

# Snake and Ladder based Algorithm for Steganographic Application of Specific Streamline Bits on Prime Gap Method

Jas R Sheth

Department of Electrical and Electronics Engineering  
VJTI, Mumbai ,India.

## ABSTRACT

Steganography is the art of hiding data in a particular form of media and making it accessible for the recipient. This process of encrypting data can be embedded in media like image and audio. This paper represents a snake and ladder based algorithm for encrypting a streamline of bits in a greyscale image.

## Keywords

Image Stegnography, Snake and Ladder Algorithm , LSB bit plane Stenography, Edge encryption, Prime Gap.

## 1. INTRODUCTION

Stegnography is an age old method to hide data . But with the advent in media technology, many different methods have been laid down for the same. It has been possible to apply this method in image ,video, text and audio. The growth in Information Technology has made it necessary for encrypting essential data to make it revertible to the desired one.

Steganography is complementary to cryptography, where it aims at hiding the existence of a message rather than making the message illegible through encryption. Thus Stegnographic applications are important where public interference is to be prohibited and keep the original data being corrupted.

## 2. a) CLASSIFICATION

Stegnography can be classified[1] into pure , symmetric and asymmetric. Pure Stegnography does not need any exchange of information but the latter two requires the exchange of information via a media.

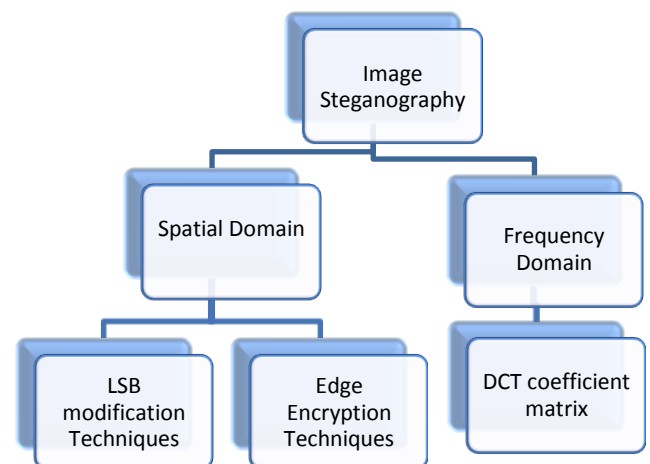
The various Carrier Objects used are as follows:

- Network Protocols such as TCP ,IP and UDP
- Audio Format such as mpi ,wav
- Text such as null characters and morse code including html and java
- Image files
- Video formats such as mpeg

This paper represents a steganographic methodology using Cover as a Image.

Images are cover objects in Steganography. The data to be encrypted is embedded based on the method adopted in Image Steganography.

## b) IMAGE STEGNOGRAPHY



Spatial domain involve direct manipulation of pixels in an image. Frequency

domain techniques are based on modifying the Fourier transform of an image.

Steganography algorithm operate on three types of images:

- Pallete based images(i.e.GIF images)
- Raw images(i.e,BMP format)
- JPEG images.


One of the most popular format used on the internet is JPEG (Joint Photographic Expert Group). [6] It provide large compression ratio and maintain high image quality by measuring PSNR value.

LSB modification derived from the fact that modification to

Least Significant Bits cannot be perceived by human eyes.

The following is a basic example of LSB plane slicing on a 3x3 image for 3 bit quantization

7	2	5
4	1	2
5	6	3

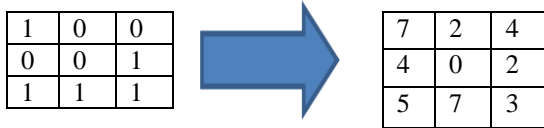


6	2	4
4	0	2
4	6	2

Original Image

Sliced Image

The LSB bit plane is now embedded by a sequence of bits as shown



**Secret Message**

**Stegno Image**

However this method is not so robust and have a low PSNR, thus affecting the encrypted data. As all the pixels are altered, the stream of bits can be easily extracted by reverse algorithm.

This method is overcome by Edge Encryption Techniques. Human eye is not capable to detect high frequency components in an Image. This ideology is developed and explored in Discrete Cosine Transform In JPEG[5]. Edges are distinguished by two methods

- Pixel Value Difference (PVD)
- Edge Detection Operators like Roberts Perwitt and Canny

The use of operators depends upon the application. Edge Encryption Techniques involves a Stegno-Key for safety and enabling the recipient to receive the secret data.

