Analysis of Several Image Steganography Techniques in Spatial Domain: A Survey

Munesh Chandra Trivedi
Computer Science Department
ABES Engineering College
Ghaziabad, India
+91-9999013200
muneshtrivedi@gmail.com

Shivani Sharma
Computer Science Department
ABES Engineering College
Ghaziabad, India
+91-8800764073
Shivanisharma2804@gmail.com

Virendra Kumar Yadav
Computer Science Department
ABES Engineering College
Ghaziabad, India
+91-7530968048
virendrashines@gmail.com

ABSTRACT
Steganography enables user to hide confidential data in any digital medium such that its existence cannot be concealed by the third party. Several research work is being is conducted to improve steganography algorithm's efficiency. Recent trends in computing technology use steganography as an important tool for hiding confidential data. This paper summarizes some of the research work conducted in the field of image steganography in spatial domain along with their advantages and disadvantages. Future research work and experimental results of some techniques is also being discussed. The key goal is to show the powerful impact of steganography in information hiding and image processing domain.

General Terms
Security.

Keywords
Spatial domain, frequency domain, edge detection, mean square error, intensity, distortion.

1. INTRODUCTION

In the age of information technology, secured and confidential communication is the main need of individual. Classical method achieves this but their performance degrades and does not cope up with recent advancement in computing technology. Different steganography techniques have been used since ancient times like invisible ink; microdots character arrangements etc [1]. Now with the digitization of modern times, several digital mediums can be used to perform steganography such as image, text, audio, video etc [2].

ICTCS '16, March 04-05, 2016, Udaipur, India
 ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905294

So for this purpose steganography provides a mechanism by which data can be securely transmitted. Steganography is a technique which enables to hide data inside any digital medium such that it is not detectable in a covert channel. While applying steganography some parameters has been taken care of like quality of the cover image should be maintained, level of security, space requirement and resource utilization.

1.1 Image Steganography
Without secure communication images can be used for illegal and unwanted activity. Image steganography emerges as a helpful tool which serves to protect data and other intellectual properties from unwanted attacks. It focuses on three important points –where to hide secret message in the cover image, how securely embedding is done and how safe is the payload. Some parameters affect the development of steganography technique which include capacity, robustness, capability, delectability, complexity and security (perceptual and transparency).Hiding capacity is also known as embedding capacity. The main concern while developing a new steganographic algorithm is to increase the hiding capacity with minimum distortion and time complexity. Image steganography technique is classified as spatial domain technique, frequency domain technique, spread spectrum technique and statistical technique [4] but mainly image steganography is classified into two domains i.e. spatial and transform domain. Spatial domain is also known as image domain and frequency domain is known as transform domain. In spatial domain pixel value is direct manipulated i.e. embedding of data is done directly to intensity of pixel[3] while in frequency domain Fourier transform is modified by converting pixel value to pixel frequency, after this data is embedded in the image. Spatial domain is based on the physical location of pixels in an image [5].There are many simple and powerful techniques in spatial domain. In spread spectrum method while sending information message is spreaded over a wide frequency bandwidth than the minimum required bandwidth. In statistical method various numerical properties of the cover image has been altered and hide the message bits in the block of a cover image. They are mainly characterized by some features such as simplicity, reduced hardware requirement, shortened implementation time and overall low time complexity [6]. The main focus in this paper is on spatial domain only. In the spatial domain pixel intensities can be modified without concerning pixel location, modification is done on the basis of neighboring pixel intensities.

2. VARIOUS TECHNIQUES FOR IMAGE STEGANOGRAPHY

2.1 Pixel Indicator Technique for color image

It is mainly designed to work on 24 bit/pixel RGB images. Adnan Abdul-Aziz Gutub [7] proposed a method PIT (Pixel Indicator Technique) which uses RGB images as cover. There are mainly two phases, Phase I is construction phase and Phase II is known as recovery phase. In phase I this technique uses 2 LSB bits of any one of RGB channels as an indicator of secret data existence in the other two color components. Many combinations of RGB can be formed such as RBG, GBR, GRB, BRG and BGR out of which indicator channel is chosen. The indicator LSB bits are available randomly on the basis of image and its properties. Indicator value based action is as shown in table below,

