y. H. Liao and C. H. Ko. (2011). Concealing Information in Image Mosaics Based on Tile Image Features. Journal of the Chinese Institute of Engineers Vol. 34 (3), pp: 429-440. doi: 10.1080/02533839.2011.565618.