ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

An Efficient and Secure Data Hiding Technique – Steganography

Abhilasha Ramdas Bhagat[1], A. Prof. Ashish B Dhembhare[2]

PG Student, Dept. of Electronics & Telecomm., P.R.M.I.T & R, Badnera, Amravati, Maharashtra, India[1]

Assistant Professor, Dept. of Electronics & Telecomm., P.R.M.I.T & R, Badnera, Amravati, Maharashtra, India[2]

ABSTRACT: The technique to hide secret data in some carrier without any apparent evidence of data exchange is called as Steganography. The main goal of Steganography is to hide securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. Steganography is used to secretly communicate information between people. The propose of a framework for the detection of the least significant bit (LSB) steganography with the use of digital media files as cover objects. It can compute a robust estimate of the length of a secret message hidden in the LSBs of samples for a large class of digital media contents such as image, video, and audio, in which the signals consist of correlated samples. In the traditional steganography techniques principle was either to replace a certain part of the frequency components of the carrier image, or to replace all the least significant bits of a multi-valued image with the secret data. Our new steganography uses a video as the carrier data, and we hide secret information in the bit-planes of the carrier.

KEYWORDS: BPCS, carrier media, cryptography, data hiding, information hiding, steganography, stego audio, stego image, stego video.

I. INTRODUCTION

Text Steganography is defined as "secure hiding information technique within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected". Encryption provides an approach to information security, and encryption programs readily available. However, encryption clearly marks are a message as containing "secret data" information, and the encrypted message becomes subject to attack. Many cases it is desirable to send secret information without anyone noticing that information has been sent is secret information.

Steganography and Cryptography is sister in the data hiding techniques. Cryptography is the practice of scrambling or misplacing letters in a message in an undetectable form to prevent others from understanding it. Steganography is the study of obscuring the message so that it cannot be seen.

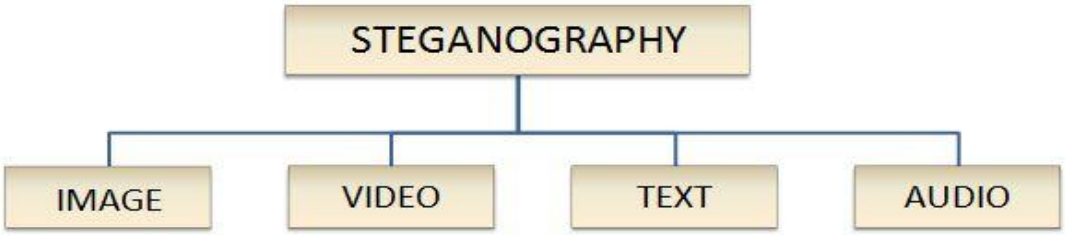

Fig 1 Types of Steganography

Steganography presents another approach to information security. In Steganography, data is hidden in a (carrier) vessel.

A) Types of Steganography
Fig.1.represents the steganography and its types as detailed below:
a) Image steganography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

A variety of vessels are possible, such as images, sound clips, video clips. In recent years, steganographic programs have been found on Internet home pages. Some of them use image data as a container of the secret information. This technique is called as image steganography.

b) Audio steganography
The methods in which data is hidden in sound files using properties of the Human Auditory System (HAS). Sound files consists of header and data bytes .The data bytes of sound files are the least recognized sound bits and are replaced by secret data . This technique is called as audio steganography. Hiding additional information into audio sequences is a more difficult task than that of images, due to supremacy of the HAS over human visual system [1]

c) Video steganography
Out of the above mentioned steganographic technique the capacity of storage of secret data increases in video steganography .The video comprised of image and audio. Video steganography enables to hide data in image as well as in audio and generate stego video. Other program hides the secret information in a specific band of the frequency component of the carrier. Some of the programs use sampling error in image digitization. However, all those Steganographic techniques are limited in terms of information hiding capacity.

d) Text steganography
Hiding secret information in text is the most important method of steganography. The method proposes to hide a secret message in every *mth* letter of every word of a text message. Text steganography using digital files is used to lesser extent as text files have a very small amount of redundant data.