### 3. PIXEL VALUE DIFFERENCING

Pixel Value Differencing[9] is able to provide a high quality stegno image in spite of the high capacity of the concealed information. That is, the number of insertion bits is dependent on whether the pixel is an edge area or smooth area. In edge area the difference between the adjacent pixels is more, whereas in smooth area it is less. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas. This method hides the data in the target pixel by finding the characteristics of four pixels surrounding it.

Few of the various techniques implemented under Image Stegnography are as follows :

**a. Difference Expansion (DE):** It is a 1-D Haar Wavelet based proposed by Tian [2] used for hiding data. At a time only one pixel pair is used then integer average of these pixel pairs and difference of these pixels is computed. The difference value is used to embed the secret data; hence it is named as difference expansion. The difference value is doubled and bit is embedded either by expanding difference or by changing the LSB of difference value. So two categories of pixels are made which are Expandable pixels and Changeable pixels. To prevent overflow / underflow problem, a location map is required. This technique has good hiding capacity but content of image is not taken into account so Distortion is always present.

**b. Histogram Modification Technique:** In this method proposed by Ni [4] the peak and zero points are calculated from the histogram of the image. The peak points are used for hiding the data. The cover image and the secret data can be recovered with the help of auxiliary equation. However, this method is ineffective in case of flat Histograms.

**c. Prediction based scheme :** It is an extension to the Difference Method proposed by Thodi [5]. It uses prediction data error rather than using the actual pixel value difference to

hide the data. This method has a increase capacity to store the data but at the cost of PSNR and MSE given by equation (1) and (2)

$$\text{PSNR} = 10\log_{10}255/\text{MSE}^2 \quad (1)$$

$$\text{MSE} = (1/(M*N)) \sum^i \sum^j ((I'(i,j) - I(i,j))^2 \quad (2)$$

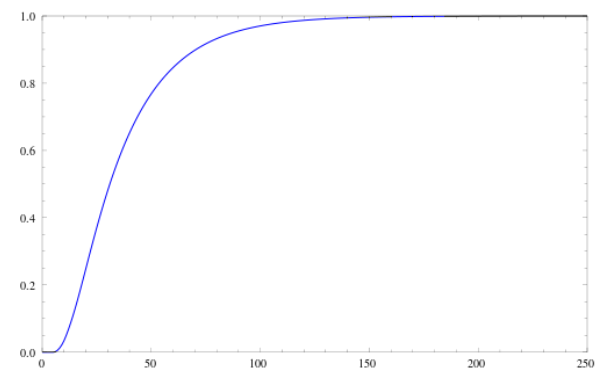
where  $I'$  is marked image formed by embedding data.

## 4. HISTORY OF SNAKE AND LADDER

Snake and Ladder is an ancient game having it roots of origin in Indian culture. It is known as Spear's Game in United Kingdom on a 10 x10 board. The participant have a die having the equi-spaced probability of 1/6 of each roll of a die.

This paper discusses the algorithm based on the game of Snakes and Ladder and the movement of participant based on the Prime and Non Prime value of pixel location. The stegno key is encrypted on maximum PVD obtained.

The following Figure 1 is a probability distribution function of completing the game of Snakes and Ladder in definite chances.



**Figure 1: Probability Distribution Function for completion of Snakes and Ladder**

It shows that that probability of completing the game approximately reaches a threshold of 90 to 100. This concept is used to decide the number of streamline bits .

## 5. PROPOSED ALGORITHM

In this paper the idea of PDF from Snake and Ladder game is developed in Image Stegnography along with the concept of Pixel Value Differencing for encrypting the Stego key and length of secret data .The Image matrix is considered as  $M \times N$  board of mentioned game. The Starting address of encrypting and decrypting the streamline bits is based on the Stego Key1. As the game of Snake and Ladder is from the first row of the board  $[C(1,J)]$  , we have the Stego Key1 as the column of Image Matrix where  $C$  is the grey level Cover Image and  $D$  is matrix obtained after performing PVD

Stego Key = Column Address on First Row.  
 Starting Address =  $D(1, \text{Stego key})$ .

### Encrypting Process and Algorithm

For encrypting the Stego Key , Pixel Value Differencing is carried out. The maximum value in the PVD matrix is computed and the Stego Key is stored as an offset from 255.

$D(i,j) = C(i,j+1) - C(i,j)$  where  $i$  computed from  $i$  to row of  $C$ .

To encrypt the Stegno Key1 of Starting address

$$D(p,q)=255-\text{maximum}[D(i,j)]$$

This offsets the Stegno key of Starting Address.