Table 1. Indicator values Based action

Indicator Channel	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2bits of hidden data
10	2bits of hidden data	No hidden data
11	2bits of hidden data	2bits of hidden data

If the indicator channel is selected than other two channels serves as channel 1 and channel 2 respectively. For example if Red is chosen as indicator channel then green will be channel 1 and blue is channel 2 respectively. Similarly follows for other sequences. Size of the hidden message is stored in the first 8 bytes of the cover image and is also used to define the beginning of the indicator channel sequence. All the LSB's of RGB channels are consumed by the 8 bytes, assuming it is enough to store the size of the hidden bits. There are mainly two levels, first level assumes indicator choice and second one is data hiding channels as shown in table given below. There are six possible selections which are obtained from the length of message indicated as N. Now three cases arises depending on the value of N i.e. either even, prime or else .Indicator channel selection criteria works as follows,

Table 2. Indicator Channel Selection Criteria

Type of length (N) of secret message	I Level Selection Select indicator channel, first element of sequence	II Level Selection Binary N parity-bit	
		Odd Parity	Even Parity
Even	R	GB	BG
Prime	B	RG	GR
Else	G	RB	BR

Phase II corresponds to recovery phase which is performed in reverse manner of phase I. It starts with reading the length of the message (N) from the first 8 bytes of the image. The value of N is then used to specify the sequence of the channels as indicators and will stop based on the length of the secret message. The proposed technique is applied on a BMP image and this PIT method is compared to stego-1 bit, stego-2 bit, stego-3 bit, stego-4 bit and stego color cycle techniques. Bits are increased to measure the security level of the proposed method. If the length of the message is changed then selection of the sequence of RGB will also change, reflecting the distribution in all channels. To measure security vs. capacity multi-bits per channel is used in the same cover image. No visual difference is identified by using 2 LSB bits, XOR operation is being performed to mark differences in stego and cover image, indication channel varies from pixel to pixel with natural random value depending on the pixels of cover image, uses one channel for indication and data is embedded in other two channel components.

2.2 Hash based approach for secure keyless color image steganography

Hash based approach uses a hash key which will generate a pattern of pixels and data will be stored in those generated pixels. As this approach is applied to color images, three bands will be used i.e. RGB to hide data. The data will be stored in the selected pixel which a can be either RGB. Ankit Chaudhary et al [8]. This method uses keyless steganography approach and to increase the security message is distributed the secret data throughout the image and not only to specific portions. One of the best keyless steganography approaches is PIT (Pixel Indicator Technique) algorithm proposed by A.Gutub [9]. In this a color channel is used as a pixel indicator and other two channels are used to embed secret message. Proposed method tries to overcome the limitations of the methods suggested in [10], which is an improved version of [9].This method focus on a single function i.e. randomization function and does not calculate the values of K1 and K2, whose values are dependent on secret message length and size of the cover image. Random distribution is carried out using indicator values. Current method uses MSB(Most Significant Bit) of RGB channel as a pixel indicator values and does not utilize the entire channel as done in [10].Firstly compression is being carried out on the text message file ,then MSB indicates the sequence in which message is to be hidden using LSB. Indicator values works as follows:

Table 3. Indicator values

MSB bits of Red, Green and Blue channel sequentially	Sequence of channel's LSB bits where the message bits needs to be Hidden
000	Red, Green and Blue (RGB)
001	Red, Green and Blue (RGB)
010	Red, Blue and Green (RBG)
011	Blue, Red and Green (BRG)
100	Blue, Green and Red (BGR)
101	Green, Red and Blue (GRB)
110	Green, Blue and Red (GBR)
111	Green, Blue and Red (GBR)

This non-linearity increases the security and is difficult to decode. This scheme is suggested in [10].Instead of using a fixed key number K2, which indicates the gap between two pixel values as suggested in [10], this method suggests a randomized method based on hashing technique with respect to MSB of RGB. Now the gap depends on the value of R, which is a random number generated based on the seed value S. Secret data will be embedded after R no. of bytes. The resultant out is stego image which is passed to the receiver's end. Extraction will be done in reverse manner of the embedding process. Firstly message is retrieved by skipping R no. of bytes every time ,using indicator values as shown in Table III, by which we get a compressed text file. After that decompression is carried out and the output is the original text message file. Message is randomly distributed throughout the image i.e. not based on ROI approach.

