SURVEY OF IMAGE STEGANOGRAPHY USING SPATIAL DOMAIN TECHNIQUES

Anjli J Patel, Ms. Jayna B.Shah
Dept of computer engineering
Sardar Vallabhbhai Patel Institute of Technology, Vasad-388306, Gujarat, India

Abstract- **Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. This paper discusses existing BPCS (Bit Plane Complexity Segmentation) steganography technique. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. This algorithm offers higher hiding capacity due to that it exploits the variance of complex regions in each bit plane. In contrast, the BPCS algorithm provided a much more effective method for obtaining a 50% capacity since visual attacks did not suffice for detection. We termed our steganography "BPCS-Steganography," which stands for Bit-Plane Complexity Segmentation Steganography.**

***Index Terms*—** **BPCS, carrier image, Data security, Information hiding, Steganography, Stego image.**

I. INTRODUCTION

In recent years, information security is in major part of this digital world. Computers and the internet is major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of Cryptography and steganography schemes. Steganography is a powerful security tool that provides a high level of security, particularly when it is combined with encryption.

Information hiding has become a hotspot in the research field of information security. Through embedding unnoticeable secrets into digital media signals such as images, audio and video, information hiding realizes the function of copyright protection and secret communication. Information hiding mainly consists of two main branches, which are digital cryptography and steganography.

Steganography differs from cryptography. The goal of cryptography is to secure communications by changing the information into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information will not be detectable [1][2][3]. A steganography system consists of three elements: carrier object which hides the secret message, the secret message and the stego object which is the cover object with message embedded inside it. There are different types of techniques of steganography which are depends on which types of carrier object used for stenography purpose. For example text, image, network protocol, audio or video.

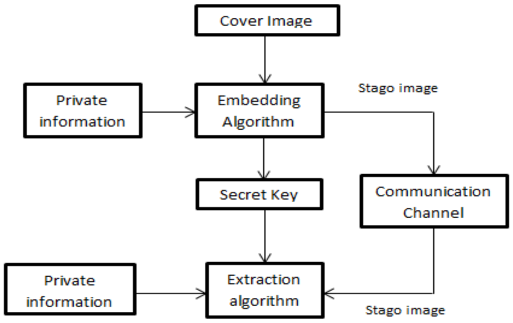

Fig.1. Generic form of image Steganography

As shown in figure 1 this is the simple flow of steganography technique. As shown in figure by using embedded algorithm private information are embedded in cover image so after embedding process stego image created. This stego image transmitted through communication channel and at receiver side authorized person can extract private information.

To clarify the idea of steganography, the three famous characters named Alice, Bob and Ward are used [4]. Alice (A) wants to send a secret message (M) to Bob (B). Bob must receive it safely without raising suspicion. To do that, Alice changes the message (M) into a steganography object (stego-object, i.e. new file carrying the embedded-object) (S). Stego-object is created by covering the message (M) with another random harmless message to produce a cover (C, i.e. data file that will hold the secret message). Covering the massage (M) with message (C) happens by using a secret key (stego-key) (K). Now Alice should be able to send the stego-object (S) to Bob without being detected by Ward. When Bob receives (S) he will use the stego-key (K) which he already knows to reproduce secret message (M) from the cover message (C) and be able to read it. Steganography have to guarantee these requirements:

- Robustness: information is robust when it is embedded inside an image and although it disappeared behind it but it is not destroyed, it is present, but is only detected with reliability after modifying the image.
- Undetectability: the data hidden under an image cannot be detected as long as the cover image is not doubtable or suspicious and looks unchanged.
- Perceptual transparency: this requirement depends on human visual and audio system. If the hidden data didn't raise the attention of human systems and no one could distinguish whether the cover contains secret data then this requirement is guaranteed.
- Security: as long as no one other than the legal receiver can remove the embedded data from behind cover, the embedding algorithm is said to be secure. This requirement assures that no targeted attacks can detect or view the hidden message unless they have a full knowledge of the embedding algorithm.

This paper will first outline BPCS steganography concept and principle. Then descriptions about BPCS embedding and extraction technique for digital images will explain. In this paper, we use uncompressed image as a carrier image or base image to hide any information. Any compressed image may be lossy or lossless compression. If compressed image is lossy then we lost our nearly 25% of hidden information because of result in a significant reduction of the file size [13]. BPCS technique explains in brief in this paper.