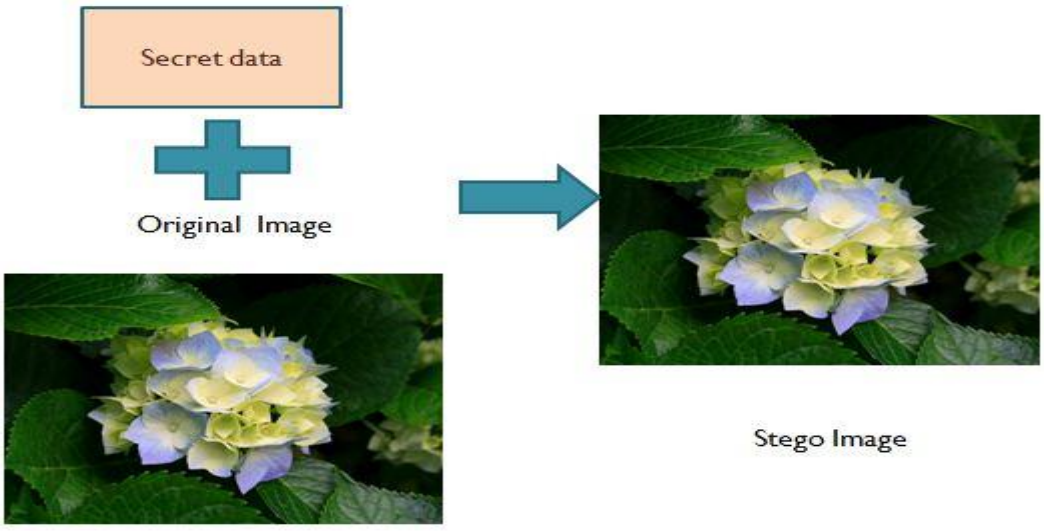

Fig 2: Generation of stego image

B) Model of Steganography
Fig.2.represents the formation of stego imagefrom the cover image.

Definitions:
Cover image: It is defined as the original image into which the required information is hidden. It is also called as carrier image. The information should be hidden in such a manner that there are no significant changes in the properties of the cover image.

Stego image: It is an image obtained by the combination of the secret information and cover image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Perceptibility: It is the ability of a not the intended recipient to visually detect the presence of hidden information in the stego image. The hiding algorithm is imperceptible when used on a particular image if an innocent third party, interested in the content of the cover image, is unaware of the presence of the secret information. This requires that the embedding process should not degrade the visual quality of the cover image.

Robustness: It describes the ability of the Secret information to survive the embedding and extraction process, even in the face of manipulations of the stego image such as filtering, cropping, rotating and compression.
Security: It is inability of an unauthenticated user to detect hidden images which are accessible only to the authorized user [2]. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when statistical properties of data of the cover and stego images are identical.

C) Key based Steganography

On the basis of keys the types of Steganography are of three types and these categories convey the level of security with which the stego message is embedded, hidden, transmitted and read.

1. Pure steganography
Pure steganography uses no keypad system to hide clear text or 'null cipher' text into the cover data in order to hide the presence of a secret message. It is the method which is less secure. In steganalyses, this method is the easiest way to detect since once detected the message can only have hidden in as many ways as the number of steganographical algorithms which exists.

2. Public key steganography
A public key steganography allows two unknown parties, who don't know each other or exchanged a secret data, to send hidden messages over a public channel so that an unauthenticated user cannot even detect that these hidden messages are being sent. Generally, two parties (authenticated users) wishing to communicate steganographically, without agreement on a secret key. In this principle we have two keys, one is the public key which can be obtained from public and other a private key. Public key is used for encryption process and private key is used for decryption process as represented in Fig.3.

