Variable Least Significant Bits Stegnography using Modular Distance Technique

Sahib Khan[1]
Dept. of Telecommunication Engineering
University of Engineering and Technology, Taxila
Taxila, Pakistan
engrsahib_khn@yahoo.com

Muhammad Haroon Yousaf[2]
Dept. of Computer Engineering
University of Engineering and Technology, Taxila
Taxila, Pakistan
haroon.yousaf@uettaxila.edu.pk

Abstract—**This work proposes a spanking new technique, Modular Distance Technique, to implement Variable Least Significant Bits Stegnography, in spatial domain, providing twofold security. It is an overriding and secure data embedding technique having low data hiding capacity of with least distortion. This is much immune to Steganalysis providing a large Key Size. This technique can be implemented with Euclidean, Chess Board and City Block distances with same data hiding capacity for each and contributing significantly to the key size. The key size of modular distance technique is almost 27 times of the size of cover image. Low distortion made it difficult for intruder to detected hidden information and large key size make it difficult to extract the hidden information. This technique is contributing a data hiding capacity of 12.5% to 56.25% with SNR ranging from 29.7db to 8db. The hiding capacity and SNR varies with changing reference pixel, base of Mod and type of distance.**

Keywords: VLSB Stegnography; Steganalysis; Key size; Mod; Reference pixel

I. INTRODUCTION

This Stegnography is an art of concealed writing i.e. to hide useful information inside other risk-free cover file in a way that does not allow any snooper to even detect that there is a hidden information present [2] and transmitting hidden messages through innocuous cover carrier in such a manner that the existence of the embedded messages is imperceptible [1].

The history of Stegnography is very old; starting from Greeks till today it is used in a variety of applications. Greeks used it writing message on some material and later covering it with wax, tattooing messages on bald head, later growing hair to cover it up. In World War II invisible inks were used to write messages in between the lines of normal text message [7]. World War II saw the use of microdots by Germans. In microdots technology, photograph of secret message taken was reduced to size of a period. This technology was called "the enemy's master piece of espionage" by FBI director J. Edgar Hoover [8].

Now a day's Stegnography has found many applications [14 and 16] and become an emerging research area, encompassing copyright protection, water marking [4 and 5], fingerprinting and data hiding. A broad overview of data embedding and watermarking methods is available in [9]. Additional resources related to Stegnography and watermarking are obtainable at [10].

To implement Stegnography both in spatial domain or transform domain many different techniques have been introduced [19 and 20]. Discrete Cosine Transform (DCT) is used and data is hidden by exploiting the coefficient of DCT of the cover image [11]. Wavelet Transform is also used for data hiding. The most important technique implemented in spatial domain is least significant bits (LSB) Stegnography [24] utilizing the least significant bits of cover file elements (pixels, samples etc). The 4 Least Significant (4LSB) Stegnography is one of the well-known techniques of this family. In 4LSB Stenography four least significant bits of cover file elements are used for data embedding [12]. The 4LSB method is implemented for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media. The 4LSB Stegnography [6 and 13] is having a good enough data hiding capacity of 50% and is used for the exchange of secret information over public channel in a safe way. All algorithms employed for any type of format have pros and cons and depend upon the environments used [15]

II. VLSB STEGNOGRAPHY

Although 4LSB Stegnography is very effective [3] but this technique is very insecure. Once a snooper come to know that hidden information is present it is very easy to retrieve the hidden information. To overcome this problem a new data hiding method is proposed called Variable Least Significant Bits (VLSB) Stegnography having variable data hiding capacity and distortion. This technique is used o hide variable amount of data in cover file in more secure way [22], instead of a fix data as in 4LSB Stegnography. To hide variable amount of data in cover file in more secure way using VLSB Stegnography a variable amount of data is hidden in every individual pixel of each sector of the cover file. VLSB Stegnography can be implemented in various ways depending on the algorithm devised. A proper algorithm is needed to decide that how much data should be hidden in which pixel or group of pixels of cover image. VLSB Stegnography has been implemented with Decreasing Distance Decreasing Bits Algorithm [21] with significantly increased hiding capacity, distortion and key size. The distortion created in cover image

using DDDB algorithm is non uniform over the cover the stego image and is very significant for larger hiding capacity.