II. IMAGE STEGANOGRAPHY TECHNIQUES

Image steganography can be broadly classified into spatial domain, transform domain, spread spectrum and model based steganography as depicted in Figure2.In spatial domain, secret message is embedded in pixel value directly [13].

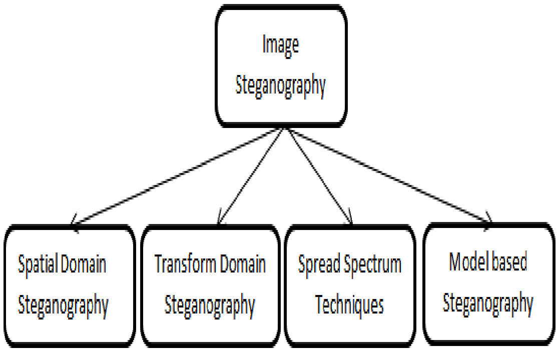
Image Steganography
Spatial Domain Steganography
Transform Domain Steganography
Spread Spectrum Techniques
Model based Steganography

Fig.2Image steganography techniques

Spatial Domain Techniques: Spatial domain techniques include bitwise manipulation of intensity of pixels and noise manipulation. There are various approaches to embed data in spatial domain. Most commonly used and simple techniques for spatial domain are Least Significant Bit (LSB) Methods [15].

1. Least Significant Bit substitution

Embedding can be achieved by simply replacing LSB of the randomly selected pixel in the cover image with the secret message bit. Let Pi is the pixel value of an image. It can be expressed in binary form as follows:

$Pi=(b0, b1, b2, b3, b4, b5, b6, b7)^2$

Where*b7* is MSB and is b0 LSB. The biggest advantage of the LSB substitution method is the simplicity [13].

2. Optimal Pixel Adjustment Procedure (OPAP):

The OPAP scheme was developed as an improvement over the LSB based algorithm. The OPAP scheme modifies the embedded bits in order to improve the overall visibility of the stego image. The adjustment is done on the basis of the pixel differences between original pixel p_i and the pixel p_i' of the stego-image. If the difference is δ_i then depending on it pixel modification is done on the pixels before the embedded pixel so as to minimize the difference between the original pixel and the embedded stego pixel.

3. Pixel Value Differencing:

In the Pixel Value Differencing or PVD scheme number of insertion bits in PVD depends on whether the pixel is an edge or a smooth area. Human Visual System is sensitive to subtle changes in the smooth areas as compared to the edges. This is primarily because the difference between pixels in the smooth areas is much less as compared to that between the edge pixels and embedding in edge pixels causes less visual distortion. PVD does not cause much visual distortion and neither it is directly susceptible to the histogram attack as the LSB substitution. It is however susceptible to histogram analysis of the differences of the pixel pairs and χ^2*-attack.*

4. SLSB:

The Selected LSB algorithm or the SLSB proposed in embeds into single color components of the pixels. It does not necessarily embed into the LSBs only but chooses the color plane and the modifiable bits of the color plane in such a manner that will produce the minimum distortion. It falls in the category of the filtering algorithms as it applies a sample pair analysis filter before embedding to ensure that only the best candidate pixels are selected for embedding. It can embed at a rate of more than 1 bit per pixels. This however might lead to alteration of the degree of randomness of the pixels of the image and thereby makes it susceptible to statistical attacks when used for high degree of embedding.

5. BPCS (Bit-Plane Complexity Segmentation Steganography):

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason. BPCS is the development of LSB method, and it has better performance than the simple LSB method. The major idea is that multiple bit-planes of the cover images are divided into fixed-size blocks. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern.

Domain	**Algo**	**Security Level**	**Capacity (bpp)**	**Image Support**	**Complexity**
Spatial	LSB	L	1-3	Lossless	L
	OPAP	M	1	Lossless	M
	PVD	M	>1	Lossless	M
	SLSB	M	1-3	Lossless	M
	BPCS	H	>1	Lossless	M

*L=Low, M=Medium, H=High, VH=Very High

TABLE I. 1PARAMETER BASED COMPARISON

Techniques	**Mechanism**
LSB	Substitute the LSB
OPAP	Adjust the pixels before the embedded pixels for better visibility
PVD	Embeds data in difference of neighboring pixels (edge and smooth)
SLSB	Embeds data in the color component which has maximum variation
BPCS	Substitute both LSB and MSB. BPCS use of the characteristics of the human vision system.