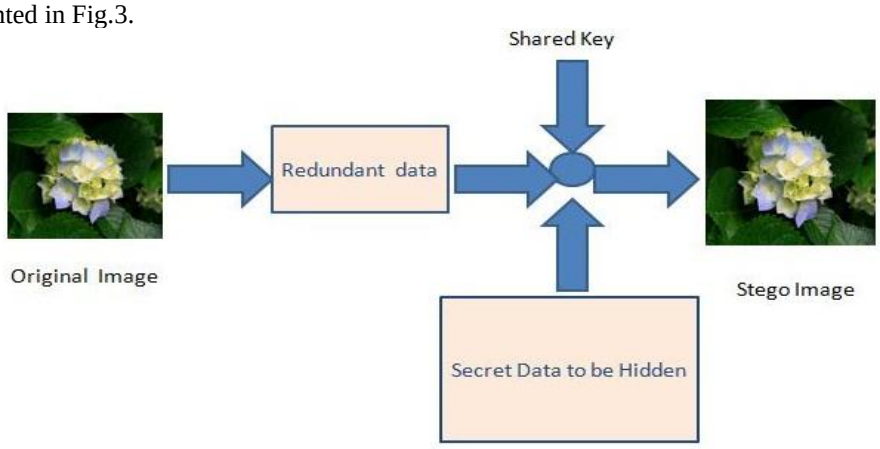

Fig 3: Block diagram of public key steganography

3. Private key steganography
A private key steganography enables two unknown parties with a shared secret key to send hidden messages unrecognizable manner over a public channel. This can be used if the two parties communicating trust each other completely. The block diagram of private key steganography is shown in Fig.4.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

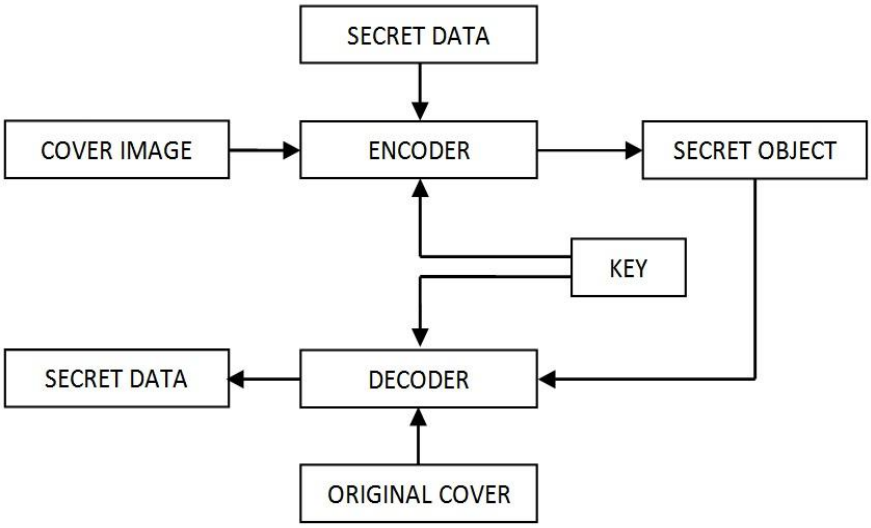

Fig 4: Block diagram of private key steganography

II. RELATED WORK

Steganography has been an active research topic for decades and review of all the text detection methods is impossible. So some papers related to the proposed system are mentioned as below:

Park et al., [3], has proposed an image steganography method uses AC coefficients of the Discrete Cosine Transform (DCT) domain to verify the secret information that is hidden in a spatial domain of the Carrier image had been remove, replaced, forged or changed by attackers. LIU Tong and QIU, Zheng-ding [4], have presented a method that hide the secret data or message into a color image by the quantization based Steganography in which it guarantees the transportation of the secret data which will not attract the attention of eavesdropper. In this method the original RGB image was transformed to YCbCr to use the perceptual masking function of YCbCr components; since the marked strength is matched according to the human visual system. The perceptual quality of the watermarked image is not severely deteriorated. The hidden message could be reliably extracted without degrading original image.

G. Mastronadi et al., [5], proposed the effects of Steganography in various image formats viz., GIF, BMP, JPEG, etc. With the use of different formats, an idea of how bits of textual secret data can be hidden without perceptually deteriorating the quality of the image and also gives the idea of where to inject the embedding bits in order to achieve the best result in terms of length of the textual message and maintain quality of the image. J. Fridrich et al., [6], has proposed the analyses of the security of Least Significant Bit (LSB) for hiding messages in high-color-depth images frame. They have pointed a steganographic attack that is stego-only attack. The method makes us able to detect the existence of pseudorandom message randomly spread in a color image with reliability based on statistical analysis of the image colors in the RGB pixel.