2.3 Pixel Value Differencing

Pixel value differencing method (PVD) was proposed by Wu and Tsai [11] which classifies image area on the basis of two regions i.e. smoother region and hard region[12].Smoother region have small difference with their neighboring pixel value so not an ideal one to embed data. On the other hand hard regions are suitable for embedding data as they have large difference with their neighborhood pixels. PVD methods possess high embedding capacity and imperceptibility. Human Visual System (HVS) is less sensitive to changes in edges as compared to smoother regions because edge pixels cause less distortion in the image. This method divides the cover image into non-overlapping blocks. A block contains two connecting pixels and then pixel difference is modified in each pair for data embedding. Larger difference means greater modification in the cover image. While doing extraction original range table is required so that stego image can be portioned by the same method as used in original (cover) image. There are two modified versions of PVD which are Tri-way pixel value differencing (TPVD) method [13] and Adaptive pixel value differencing (APVD) method [14].PVD method uses only one direction for embedding data while TPVD method uses three dimension pixels selection i.e. horizontal, vertical and diagonal dimension. Essential requirement of this method is pre-processing of image into 2x2 pixel blocks. APVD method is applied to gray scale images only and has hidden capacity will be equal to Wu-Tsai's PVD method .The stego image quality of APVD method is satisfactory. Several PVD approaches have been proposed [15].

2.4 Pixel Value Modification

Nagaraj et al [16] proposed a method of pixel value modification method by Modulus 3 function. In this method a color image is divided into 3 color planes (RGB). Each pixel has 24 bits, each one as 8 bit components in pixel. All the 3 planes have been used for embedding data. Each color components of a pixel has been separated and each having a matrix of dimension X*Y. PVM hides data in a sequential manner i.e. first bit is embedded in red component matrix, second bit in green component matrix and third bit in blue component matrix. Similarly this process will be followed for rest of the bits. Modulus 3 operation is applied in both embedding and extracting procedure. Modulus operation is applied on f and d, where d is the secret digits and f is the output generated after applying modulus operation. The pixel value of the cover image that is selected for embedding secret data should fall in the range of $0 \le gi \le 250$. Secret data is being converted into base values 0, 1 and 2 which have to be embedded in RGB planes. A function f is calculated for each plane by Eq (1),

$$f=f(g_1,g_2,g_3,\ldots\ldots g_n)= \sum g_{ri} \bmod 3 \quad (\text{for } i=1 \text{ to } n) \qquad (1)$$

where $g_1,g_2,g_3,\ldots\ldots g_n$ are pixel values of image matrix and g_{ri}, g_{gi}, g_{bi} is decimal value RGB pixel.

Three cases are being followed:

Case 1: If f is equal to d, then no modification is needed. The old value of g_{ri} is assigned as a new pixel value.
Case 2: If f is not equal to d and f<d , then the value of g_{ri} is increased by 1 i.e. $g_{ri}+1$ is the new modified value.
Case 3: If f is not equal to d and f>d, then the value of g_{ri} is decreased by 1 i.e. $g_{ri}-1$ is the new modified value.

These three cases will be used repeatedly for embedding secret data in RGB planes of the cover image. After doing modification of pixel values in the cover image, the combination of RGB planes will result in stego image .Extraction of bits will be done by dividing the stego image into three planes RGB respectively. Now, the pixel value in the range $0 \le gi \le 253$ will be selected from the RGB plane of stego image. Now the pixel value will be extracted by applying Eq. (2), which will give the value of d ,

$$d=g_{ri}' \bmod 3 \qquad (2)$$

Eq. (2) will be used on green and blue plane in a similar manner. Now the obtained secret digits of base 3 will be converted into original secret data.

2.5 Specific regions of interest (ROI)

It is a new approach in image steganography as it targets only specific regions within an image where secret data has to be embedded. Specific area used must ensure less distortion in the cover image. One of the most popular methods is edge regions in an image which provides randomized pixel positions [17]. By embedding secret data in randomized pixel positions payload is being scattered throughout the cover image and it reduces the probability of detection of secret message for a steganalyst. Along with scattering the payload, one of the main concerns is providing security to the payload.