TABLE II. MECHANISM OF DIFFERENT SPATIAL DOMAIN TECHNIQUES

Techniques	**Advantages**	**Disadvantages**
LSB	It is simple technique.	We can substitute up to 4 bits but image quality can be destroyed.
OPAP	After embedding process quality of stego image is improved.	When an image having large areas with same color shades are used as cover image, change in pixel can be easily detected in OPAP.
PVD	The capacity is increased and after embedding process the quality	This technique not support lossy image.

	distortion is lower.	
SLSB	It will produce the minimum distortion of cover image as possible.	Change lsb bit only in one color bit plane so the capacity is lower.
BPCS	Hiding capacity of color image is approx. 50%.	More complex cover image is required, and it is not robust.

TABLE III. ADVANTAGES AND DISADVATAGES OF DIFFERENT SPATIAL DOMAIN TECHNIQUES

III. BPCS STEGANOGRAPHY CONCEPT

BPCS [5] stands for Bit-Plane Complexity Segmentation Steganography. BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason. BPCS is the development of LSB method, and it has better performance than the simple LSB method. The major idea is that multiple bit-planes of the cover images are divided into fixed-size blocks. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern; therefore, we can replace all of the “noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. So this method has better visual imperceptibility. Besides, for the secret can be embedded in several bit-planes, compared with the LSB method it has greater data embedding capacity [6].

All of the traditional steganography techniques have limited information-hiding capacity. They can hide only 10-15% of the data amounts of the carrier. This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multi valued image with the secret information. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. In this technique, first the carrier image is divided into two regions “noisy-like regions” and “informative regions”. Informative images are simple, while noise-like images are complex. we can replace “noisy-like region” of the bit plane of carrier image with secret information without destroying image quality BPCS steganography is same like LSB technique but difference is LSB technique hide data in last four bits i.e. only in the 4 LSB bits while BPCS technique hide data in MSB plane along with the LSB planes provided more storage and embedding data.

The merits of BPCS steganography are as follows:

(1) Approx. information hiding capacity of color image is 50%.

(2) A sharpening operation on the carrier image increases the embedding quite a bit.

(3) Canonical Gray Coded (CGC) bit planes are more suitable for BPCS steganography than Pure Binary Coded (PBC) bit planes.

(4) Data compression and encryption operation on secret data makes the embedded data more intangible.

3.1 Bit-Plane Decomposition of a Multi-Valued Image [7]

A multi-valued image (P) consisting of n-bit pixels can be decomposed into a set of n binary pictures. For example, if the image is an n-bit gray image, it is shown as, P= [P1, P2..., Pn].

In case the image is a Red, Green, Blue color picture, it is shown byP=[PR1,PR2,..,PRn,PG1,PG2,..,PGn,PB1,PB2,..,PBn],

Where PR1, PG1, PB1 are the most significant bit-planes (MSB), while PRn, PGn, PBn are the least significant planes (LSB).

3.2 PBC to CGC conversion [7]

In BPCS-Steganography embedding operation is executed after the vessel image has been transformed from PBC to CGC. This is because CGC is better than PBC in producing a "better looking (or, blocking-less)" stego image. The reason is as follows. For example,

Let "n-th least plane" be the n-th Least Significant bit-plane. (For example, the 3rd least plane in PBC as above is the b2 bit-plane.)

"Embedding a file-block in an n-th least PBC plane" actually means "changing the colors of several pixels in that block by the value 2n-1 "uniformly.”

If a bit in the 3rd least plane is changed from "0" to "1", it actually changes 0 (= 0000)−> 4 (= 0100),

$1\ (= 0001) -> 5\ (= 0101),\ 2\ (= 0010) -> 6\ (= 0110),\ 3\ (= 0011) -> 7\ (= 0111), and\ 8\ (= 1000) -> 12\ (= 1100), \ldots$. The amount of the change is always 4, and will cause a blocking effect.

While in the CGC embedding, the color change "differs pixel by pixel" in the block ranging from 1 to 2n-1. The average change in the block is 2n-1.

The change occurs like,$0\ (= 0000) -> 7\ (= 0100), 1\ (= 0001) -> 6\ (= 0101), 2\ (= 0011) -> 5\ (= 0111),\ 3\ (= 0010) -> 4\ (= 0110), and\ 12\ (= 1010) -> 11\ (= 1110), \ldots$ .The amount of the change in this case differs case by case, but the average is 4. This will not produce a blocking effect remarkably.