L.M. Marvel et al., [7], have explored a method of embedding data within image frame .Combing Steganography, spread spectrum communication, error control coding and Image processing the secret information is embedded within the noise, then added to the Image frame. The noise is kept at low levels so that it is not perceptible to human eye and recognizable to detection by computer analysis without access to the original image. N. F. Johnson and Sushil Jajodia [8], have explored a method to detect the presence of hidden message and also to find the location of the hidden information that was hidden in the cover image. Chin-Chen Chang et al., [9], have described a pattern based image Steganography (PBIS) in which first the Discrete Wavelet Transformation is done on the image frame, separating the overlapped blocks and then classifies the wavelet coefficients of these overlapped blocks into a various patterns. The secret data or information is embedded into the digital image by altering the coefficient patterns.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

C. Manikopoloulos et al., [10], have proposed a Steganography detection system (SDS) and its application to the detection of block DCT-based Steganography in gray-scale images, segmenting into 8x8 blocks. The differences of coefficients of the block DCT transforms of the watermarked / unwatermarked images from the original are treated as features. The Steganography detection system makes use of statistical preprocessing, over an observable region of each image that produces feature vectors over the regions. The vectors are then fed in a simple neural network classifier.
R. Chandramouli [11], proposed two algorithms: coordinated search and random search in the optimization framework. These covert channels are reason of security concern because they can be used to pass malicious messages. These messages could be in the form of computer viruses, terrorist messages, spy programs, etc. Ying Wang and Pierre Moulin [12], have presented a steganalyses of a block-DCT image Steganography in which information is embedded in 8 x 8 block-DCT coefficients. Because of the block structure of DCT , pairs of neighboring pixels within an 8 x 8 block have difference in statistics from those across two 8 x 8 blocks. Two histograms of differences of pixels are computed (one for each Population), from which a Kolmogorov-Smirnov (K-S) binary hypothesis test is derived for deciding whether a given image frame is a stego-image or a cover-image. The non-stationary block-DCT Steganography reveals the presence of hidden information .The differences between the distribution of pixel pairs from one block and across blocks provides a measurement for the detection of stego-images. The steganalyses method gives better result for smooth images than for noise-like images.

Vidyasagar M. Potdor and Elizabeth Chang [13], presented a steganographic algorithm in which the secret information or the message is hidden into the carrier vessel by modifying the grey *m* level values of the grey scale image pixels. Thus the steganographic algorithm enables secret communication, to recover hidden information within the spatial domain of the image along with low computational Complexity and high information hiding capacity.

III. PROPOSED SYSTEM

A) *LSB algorithm*
A simple way of steganography is based on replacing the least significant bit layer of images, known as the LSB technique. In the LSB (least significant bits) technique, the LSB of the pixels of the images frame of video is replaced by the message which bits are permuted before embedding. In some cases, LSB of pixels are arranged in random or in certain areas of image frames of video and sometimes increment or decrement the pixel value.

In [14] LSB technique, the LSB of the pixels of image frame of video is replaced by the message to be sent. The message bits are processed before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified. Popular steganographic tools based on LSB embedding vary in their approach in terms of hiding information. Some of the algorithms can change LSB of pixels visited in a random walk, others modify pixels in spatial areas of images, or instead of just changing the last bit they increment or decrement the pixel value.
Another way for hiding in spatial domain in this method, noise that statistically resemble common processing distortion, e.g., scanner noise, or digital camera noise, is made available to pixels on a random walk of image . The noise is generated by a pseudo random noise generator using a shared key. A *parity function* is defined to embed and detect the message signal modulated by the generated noise. Least significant bit (LSB) insertion is a common, easiest approach for embedding information in a cover image. The least significant bit (in other words, the 8th bit) of the bytes inside an image is changed to a bit of the secret message. While using a 24-bit image, a bit of each of the red, green and blue color components are used, since they are each represented by a byte. One can store 3 bits in each pixel.