To get a uniform and non-detectable distortion with a large key size a new technique, Modular Distance Technique, is presented in this work. The proposed technique is having a small data hiding capacity with negligible distortion and large key size and provides twofold security mechanism. Low distortion and large SNR made the hidden message imperceptible and large key size make it hard to retrieve the hidden information

III. MODULAR DISTANCE TECHNIQUE

The main theme of VLSB Stegnography is to hide variable amount of data in a cover file/image and an appropriate algorithm/technique is needed to implement it. Modular distance Technique (MDT) is one of such methodologies to implement VLSB Stegnography with small data hiding capacity and large key size and signal to noise ratio (SNR).

MDT is a distance based technique it can be implemented with Euclidean, Chess Board and City Block distance. The prevision of three types of distances is very important and contribute much to the key size because the snoopers is not aware of the type of distance used on the sender side in data hiding process.

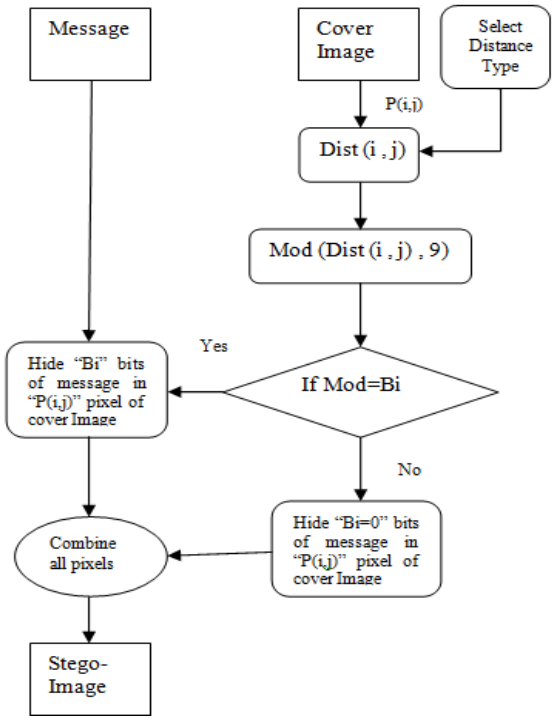


Figure1. VLSB Stegnography with Modulus Distance

To implement VLSB Stegnography with MDT first of all a reference pixel/point usually the centre point is selected. Then the distance between the reference pixel and the pixel under process is calculated by using either Euclidean, Chess Board or City Block distances. MDT then takes the modulus of the calculated distance and on the bases of the value of modulus the number of bits "Bi" to be embedded in that pixel is decided. The number of bits to be substituted varies from 0 to 8 and any number of bits within this range can be embedded in a specific pixel. How much bits "Bi" are embedded in a pixel is the key to retrieve the hidden information. This contributes much to the security of the information. After all pixels of a cover image or the whole message are processed, all the pixels are combined to get a stego image. The stego image should be much closed to the original cover file in resemblance so that the snoopers doesn't suspect about the presence of the hidden information.

The implementation of Variable Least Significant Bits Stegnography with Modular Distance Technique is shown in block diagram in figure 1.

A. *Hiding Capacity*

The data hiding capacity of VLSB Stegnography using Modular Distance Technique varies with reference pixel, type of distance and the base of modulus. The gray scale image is a 2-D array of pixels having "R" number of row and "C" number of columns, so the total number of pixels "N" is:

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

And each pixel's intensity is represented by 8bits. So the total size of the image in bits is:

$$Size_{total} = N \times 8 \quad (2)$$

Modular Distance technique provides us the liberty to embed any number of bits "Bi" ranging from 0 to 8 in a pixel of a cover image. The total data to be hidden in a cover image is dependent on the number of bits "Bi" substituted in each pixel. So the total bits embedded "Be" in the cover image are:

$$B_e = \sum_{i=1}^{N} Bi \quad (3)$$

The data hiding capacity "C" of VLSB Stegnography using Modular Distance technique is:

$$C = \frac{B_e}{Size_{total}} \times 100 \quad (4)$$

B. *Key Size*

Modular Distance Technique is much secure method for the implementation of VLSB Stegnography. This much immune to Steganalysis; because of it's of built-in encryption. The aim of Stegnography is to hide data in a cover file in non-perceivable manner but if snoopers comes to know about the presence of secret, the snoopers has to try "K" different combinations to extract the hidden data exactly. The key size of MDT depends on the size of cover image and number of types of distances. An image with rows "R" and columns "C" will have a total of "N" pixels in the image. Using MDT we can hide a number of bits "Bi" ranging from 0 to 8 bits each pixel so there are 9 possible values for a single pixel and three choices of distance type in MDT. So the total key size "K" of Modular Distance Technique is:

$$K = 3 * (R * C) * C_1^9 \quad (5)$$

$$K = 3 * (R * C) * 9 \quad (6)$$

$$K = 27 * (R * C) \quad (7)$$

$$K = 27 * N \quad (8)$$

Where N: Size of cover image.
R: Number of rows of cover image
C: Number of columns of cover image
K: Number of possible keys (Key Size)