Consequently, we conclude that CGC is better than PBC.

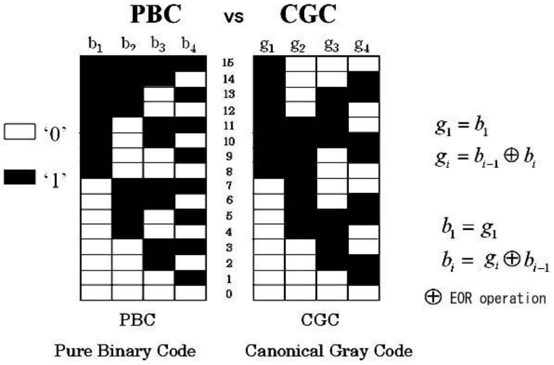

Fig.3 PBC vs CGC in Binary Image

3.3 The complexity of binary images

There is no standard definition of image complexity. Niimi and Kawaguchi discussed this problem in connection with the image threshold problem, and proposed three types of complexity measures [8][9][10][11].The different methods to find complexity of binary images are used to create segment between "informative" and "noise-like" image. First by applying bit slicing algorithm we can get n-bit planes as shown in fig 4. Then by using different types of complexity measure method we can find complexity in accurate way. BPCS-steganography adopts black-and-white border complexity method explained next.

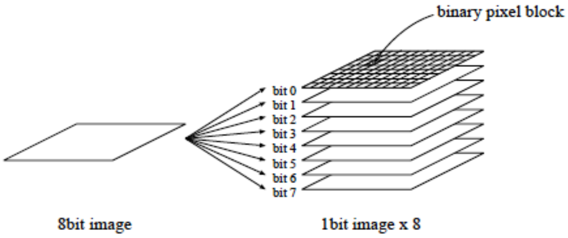

Fig.4. Binary pixel blocks on bit-planes

3.3.1 Black-and-White Border Complexity Measure

The length of the black-and-white border in a binary image is a good measure for image complexity. If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4.

We define the image complexity as

$$\alpha = \frac{\mathrm{k}}{\text{The max. possible B} - \text{W pixel changes in image}}$$

Where, k is the total length of B-W border in the image. So, the value range of α over $0 \le \alpha \le 1.$

For binary image, minimum border length is 0. The equation for maximum length of the border for $2^n \times 2^n$ binary image is given by $2 \times 2^n \times (2^n - 1)$.

Thus, image complexity is also given by

$$\alpha = \frac{k}{2 \times 2^n \times (2^n - 1)}$$

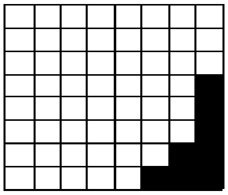

Fig.5. a simple block

For example, $2^3 \times 2^3$ (8×8) block in fig. 5 contain maximum border $= 2 \times 2^3 \times (2^3 - 1) = 112$ and total border of image = 8. Thus, $\alpha = \frac{8}{112}$ is complexity of image block.

3.4 Conjugation of a binary image

In BPCS, we need to perform segmentation of noise-like regions and informative regions. Informative patterns are look like simple pattern, while complex regions are very complex part of our image. If secret data is noise-like then it is directly embedded in noise-like regions of the vessel image. If secret data is informative then it has to undergo conjugation operation in order to transform it to complex pattern. Let P be a $2^n \times 2^n$ size black-and-white image with black as the foreground area and white as the background area. W and B denote all-white and all-black patterns, respectively. here two checkerboard patterns are introduce Wc and Bc, where c has a white pixel at the upper-left position, and Bc is its complement, i.e., the upper-left pixel is black. We regard black and white pixels as having a logical value of “1” and “0”, respectively.

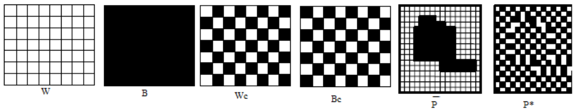

Fig.6. Binary plane patterns

Conjugation operation is kind on XOR operation image with Wc and Bc. Let P is binary image and conjugation operation with Wc create P*. Correspondence between P and P* is one-to-one. There are certain property of P and P* as follow.