(00101101 00011100 01011100)
(10100110 11000110 00001100)
(11010010 10001101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image frame, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

(11010001**0** 10101100**0** 01100011)

The number was embedded into the first 8 bytes of the block, only the 3 highlighted bits needed to be changed according to the embedded or hidden message. Only half of the bits in an image will need to be modified or replaced to hide a secret message using the maximum cover size. The image consists of 256 possible intensities of each primary color, changing the LSB of a pixel results in little changes in the intensity of the colors. These changes cannot be perceived or recognized by the human eye - thus the message is successfully hidden. With a chosen image, one can even hide the message in the least as well as second to least significant bit and still not recognize the difference .In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to hide the secret information. This approach is very easiest to detect. A little more secure system is for the sender and receiver to share a secret key that specifies only certain pixels are to be changed. Should an unauthenticated user suspect that LSB steganography has been used, he is unable of knowing which pixels to target without the secret key.

In its simplest form, LSB uses BMP images, since they use lossless compression. Unfortunately unable to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels size are rarely used on the Internet and might arouse suspicion. For this reason, LSB steganography has developed for use with other image file formats. In steganography, data is embedded inside a vessel or container that looks like it contains only something else. A variety of carrier vessels are available, such as digital images, sound clips, and even executable files.

All of the available steganographic techniques have limited information-hiding capacity. They can embed only 10% (or less) of the data amounts of the vessel. This technique uses an image frame from video as the vessel data, and we embed secret information in the bit-planes of the vessel. We can replace all of the "noise-like" regions in the bit-planes of the vessel image frame of video with secret data without deteriorating the image quality .This video is called as stego video. We termed our steganography "BPCS" which stands for Bit-Plane Complexity Segmentation steganography.

B) Mechanism

i) Proposed BPCS Steganography Algorithm

Bit Plane Slicing Concept in BPCS: Here we are using the bit plane slicing concept. The bit plane slicing can be explained with the help of Fig 3 .The operation of splitting the image into the binary planes is called "Bit plane slicing". Pixels are digital numbers which are composed of bits. In an 8-bit image, intensity of each pixel is represented in form 8-bits. The 8-bit image is comprised of eight 1-bit plane regions from bit plane "0" (LSB) to bit-plane "7" (MSB). Plane "0" containing all lowest order bits of all pixels in the image while plane "7" containing all higher order bits. Bit plane Slicing is very useful for image compression. Complexity of each bit–plane pattern increases from MSB to LSB. Fig.5. represents the bit plane decomposition of image frame.

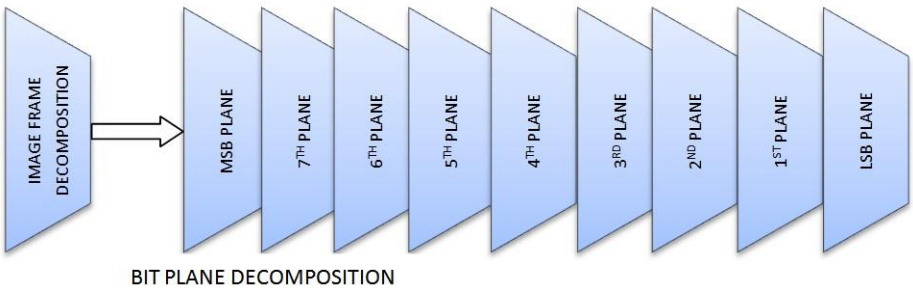

Fig 5: Binary pixel blocks on bit-planes and decomposition

ii) The definition of image complexity

The length of the black-and-white border in a binary image is a good measure for calculating image complexity. If the border is long, the image is more complex, otherwise it is simple. The total length of the black-and-white border is the summation of the number of color-changes along the rows and columns in an image. Take an example; a single black

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

pixel surrounded by white background pixels has the boarder length of 4. We will define the image complexity α by the following.

$$\alpha = \frac{k}{(\text{The max.possible } B-W \text{ changes in the image})} \quad \text{.....(1)}$$

Where, k is the total length of black-and-white border in the image frame of video. The value ranges over $0 \leq \alpha \leq 1$. Image complexity (α) is calculated for the whole image area. It gives us the complexity of a binary image frame of video. However, we can also use α for a local image complexity.Fig.4. represents the binary pattern of pixel of image.

iii) Conjugation of a binary image

Let Q be an 8X8 size black-and-white image frame of video with black as the foreground area and white as the background area. Now we will introduce two checkerboard patterns of Wc and Bc, where Wc has a white pixel at the upper-left position, and Bc is its complement, i.e., the upper-left pixel is black. We describe black and white pixels as having a logical value of 1 and 0, respectively.