The reference point/pixel also contribute a lot to the key size as there are "N" number of pixels/point is cover image and any of the pixel can be used as a reference. The reference point used on the sender side during data hiding process should be kept secret without the knowledge of an exact reference the retrieval of data/message is impossible. Now if the reference point is considered then the key size will be:

$$K = 27 * N * N \quad (9)$$

$$K = 27 * N^2 \quad (10)$$

$$K = 27 * (R * C)^2 \quad (11)$$

So there are a total "K" number of possible ways 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 Stego-Image even if the snoopers came to know that some data is hidden in the image he must have to try "K" various combinations to retrieve data exactly.

C. SNR and PSNR

The aim of Stegnography is to hide information in a cover image in such a manner that no one detects the presence of hidden data. For a best Stegnographic technique the stego should be closely resemble to the cover image. The quality of the stego-image is measured quantitatively by calculating signal to noise ratio (SNR) [17 and 18] and peak signal to noise ratio (PSNR) [17 and 18]. SNR for a Stego image in Decibels is calculated as:

$$SNR = -10Log\left[\frac{sum((Cover - Stego)^2}{sum((Cover)^2)}\right]^{-1} \quad (12)$$

And PSNR for a stego image in Decibels is calculated as:

$$PSNR = -10Log(Mean((Cover - Stego)^2)) \quad (13)$$

IV. Implantation

The results presented in this paper is obtained by implementing the VLSB Stegnography using Modular Distance Technique (MDT) by selecting centre pixel of cover image as reference pixel and calculating the distances of all the pixels are calculated with respect to the reference point. Then mod 8 of the distance of each pixel is taken. If the mod 8 of the distance is 0, 8 bits are used for data hiding in that pixel if mod 8 are 1, 2, 3, 4, 5, 6 and 7, then 7, 6, 5, 4, 3, 2 and 1 bits are used for data hiding respectively. The data hiding capacity, SNR and PSNR of the stego image are calculated. Then the reference point was changed the same combination was applied to calculate Capacity, SNR and PSNR. The results obtained using different type of distances; bases of mod and reference point are given in detail in experimental results section.

V. Experimental Results

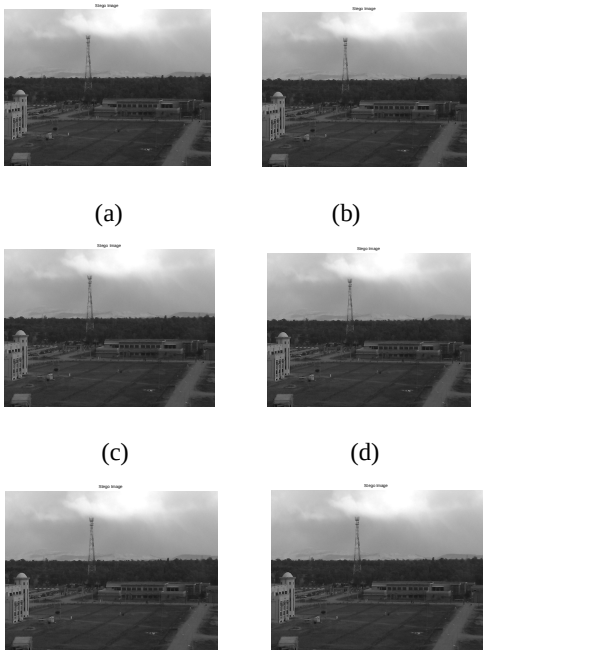
As I discussed in the earlier section that Modular Distance Technique can be implemented using three different types of distance i.e. Euclidean distance, Chess Board distance and City Block distance. In this section the results of Variable Least Significant Bits Stegnography using MDT method with different bases of mod function and with different reference point/pixel are presented one by one in details.