2.6 Edge Region Based Steganography

It comes under Object Based Steganography. Mostly edge based approaches uses PVD method for separating hard and smooth regions of a cover image. Edges are used for hiding data as they can bear more variation than smooth areas and the probability of detection is less. In 2007, a new LSB technique has been introduced known as RELSB (Random Edge LSB). This technique hides data randomly into the regions that are having least similarity with their neighborhood. These regions contain thin lines, end of lines, edges etc. To extract such regions Robert Cross Gradient Operator is used. Then PRNG (Pseudo Random Number Generator) algorithm is used to select random locations in these regions. Data is embedded in a manner that same edges and line pixels are detected before and after data embedding [18]. In 2008, an edge based approach LSB approach was introduced [19]. This technique is the combination of LSB substitution and PVD (Pixel Value Differencing) method. This technique is efficient as it provides imperceptibility and more capacity to hide data. In 2010, a hybrid edge detection method was introduced which increases the embedding capacity with high PSNR rate. It fuses two edge detector methods which are fuzzy edge detector [20] and Canny edge detector [21] to provide more number of edge pixels than their individual results. Hybrid detector divides the image into non overlapping block of size say n. In each block LSB of first pixel is used to describe the status of other pixel which can be edge and non edge pixel.

2.7 Chaos Based Edge Adaptive Image Steganography

Edge adaptive embedding methods provide necessary pixel randomization because in an image edge regions are scattered throughout an image. This method uses Canny's Edge Detection method [22] for detecting edge pixels in a vessel (cover) image and embed data only in the selected pixels. Canny's Edge detection method has based proposed in 1986 and has been considered superior to other edge detection methods. Used commonly for testing and real time implementation. To increase the security of the payload encryption technique chaotic maps has been used widely

such as Henon's Map, Logistic Maps etc. In this approach Cat Mapping has been used to distort the payload initially. Cat Mapping[23] posses an important feature i.e. when it is applied to an image then after a certain number of iterations Cat Mapping gives original image. Besides intermediate stages contains distorted image having very less resemblance to the original image.

Basic operation and formulation : Image is break off one unit up, then one unit to the right, and all that lies outside that unit square is shifted back by the unit until it's within the square[17]. It can be expressed mathematically as,

$$\Gamma\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = \begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} mod\ 1 \quad (3)$$

Where gives the Cat Map transform over the original pixels x and y, generally for an NXN image,

$$\Gamma\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = \begin{bmatrix}1 & p_1\\ p_2 & p_1p_2+1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} mod\ N$$

$$\text{where } p_1, p_2 \in \mathbb{Z} \text{ and } p_1, p_2 \geq 1. \quad (4)$$

Eq. (1) is a special case of Eq. (2) when p1=p2=N=1.
These values of p are altered to increase the number of iterations so that original image can be retrieved. This approach uses Cat Mapping in two steps – (1) First step is being performed before embedding of data, in this step payload is iterated k times (k<n, where kth iteration gives the most distorted transformation of the payload and n is the number of iteration being performed to construct the original image) and (2) Second step performs extraction of original message from the retrieved distorted payload.
Ratnakirti Roy et al. [17] proposed mechanism is divided in two phases, Phase I) Payload Scrambling Algorithm: It finds kth iteration of Cat Mapping and apply on the input image which has the lowest similarity with the original payload. Embedding Algorithm: Embedding is done by using two approaches –matrix encoding[24] and LSB Matching(LSBM)[25].Matrix encoding embeds secret data into the cover image changing a minimum number of pixels and LSB Matching diminishes the POV (Pair Of value)effect of the LSB Replacement method. Stego image is then passed to the receiver for extraction. Phase II) Extraction : It is performed in a reverse manner of embedding process .Exhibits low probability of detection when subjected to X2-stetganalysis, embedding efficiency is improved by using matrix encoding). Diminishes POV effect of LSBM method, no Step Effect [26] as in PVD. Time Complexity of detection of edges, embedding and extraction algorithm is O (n).Space complexity of the proposed algorithm is O (n).