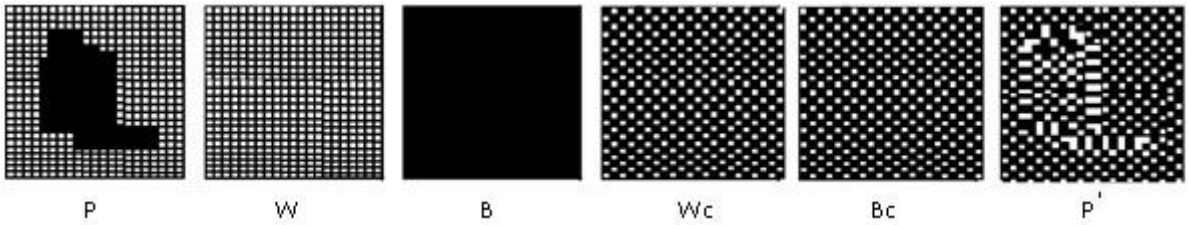

Fig 4: Illustration of each binary pattern

Q is interpreted as follows. Pixels in the foreground area consist of B pattern, while pixels in the background area consist of W pattern. Now we define Q* as the conjugate of Q. The most important property about conjugation is the following. Let α (Q) be the complexity of a given image Q, then we have, α (Q*) = 1- α (Q).

The complexity value of Q* is always symmetrical against Q assuming α = 0.5. For example, if Q has a complexity of 0.7, then Q* has a complexity of 0.3.Replace complex image-data block to message block (secret data).

IV. SYSTEM ARCHITECTURE

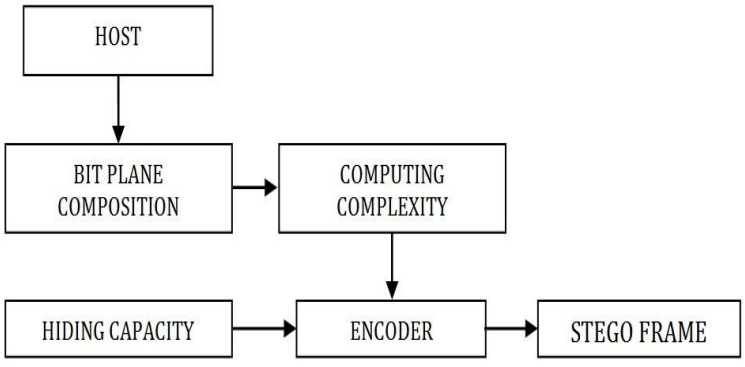

Fig 7: Stego-encoder

Fig.7. represents the block diagram of stego encoder in which the image frame of video is decomposed into planes and complexity of each plane is calculated using (1). More complexity of frame more data can be embedded in carrier. Thus the frame generated is called as stego frame.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

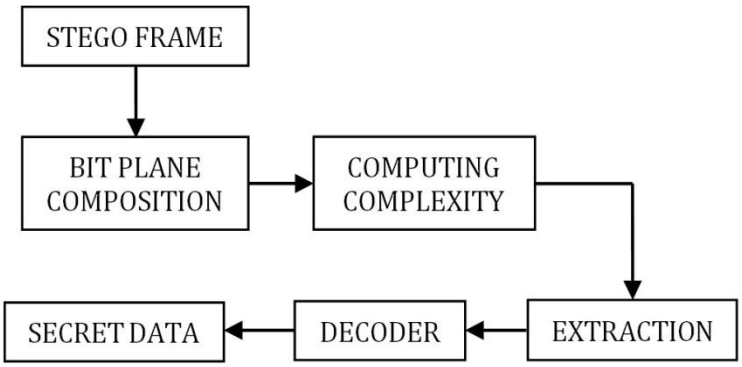

Fig 8: Stego-decoder

Fig.8.represents the block diagram of stego decoder in which the stego frame is decomposed into bit plane and complexity of each bit plane is calculated and the secret data embedded in frame is extracted.

V. RESULTS AND DISCUSSION

Analysis of the steganographic techniques dealt with the performance parameters such as security level, hiding capacity of BPCS algorithm was better than LSB steganography .It is proposed to obtain a better PSNR, BER using the proposed BPCS algorithms.