A. Results of MDT using Euclidean Distance

To scrutinize the effect of change in the reference point/pixel on the Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the Mod is kept constant and reference point is changed. The results are obtained for Mod 8 and with reference point centre, (0,0), (1,10), (10,1), (100,50) and (500,500) and the stego images obtained are shown in figure 2(a, b, c, d, e and f) respectively. The hiding capacity, SNR and PSNR are listed in Table 1. It has been observed from the experimental results that the parameters (Capacity, SNR and PSNR) vary with changing reference points.

Table 1: Capacity, SNR and PSNR using Euclidean Distance with varying reference points

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	8	Centre	12.5000%	29.7496	5.6852
2	8	(0,0)	12.5070	29.6667	5.6022
3	8	(1,10)	12.5168	29.4023	5.3378
4	8	(10,1)	12.5168	29.4014	5.3369
5	8	(100,50)	12.5169	29.3964	5.3319
6	8	(500,500)	12.5200	29.5388	5.4744



(a) (b)

(c) (d)

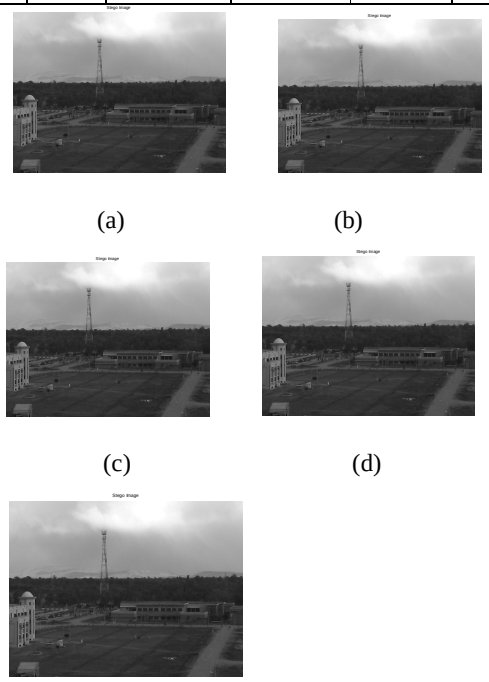
(e) (f)

Figure 2: The resulted stego images from VLSB Stegnography using MDT with Euclidean distance for fixed base of modulus and varying reference point/pixel (a) Stego image with Centre as a reference point (b) Stego image with (0,0) as a reference point (c) Stego image with (1,10) as a reference point (d) Stego image with (10,1) as a reference point (e) Stego image with (100,500) as a reference point (f) Stego image with (500,500) as a reference point

Now to evaluate the outcome of VLSB Stegnography Implemented with MDT for changing the value of Base of Modulus of distance. To get Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the reference point is kept fixed i.e. (10,1) and Base of the Modulus is altered. The results are obtained for Base 16, 8, 4, 2 and 1 with a fixed reference point (10,1) and the stego images obtained are shown in figure 3(a, b, c, d and e) respectively. The hiding capacity, SNR and PSNR are listed in Table 2. It has been observed from the experimental outcome that the Hiding Capacity increases with deceasing Base of Mod while SNR and PSNR decreases.

Table 2: Capacity, SNR and PSNR using Euclidean Distance with Varying Base of Mod

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	16	(10,1)	12.5081%	29.5760	5.5115
2	8	(10,1)	12.5168%	12.5168	5.3369
3	4	(10,1)	12.5350%	29.0572	4.9927
4	2	(10,1)	12.5734%	28.4121	4.3476
5	1	(10,1)	12.6537%	27.3269	3.2624



(a) (b)

(c) (d)

(e)

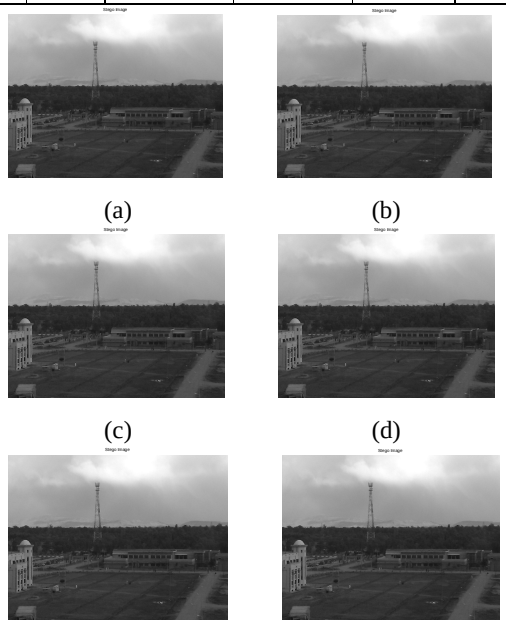
Figure 3: The resulted stego images from VLSB Stegnography using MDT with Euclidean distance for fixed reference point (10, 1) and varying bases of Mod (a) Stego image with Mod 16 (b) Stego image with Mod 8 (c) Stego image with Mod 4 (d) Stego image with Mod 2 (e) Stego image with Mod 1