2.8 Adaptive Pixel Pair Matching

The basic idea of PPM is to use a pixel pair (x, y) as a reference co-ordinate, then search for a coordinate (x', y') in the pre-defined neighborhood set of this pixel pair, which depends on the given message bit such that f (x', y') =SB, where f is the extraction function and SB is the secret data bit in binary notation. Searched co-ordinate (x', y') replaces the pixel pair (x, y) to hide the secret message bit. Range of SB lies in the range of 0 and B-1 and of SB must be integer s lies between 0 and B-1.There is a condition that each integer must occur at least once and f (x', y') $\sum$ ϕ (x, y). For having low distortion values in ϕ (x, y) should be less. A best PPM method should fulfill following requirements 1) The number of co-ordinates in ϕ (x, y) should be exactly B 2) The value of f in these co-ordinates are mutually exclusive 2) ϕ (x, y) and f(x, y) is designed in a manner that the whole system is capable of hiding messages in any notational system so that the best value of B can be selected which ensures low distortion in the cover image. This method is proposed so that MSE can be minimized.

Encryption procedure find the minimum value of B which satisfies ⌞MXM/2 ⌟≥|SB| and convert SB into binary notational form then discrete optimization problem is solved to find B and SB. Calculation of f(x', y') is done in the next step such that f(x', y')=I,0≤i≤B-1 and then construct a random embedding sequence Q which is non repeatable by using key Kr . Message is embedded in two pixels of the cover image which are selected by using the value of Q.A modulus distance d is calculated between SB and f(x, y) by using the formula,

$$d = (SB - f(x, y)) \bmod B \quad (5)$$

The pixel pair (x, y) is then replaced with (x+xd, y+yd).Previous step is repeated until all the secret data bits are embedded. For extraction of secret data, scanning of pixel pair is done in the same order as in the embedding phase. Embedding sequence Q is constructed using key Kr. According to the embedding pixel Q two pixels (x', y') will be selected. Calculate f (x', y'), the result is the embedded bits. Previous two steps will be repeated till all the message bits are extracted. In the last step message bits are converted into binary format .Resultant is the secret data bits. Uses mapping technique with the help of pixel selection and pixel intensity method. There are several methods based on PPM like OPAP (Optical Pixel Adjustment Process), LSB (Least Significant Bit), DE (Diamond Encoding), EMD (Exploiting Modification Direction). DE is better than EMD in terms of payload by embedding data.

3. QUALITY PARAMETER ANALYSIS

3.1 MSE (Mean Square Error)

When secret data is embedded into an image, pixel values are modified which cause image distortion [27]. MSE is calculated to measure the quality of the image which represents mean square between original and stego image.It is computed by the eq.(6) given below,

$$MSE = \frac{1}{NXM}\sum_{i=0}^{N}\sum_{j=0}^{M}(p_{i,j} - p'i,j)^2 \quad (6)$$

Here MXM is the size of the image, pi,j and p'i,j represents pixel values of the original image and stego image respectively, which altogether represents reconstructed image . If mean square error is less that means stego image quality is better and large value denotes stego image contains distortion.

3.2 PSNR (Peak Signal to Noise Ratio)

It is one of the measure of image quality which is based on the pixel difference between two images[28].It is also known as SNR measure which is used to estimate the quality of cover in comparison to stego image. PSNR is calculated by the equation (7),

$$PSNR = 10\log_{10}\frac{S^2}{MSE} \quad (7)$$

Mean Square Error is required to calculate PSNR value and S denotes maximum possible pixel value of the image. If the value of

PSNR is exceeds 36 DB then the visibility of stego and cover image is same and cannot be identified by HVS.

4. CONCLUSION

This paper deals with several image steganography techniques and their contribution in information hiding domain. Some techniques are extended by researchers to overcome drawbacks of the existing technique. Quality parameter analysis is used to check efficiency, complexity (time and space), level of distortion etc. of stego image with respect to cover image.

5. ACKNOWLEDGEMENT

We would also like to thank Varsha, our friends, family members for their extreme support and blessings.

6. REFERENCES

[1] Anderson R.J.,“ Stretching the Limits of Steganography”, Springer Lecture, pp. Notes in Computer Science, vol.2 39-48, 1996.

[2] Westfeld A, J., Camenish et al., “Steganography for Radio Amateurs- A DSSS Based Approach for Slow Scan Television”, Springer-Verlag Berlin Heidelberg, pp. 201-215, 2007.

[3] Timothy J. Ross, Fuzzy Logic with Engineering Applications, Third Edition Paperback – March 1, 2010.

[4] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science(JGRCS), Volume 2, No. 4, April 2011.