VI. CONCLUSION

We have demonstrated BPCS-Steganography, which proposes the property of the human visual system with existing LSB steganography technique. BPCS-steganography increases the level of security and hiding capacity. Gray coding provides a better way of identifying which regions of the higher bit planes can be embedded. Thus it guarantees secret and secure internet communication. We observed that this steganography is a very strong information security technique, especially when in combination with encryption embedded data. Future research will include the application to vessels other than colored images, identifying and formalizing the customization parameters, and developing new applications for increasing hiding capacity of carrier.

VII. ACKNOWLEDGEMENT

I would like to present my honest gratitude to Prof. Ashish .B. Dhembhare for his immense support and guidance throughout the work.

REFERENCES

1. N. Johnson and S. Jajodia," Exploring steganography: seeing the unseen", IEEE Computer, pp.26-34, feb-1998
2. A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images," in IEEE Signal Processing Letters, vol. 12, pp. 116–119, June, 2005.
3. K. Y. Youngran Park, Hyunho Kang and K. Kobayashi, "Integrity verification of secret information in image steganography," The 20th Symposium on Information Theory and its Application, vol 9, no 2, pp. 182–185, Nov 2006.
4. L. Tong and Q. Zheng-ding, "A DWT-based Color Image Steganography Scheme," in International Conference on signal Processing, vol. 2, pp. 1568–1571, Feb 2002.
5. M. C. Giuseppe Mastronardi and F. Marino, "Steganography Effects in Various Formats of Images," in International Workshop on Intelligent Data Acquisition and Advanced computing systems: Technology and Applications, vol 2, issue 1, pp. 116–119, July 2001.
6. R. D. Jiri Fridrich and M. Long, "Steganalysis of LSB encoding in Color Images," in International Conference on signal Processing, pp. 1279–1282, Jan 2000.
7. C. T. R. Lisa M. Marvel and C. G. Boncelet, "Hiding Information in Images," in International Conference on Image Processing, pp. 396–398, Mar 1998.
8. N. F. Johnson and S. Jajodia, "Steganalaysis: The investigaton of Hidden information," in International Conference on Information Technology, vol 58, no 18 pp. 113–116, Jun 1998.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

9. C.-C. C. Tung-Shou Chen and H.-C. Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transformation and Pattern based Modification," in International Conference on Computer Networks and Mobile Computing, pp. 115–119, Mar 2003.
10. Y.-Q. S. Z. N. Constantine manikopoulos, Zheng Zhang and D. Zou, "Detection of Block DCT based Steganography in Gray-scale Images," in International Conference on Image Processing, vol 97, no 18, pp. 355–358, Feb 2002.
11. R.Chandramouli, "Web Search Steganalysis: Some Challenges and Approaches," in ISCAS, pp. 576–579, April 2004.
12. Y. Wang and P. Moulin, "Staganalysis of Block DCT Image Steganography," in International Conference on Image Processing, pp. 339–342, Mar 2003.
13. V. M. potdar and E. Chang, "Gray Level Modification Steganography for Secret Communication," in 2nd International Conference on image Processing, pp. 223–228, April 2004.
14. R. D. Jiri Fridrich and M. Long, "Steganalysis of LSB encoding in Color Images," in International Conference on signal Processing, pp. 1279–1282, Jan 2000.
15. R. J. Anderson and A. P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp.474-481
16. M. Kharrazi and N. Memon. Image steganography and steganalysis: Concepts and practice. Pages 35–49, 20031 Shrikant Khaire "Steganography Bit Plane Complexity Segmentation (BPCS) Technique", IJEST 2010
17. A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images," in IEEE Signal Processing Letters, vol. 12, pp. 116–119, June, 2005.
18. G. J. Simmons, "Results Concerning the Bandwidth of Subliminal Channels," lEEE J. on Selected Areas in Communications, vol. 16, no. 4, pp, 463473
19. A. I. Hashad and A. S. Madhan, "A Robust Steganography Technique using Discrete Cosine Transform Insertion," in International Conference on Information Technology, pp. 255–264, April 2003.
20. R. D. Jiri Fridrich and M. Long, "Steganalysis of LSB encoding in Color Images," in International Conference on signal Processing, pp. 1279–1282, Jan 2000.