The length of streamline bits is used as a 2nd Stegno Key where the immediate right diagonal pixel to the maximum in PVD matrix is used as length of streamline bits to be encrypted.

$$D(m,n)=255-D(p+1,q+1)$$

**Table 1 : Mapping of Stego Keys**

	Q	Q+1
P	Stego Key1	
P+1		Stego Key2

where m,n is the location of length of streamline bits and p,q is the location of the starting column on first row of cover image.

By PVD matrix we get the the Edge of the cover Image and hereby can hide the the two Stego keys in high frequency domain.

The encryption of two stego keys is followed by embedding the streamline bits in the Cover image by LSB modification technique.

The Snake Ladder Algorithm is used for embedding the Data using Prime - Non Prime Logic.

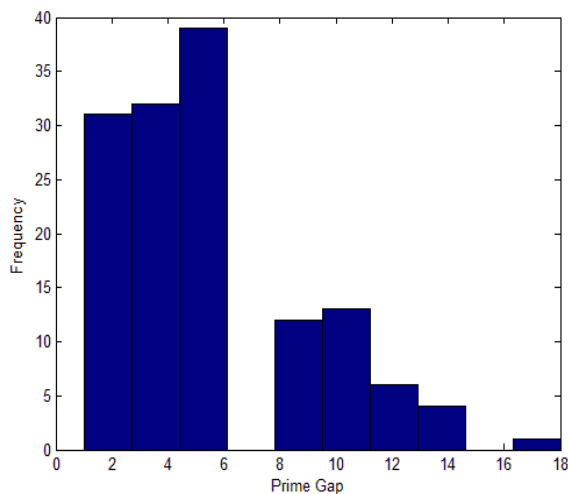
## 6. PRIME GAP FUNCTION

The prime gap is the difference between two consecutive prime numbers.

$$g_N = p_{N+1} - p_N$$

The first terms of  $g_N$  are as follows: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 2, 6, 4, 2, 6, 4, 6, 8

We observe that initially the 2 has a prominent appearance in the prime gap function and higher differences are observed as we move along the sequences of Prime Numbers.



**Figure: Histogram of Prime Gap till maximum (R,C) for Cover Image 1**

The pixel address having two variable localization parameters  
 1) row 2) column.

Let us consider the localization of pixel a function (Lof()) of two parameters r and c

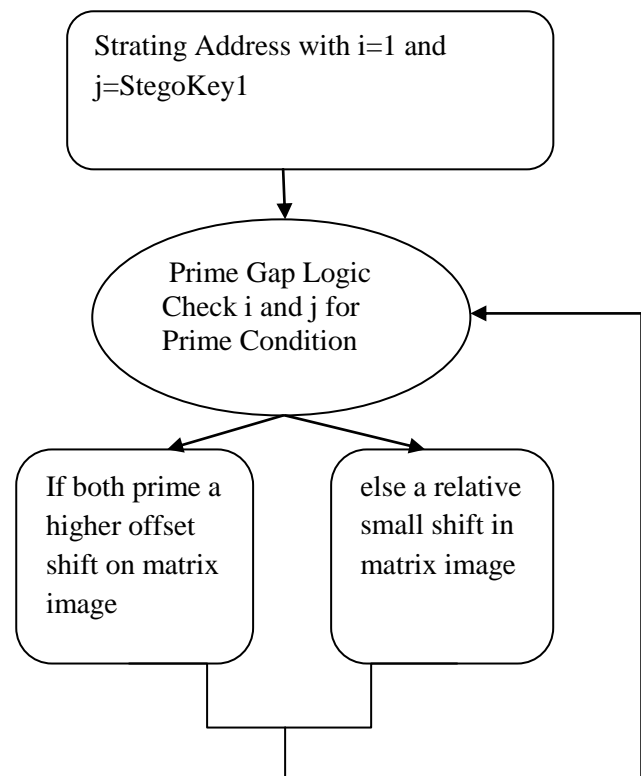
$$L = f(r_i, c_i)$$

where is the variable parameter.