B. Units Results of MDT using Chess Board Distance

To observe the effect of change in the reference point/pixel on the Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the Mod is kept constant and reference point is changed. The results are obtained for Mod 8 and with reference point centre, (0,0), (1,10), (10,1), (100,50) and (500,500) and the stego images obtained are shown in figure 4(a, b, c, d, e and f) respectively. The hiding capacity, SNR and PSNR are listed in Table 3. It has been observed that all the parameters vary with varying reference point.

Table 3: Capacity, SNR and PSNR using Chess Board Distance with varying reference points

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	8	Centre	12.5%	29.7496	5.6852
2	8	(0,0)	23.4670%	13.9030	-10.1615
3	8	(1,10)	23.4122%	13.9070	-10.1575
4	8	(10,1)	23.4123%	13.9064	-10.1580
5	8	(100,50)	23.4252%	13.8950	-10.1694
6	8	(500,500)	23.4333%	13.8959	-10.1686



(a) (b)

(c) (d)

(e) (f)

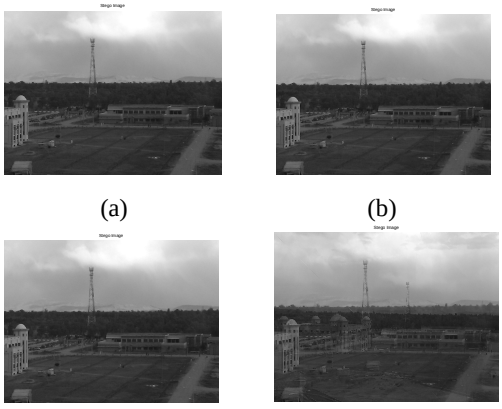
Figure 4: The resulted stego images from VLSB Stegnography using MDT with Chess Board distance for fixed base of modulus and varying reference point/pixel (a) Stego image with Centre as a reference point (b) Stego image with (0,0) as a reference point (c) Stego image with (1,10) as a reference point (d) Stego image with (10,1) as a reference point (e) Stego image with (100,500) as a reference point (f) Stego image with (500,500) as a reference point

Now to evaluate the effect of change in the value of Base of Modulus of distance on the Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the reference point is kept fixed i.e. (10,1) and Base of the Modulus is changed. The results are obtained for Base 16, 8, 4 and 3 with a fixed reference point (10,1) and the stego images obtained are shown in figure 5(a, b, c and d) respectively. It is observed experimentally that Mod 2 and Mod 1 create lots of distortion

with very large data hiding capacity. Due the no affordable distortion Mod 2 and Mod 1 can't used for Stegnographic purposes in this proposed using Chess Board distance. The hiding capacity, SNR and PSNR are listed in Table 4. It has been observed that all the parameters vary with varying the value of Base.

Table 4: Capacity, SNR and PSNR using Chess Board Distance with varying Base of Mod

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	16	(10,1)	17.9561%	16.7826	-7.2819
2	8	(10,1)	23.4123%	13.9064	-10.158
3	4	(10,1)	34.3582%	10.9521	-13.112
4	3	(10,1)	41.6555%	9.7148	-14.349



(a) (b)

(c) (d)

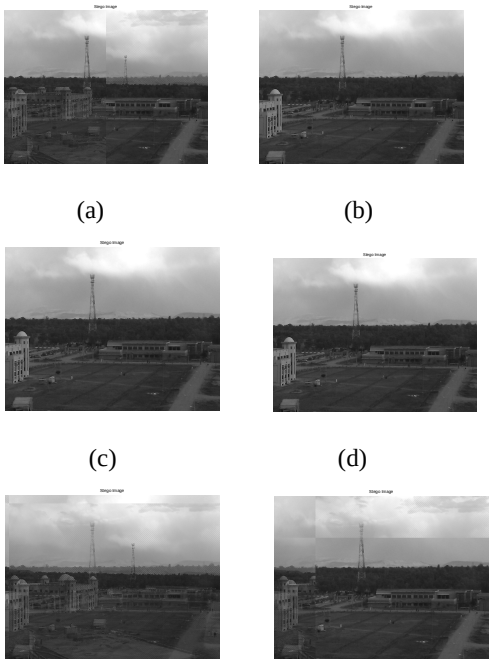
Figure 5: The resulted stego images from VLSB Stegnography using MDT with Euclidean distance for fixed reference point (10, 1) and varying bases of Mod (a) Stego image with Mod 16 (b) Stego image with Mod 8 (c) Stego image with Mod 4 (d) Stego image with Mod