[5] Diwedi Samidha et al., “Random Image Steganography in Spatial Domain”, IEEE,2013.

[6] C.V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, “Protecting Intellectual Rights: Digital Watermarking in the wavelet domain”, IEEE Int. Workshop Trends and Recent Achievements in IT, pp. 16-18, 2002.

[7] Adnan Abdul-Aziz Gutub , “ Pixel Indicator Technique for RGB Image Steganography”, JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 2, NO. 1, FEBRUARY 2010.

[8] Ankit Chaudhary et al., “A Hash Based Approach For Secure Keyless Steganography in Lossless RGB Images”, IEEE, Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 3-5 Oct. 2012.

[9] Gutub Adnan Abdul-Aziz. 2010. Pixel indicator technique for RGB image steganography. J. of Emerging Technologies in Web Intelligence. 2,1 (Feb. 2010), 56-64.

[10] Roy, Sankar. and Parekh, Ranjan. 2011. A Secure Keyless Image Steganography Approach for Lossless RGB Images. In Proceedings of ACM ICCCS-2011 (Rourkela, Odhisha, India, Feb. 11-12, 2011), 573-576.

[11] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel value differencing. Pattern Recognition Letters, 24:1613– 1626, 2003.

[12] R. Amritharajan, R. Akila, P. Deepikachowdavarapu, “A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Vol. 2, No.3, pp. 41-47, 2010.

[13] K.C. Chang, C.P Chang, P.S. Huang, and T.M. Tu, “A Novel Image Steganographic Method Using Triway Pixel-Value Differencing,” Journal of Multimedia, Vol. 3, No. 2, pp.37-44, June 2008.

[14] J.K. Mandal, Debashis Das “Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray Images through Exclusion of Underflow/Overflow ”, Computer Science & Information Series, ISBN : 978-1-921987-03-8, pp. 93-102, 2012.

[15] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” IEE Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.

[16] V.Nagaraj et al., “Color Image Steganography based on Pixel Value Modification Method Using Modulus Function”, International Conference on Electronic Engineering and Computer Science, Elsevier,2013.

[17] Ratnakirti Roy et al., “Chaos based Edge Adaptive Image Steganography”, Elsevier nternational Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

[18] Manglem Singh, Birendra Singh and Shyam Sundar Singh, “Hiding Encrypted Message in the Features of Images,”IJCSNS, vol. 7, no. 4, April 2007.

[19] H. C. Wu , N. I. Wu, C. S. Tsai, and M. S. Hwang, “ Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, no. 5pp. 611–615, 2005.

[20] Sonka, M., Hlavac, V. and Boyle, Image processing, analysis, and machine vision, Thomson Brooks/ Cole, 1999.

[21] Wen-Jan Chen a, Chin-Chen Chang, T. Hoang Ngan Le, “High payload steganography mechanism using hybrid edge detector,” Expert Systems with Applications, vol. 37, pp. 3292–3301, 2010.

[22] John Canny,"A computational approach to edge detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 8, No. 6,pp.679–698, Nov. 1986.

[23] V. I. Arnold; A. Avez , “Ergodic Problems in Classical Mechanics”, Benjamin, New York, 1968.

[24] Ron Crandall , “Some Notes on Steganography”, Posted on Steganography Mailing List, 1998. Source: http://www.dia.unisa.it/~ads/corsosecurity/www/CORSO-0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf.

[25] X. Li, B. Yang, D. Cheng, and T. Zeng, “A generalization of lsb matching”, IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009.

[26] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, “A Survey on Image Steganography and Steganalysis”, Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, April 2011, pp. 141-173.

[27] a. L. M. Jean-Bernard Martens, "Image dissimilarity", Signal Processing, vol. 70, no. 3, pp. 155-176, 1998.

[28] Yusra A. Y. Al-Najjar, Dr. Der Chen Soong, "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI",

International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012 ISSN 2229-5518.

[29] V. K. Yadav, et al. "Zero Distortion Technique: An Approach to Image Steganography on color images". In Proc. International Conference on Information and Communication Technology for Competitive Strategies, ICTCS '14, November 14 – 16 pages 79-83 (Published by ICPS-ACM, Proceedings Volume ISBN No: 978-1-4503-3216-3).