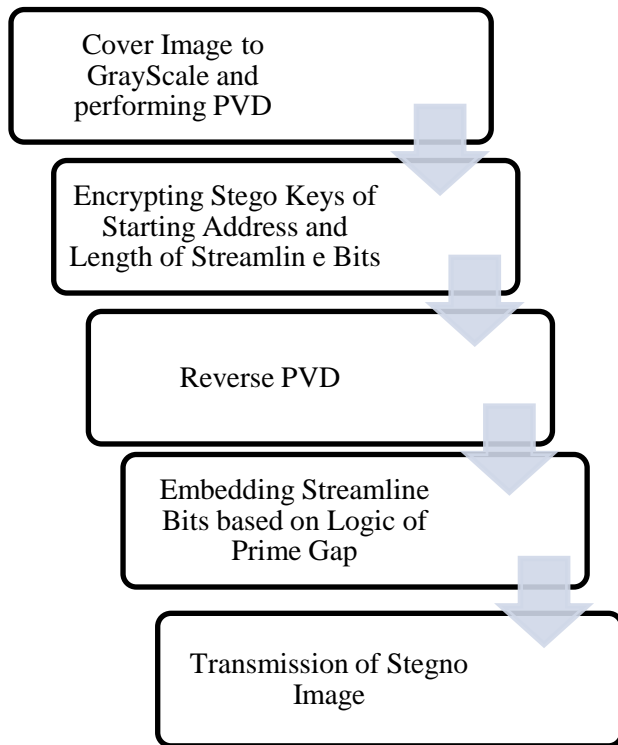
**Table 2: Probability Distribution**

$R_i$	$C_i$	Cover Image 1	Cover Image 2
Non-Prime	Non-Prime	0.9969	0.9985
Prime	Non-Prime	0.0019	9.9156e-04
Non-Prime	Prime	0.0012	5.0970e-04
Prime	Prime	2.3496e-06	5.0615e-07

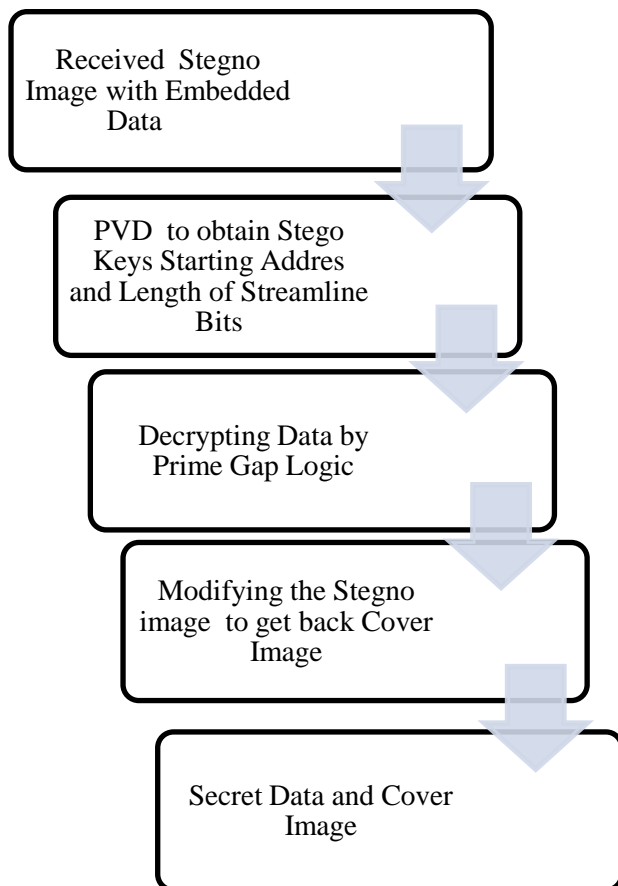
We observe that the probability of both  $r_i$  and  $c_i$  being prime is the least. Hence maximum leap in the cover image should occur when the latter case is confronted.



## 7. a) ENCRYPTION FLOWCHART

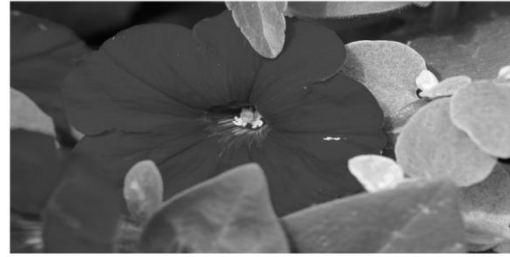


## 7. B) DECRYPTION FLOWCHART

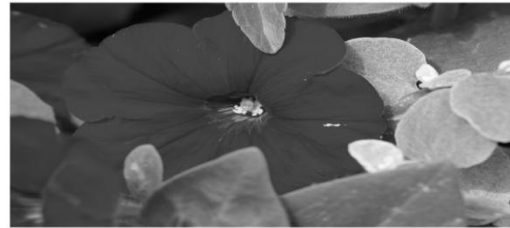


## 8. RESULTS

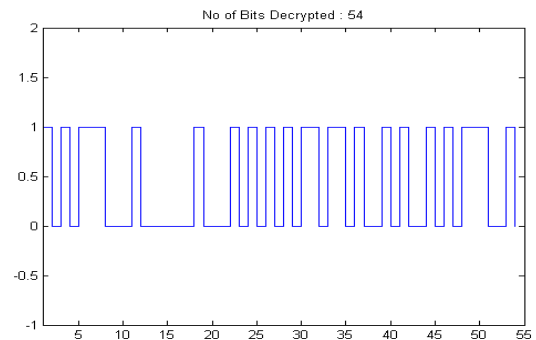
The Snake and Ladder Algorithm as discussed in this paper is implemented on various cover images and varying the length of streamline bits and results on two cover images are shown:



**Figure :Cover Image 1**



**Figure: Stegno Image 1 with 54 bits encrypted**



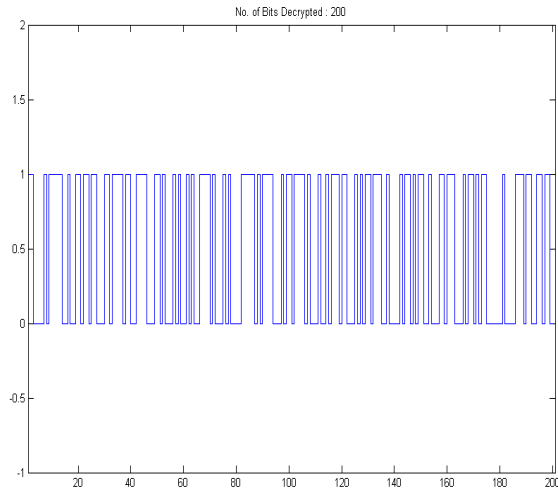
**Figure : Decrypted 54 bits**



**Figure :Cover Image 2**



**Figure: Stegno Image 2 with 54 bits encrypted**



**Figure : Decrypted 200 bits**

## 9. CONCLUSION

This paper has represented a safe and effective algorithm as compared to traditional Difference Stegnographic methods and developed a Snake and Ladder method for embedding secret data. In the recent years researchers are developing techniques to embed secret data into compression code of images. There is requirement of such methods for bandwidth limitation. As compared with the results obtained from PSNR values the proposed method has a efficient outcome as compared to the other PVD methods proposed. The future implementation works on this algorithm is on RGB sacle using multiple switching across three planes thus enabling to triple the amount of data to be encrypted. Moreover the future works also include in working on applying Stego keys encryption in frequency domain. Steganography will be major interest for researchers owing to its application in many fields. Taking a new path in Image Processing , Steganography has led open a new field of interest for researchers and developers.

## 10. REFERENCES

- [1] N.F. Johnson, S. Jajodia, Exploring Steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.
- [2] J.Tian, “Reversible Data Embedding using a Difference Expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003
- [3] T Morkel, J.H.P Eloff, M.S Olivier, “AN OVERVIEW OF IMAGE STEGANOGRAPHY Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005),2005
- [4] Z.Ni, Y.Q. Shi, N. Ansari and W. Su, “Reversible Data Hiding”, IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3 , pp. 354-362,Mar 2006.
- [5] D.M.Thodi and J. J. Rodriguez, “Expansion EmbeddingTechniques for G. K. Wallace, “The JPEG still-picture compression standard,” Commun. ACM, vol. 34, pp. 30–44, Apr. 1991.
- [6] W. B. Pennebaker and J. L. Mitchell, JPEG Still Image Data Compression Standard. New York: Van Nostrand Reinhold, 1992.
- [7] “MPEG-2 video,” ITU-T Recommendation H.262-ISO/IEC 13818-2, Jan. 1995.
- [8] “Video coding for low bitrate communication,” ITU-T Recommendation H.263, Dec. 1995. Reversible Watermarking, ” IEEE Trans. on Image Processing, vol. 16, no. 3, pp. 721–730, Mar. 2007.
- [9] K.L.chung, Y.H.Huang, W.M.Yen, W.C.Teng “Distortion Reduction for Histogram Modification Based Reversible Data Hiding” Applied Mathematics and computation, vol. 218, no.22, pp. 5819-5826, Dec 2011.
- [10] R. Chandramouli, Nasir Memon, “Analysis of LSB based Image Steganography Techniques”,Proc. International Conference on Image Processing, 2001, Vol. 3, pp. 1019-1022, 2001.
- [11] Mehdi Kharrazi, Husrev T. Sencar,Nasir Memon, “Image Steganography: Concepts and Practice”, WPSC/Lecture Note Series,pp.3, April,2004. Source: [www2.ims.nus.edu.sg/preprints/ab2004-25.pdf](http://www2.ims.nus.edu.sg/preprints/ab2004-25.pdf).