C. Equ Results of MDT using City Block Distance

To observe the effect of change in the reference point/pixel on the Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the Mod is kept constant and reference point is changed. The results are obtained for Mod 8 and with reference point centre, (0,0), (1,10), (10,1), (100,50) and (500,500) and the stego images obtained are shown in figure 6(a, b, c, d, e and f) respectively. The hiding capacity, SNR and PSNR are listed in Table 5. It has been observed that all the parameters vary with varying reference point.

Table 5: Capacity, SNR and PSNR using City Block Distance with varying reference points

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	8	Centre	23.4375%	13.9057	-10.1588
2	8	(0,0)	23.4375%	13.9052	-10.1593
3	8	(1,10)	23.4375%	13.9020	-10.1625
4	8	(10,1)	23.4375%	13.9019	-10.1626
5	8	(100,50)	23.4375%	13.9026	-10.1619
6	8	(500,500)	23.4374%	13.9046	-10.1599



(a) (b)

(c) (d)

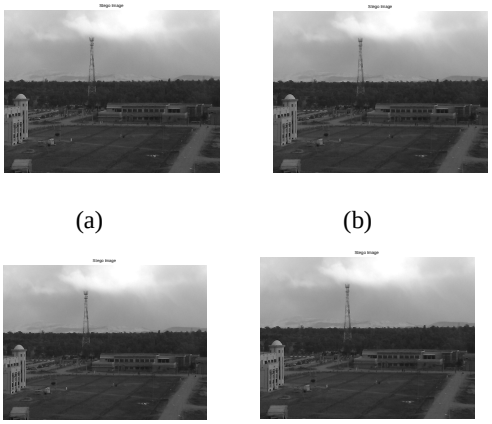
(e) (f)

Figure 6: The resulted stego images from VLSB Stegnography using MDT with City Block distance for fixed base of modulus and varying reference point/pixel (a) Stego image with Centre as a reference point (b) Stego image with (0,0) as a reference point (c) Stego image with (1,10) as a reference point (d) Stego image with (10,1) as a reference point (e) Stego image with (100,500) as a reference point (f) Stego image with (500,500) as a reference point

Now to evaluate the effect of change in the value of Base of Modulus of distance on the Hiding Capacity, SNR and PSNR, experiments were performed. Using MDT base of the reference point is kept fixed i.e. (10,1) and Base of the Modulus is changed. The results are obtained for Base 16, 8, 4, 2 and 1 with a fixed reference point (10,1) and the stego images obtained are shown in figure 7(a, b, c and d) respectively. It is observed experimentally that Mod 1 creates lots of distortion with very large data hiding capacity. Due the no affordable distortion Mod 1 can't be used for Stegnographic purposes in this proposed using City Block distance. The hiding capacity, SNR and PSNR are listed in Table 4. It has been observed that all the parameters vary with varying the value of Base.

Table 6: Capacity, SNR and PSNR using City Block Distance with varying Base of Mod

Sr. No.	Mod	Reference	Capacity	SNR	PSNR
1	16	(10,1)	17.9688%	16.8023	-7.2622
2	8	(10,1)	23.4375%	13.9019	-10.1626
3	4	(10,1)	34.3750%	10.9495	-13.1150
4	2	(10,1)	56.2500%	7.9680	-16.0965



(a) (b)

(c) (d)

Fig. 7: The resulted stego images from VLSB Stegnography using MDT with City Block distance for fixed reference point (10, 1) and varying bases of Mod (a) Stego image with Mod 16 (b) Stego image with Mod 8 (c) Stego image with Mod 4 (d) Stego image with Mod 2

Now on comparison of all the stego images with original cover image and Stego image of 4LSB Stegnography shown in figure 8 (a and b), it can be seen that all the stego images obtained by VLSB Stegnography using Modular Distance Technique closely resemble the cover image and the quality of the stego images is much better than that of 4LSB Stenography's Stego image. But at the same time it can also be seen that for some specific values of reference point and base of Mod, the stego images are much distorted even with low data hiding capacity as shown in figure 5 (d) and figurer 6 (e and f). The SNR and Capacity vary with the input parameters. The appropriate selection of Reference Pixel and Base for Mod is the key to fine results.