[30] V. K. Yadav, et al. "A Novel Approach of Bulk Data Hiding using Text Steganography". Accepted in Third International Conference on Recent Trends in Computing (ICRTC 2015) will be held in SRM University, NCR Campus, Modinagar, Ghaziabad, India during March 12th – 13th, 2015". Publisher: Elsevier Procedia Computer Science Journal.

[31] V. K. Yadav, et al. "Variable Text Generation: A Novel Technique to Generate Random Text" . In Proc. Sixth International Conference on Computational Intelligence and Communication Networks 2014, CICN 2014, pages 102-105 (Available at IEEE Xplore).

[32] V.K. Yadav, et al. "ICSECV: An Efficient Approach of Video Encryption". In Proc. Contemporary Computing (IC3), 2014 Seventh International Conference, 7-9 Aug. 2014, Pages: 425 – 430 (Available at IEEE Xplorer and DBLP, indexed by SCOPUS).

[33] V.K.Yadav, et al. "Zero Distortion Technique: An Approach to Image Steganography using Strength of Indexed Based Chaotic Sequence". In SSCC-2014, symposium proceedings published by Springer in Communications in Computer and Information Science Series(CCIS), Volume 467, 2014, pp 407-416, ISSN: 1865:0929.

[34] V.K.Yadav, et al. "Hiding Large Amount of Data using a New Approach of Video Steganography". In Proc. Fourth International conference Confluence 2013: The Next Generation Information Technology Summit, Sept 27-28, Page(s): 337 – 343 (available at IET and IEEE xplorer).

[35] V.K. Yadav, et al. "A New Video Encryption Algorithm Based on Indexed Based Chaotic Sequence". In Proc. Fourth International conference Confluence 2013: The Next Generation Information Technology Summit, Sept 27-28, Page(s): 139 – 143 (available at IET and IEEE xplorer).

[36] V.K.Yadav, et al. "CUIM: An Approach to deal with Fake Accounts on facebook" In Proc. Second International Conference on "Emerging Research in Computing, Information, Communication and Applications", ERCICA-2014, Volume-1, pages 675-680 (Publisher: Elsevier, ISBN: 9789351072607).

Table 4. Comparison of Several Image Steganography Techniques

Technique	Merits	Limitations
PIT	1) Low visual distortion when the rate of embedding is less than 3 bits. 2) Low susceptibility to histogram and visual attack at this rate.	1) Not recommended to exceed beyond 3-bit for acceptable secure systems because of transparency issues. 2) Blue channel is highly affected by the changes.
Hash Based	1) Secured randomized approach having better storage capacity up to 3.8 MB of data 2) Uses one-bit LSB to minimize the degradation of image quality. 3) To increase the storage capacity all color channels (RGB) has been utilized. 4) For security reasons lossless compression technique is being used on source secret message.	
PVD	1) Color image steganography based on PVD method is very helpful in solving the problem of overflow in pixel values of images. 2) Less visual distortion, not susceptible to histogram attack, embedding capacity is quite good.	Susceptible to histogram analysis of the difference of pixel pairs, sensitive to x^2attack, only one secret bit was embedded for two consecutive pixels, requires a range table.

PVM	1) Problem existing in PVD of overshooting 0-255 ranges for each component pixels has been removed i.e.no pixel value will exceed 0-255 range in stego image. 2) Embedding bits in different component matrix of RGB plane increases security, hiding capacity, improves the visual quality of the image. 3) Minimum changes in the histogram of cover and stego image 4) Less distortion in cover image, no range tables are required for extraction.. 5) One secret bit will be embedded in one pixel value only.	
ROI	1) Payload is being scattered throughout the cover image and it reduces the probability of detection of secret message for a steganalyst.	
Edge Based	1) To enhance security encryption is performed by using S-DES.	
Chaos Edge Adaptive	1) Canny's edge detection is highly immune to noise and is able to detect true weak edges. 2) Optimized and standard method for detecting edges in an image. 3) Ensures high fidelity and of the stego image and good imperceptibility to steganalysis attack.	
Adaptive PPM	1) Lower distortion than OPAP and DE method as the neighborhood set is compact and the digits can be embedded in any notational form. 2) Secure than OPAP and DE in case of steganalysis. 3) More messages can be embedded per modification which increases embedding efficiency. 4)MSE of APPM is lower than that of LSB,OPAP and DE.	