(a) (b)

Fig. 8: Cover Image used in Stegnographic Process and the Stego image resulted by 4LSB Stegnography (a) Cover Image (b) Stego image of 4LSB

VI. CONCLUSION

After In this paper I have proposed an efficient technique to implement VLSB Stegnography. The proposed scheme has a large key size and Signal to Noise ratio. The stego image quality is very high, closely resembles to the cover image, so that hidden information are invisible. Due to good enough SNR and large Key size the MDT is providing twofold security. The hiding capacity and SNR varies with both base of Mod and location of reference point/pixel. The selection of appropriate values of both of these parameters is very important and plays a vital role in the whole Stegnographic process.

REFERENCES

[1] S. Dumitrescu, W.X.Wu and N. Memon (2002) On steganalysis of random LSB embedding in continuous-tone images, Proc. International Conference on Image Processing, Rochester, NY, pp. 641-644.

[2] S.K. Moon and R.S. Kawitkar," Data Security using Data Hiding", International Conference on Computational Intelligence and Multimedia Applications 2007, pp.247-251.

[3] S.K. Moon and R.S. Kawitkar," Data Security Using Data Hiding" International Conference on Computational Intelligence and Multimedia Applications 2007.

[4] Jiang-Bin Zheng, David Dagan Feng and Rong-Chun Zhao, "A Multi-Channel Framework for Image Watermarking", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005

[5] F. Uccheddu, M. Corsini, M. Barni, *"Wavelet-Based Blind Watermarking of 3D Models"*, Proc. of ACM Multimedia and Security Workshop,pp.143–154, 2004

[6] Ker, A.: Improved detection of LSB steganography in grayscale images. Proc. 6th Information Hiding Workshop. Springer LNCS, vol. 3200, pp. 97-115, 2004.

[7] T. Cedric, R. Adi and I. Mcloughlin (2000), Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion, Proc. IEEE International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia,pp. 275-278.

[8] D. Kahn, the Codebreakers, Macmillan, New York, 1967.

[9] Beenish Mehboob and Rashid Aziz Faruqui," A Stegnography Implementation", IEEE, 2008.

[10] M.D. Swanson, M. Kobayashi, A.H. Tewfii, "Multimedia Data Embedding and Watermarking Technologies", *Proc. of the IEEE*, vol. 86, no. 6, June, 1998, pp. 1064-1087.

[11] http://isse.gmu.edu/~njohnson/steganography

[12] Takeshi OGIHARA, Daisuke NAKAMURA and Naokazu YOKOYA, "Data Embedding into Pictorial Images with Less Distortion Using Discrete Cosine Transform",

[13] J.Fridrich, M.Goljan, and R.Du,"Detecting," LSB Stegnography in Color and Gray –Scale Images", Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, 2001, pp.22-28.

[14] S. K. Moon, V. N. Vasnik, "Application of steganography on image file", National conference on Recent trends in Electronics, pp. 179-185.

[15] Alkhraisat Habes, "Information transmissions in computer network. Information hiding in bmp image Implementation analysis and evaluation" (Jan.2006)

[16] T. Morkel, J. H. P. Eloff, M. S. Olivier,"An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[17] http://www.mathworks.com

[18] http://www.math.ucla.edu/

[19] **R** Anderson, (ed.), **Informalion hiding: first international workshop,** Cambridge, **UK Lecture** Notes **in Computer Science,** vol. **1174,** Berlin Heidelberg New York Springer-Verlag, **1996.**

[20] W. Bender, D. Gruhl, N. Morimoto, A. **Lu,** "Techniques for Data Hiding", **IBM Systems Journal** Vol. **35,** No. **3k4. MIT** Media **Lab,** pp. **313-336, 1996.**

[21] Sahib Khan and M. Haroon Yousaf, "Implementation of Variable Least Significant Bits Stegnography using Decreasing Distance Decreasing Bits Algorithm". (unpublished)

[22] Sahib Khan and M. Haroon Yousaf, "Variable Least Significant Bits Stegnography". (To be published)

[23] http://www.kust.edu.pk