1) P* = P ⊕ Wc

2) (P*)* = P

3) P*≠ P

4) $\alpha(P^*) = 1 - \alpha(P)$

IV. BPCS STEGANOGRAPHY ALGORITHM

We termed our steganography “BPCS-Steganography,” which stands for Bit-Plane Complexity Segmentation Steganography. BPCS makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the “noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality.

In BPCS-steganography, uncompressed image file like BMP file format is used for carrier image. We segment each secret file to be embedded into a series of blocks having 8 bytes of data each. These blocks are regarded as image patterns. We call such blocks the secret blocks.

The steps for encoding algorithm (i.e. to hide private information in carrier image) in BPCS-steganography:

1. The carrier (color) image is divided into 24 different bit-planes, which create binary image for all 24-bits.

2. Transform all 24 bit-planes of carrier image from PBC to CGC system. Then all the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as 8 × 8 bits.

3. Segment each bit-plane of the carrier image into “informative” and “noise-like” regions by using a threshold value (α_0).

4. Group the bytes of the secret file into a series of secret blocks.

5. Embed each secret block into the noise-like regions of the bit-planes.

6. If a block (let say P) is less complex than the threshold (α_0), than conjugate it to make it a more complex block (P*). The conjugated block must be more complex than α_0.

7. If the block is conjugated, then record this fact in a “conjugation map”. This Make a record of the blocks that have taken conjugate processing, and this information also need to be embedded into the carrier.

8. Also embed the conjugation map as was done with the secret blocks.

9. Convert the embedded carrier image from CGC to PBC.

The decoding algorithm (i.e. to extract original private information from stego image) is just the reverse procedure of the embedding steps. The process of secret information extraction is simple. Firstly, pick up all the pieces of the carrier data whose complexity is greater thanα_0, and then pick up the extraembedded information mentioned in step (7) to confirm theblocks that have taken conjugate processing. These blocksneed take XOR operation with tessellated chock to get therecovery of secret.

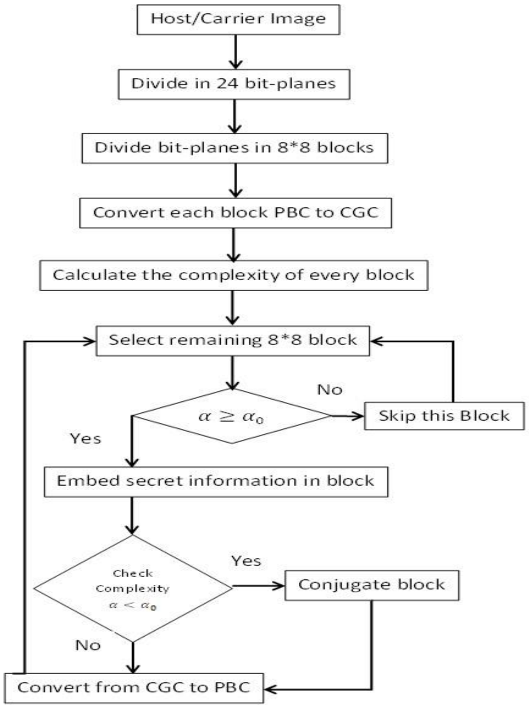
Host/Carrier Image
Divide in 24 bit-planes
Divide bit-planes in 8*8 blocks
Convert each block PBC to CGC
Calculate the complexity of every block
Select remaining 8*8 block
$\alpha \geq \alpha_0$
No
Skip this Block
Yes
Embed secret information in block
Check Complexity $\alpha < \alpha_0$
Yes
Conjugate block
No
Convert from CGC to PBC

Fig.7. Flowchart- BPCS steganography

V. EVALUATION CRITERIA

5.1 PSNR and MSE

PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods. The PSNR measures the similarity between two images (how two images are close to each other), while the MSE measures the difference between these two images.

$$MSE = \frac{1}{[N \times N]} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(i,j) - S(i,j)]^2$$

The PSNR formula as follow:

$$PSNR = \frac{10 \log_{10} 255^2}{MSE} db$$

5.2 Capacity Measure

Capacity in data hiding indicates the maximum amount of information that can be hidden and successfully recovered by the steganography system [13]. Because of that the number of hidden bits varies depending on cover image size, to measure the hidden capacity, we use bit per- pixel (bpp) given as follow:

$$bpp = \frac{hidden\ bits}{Numpix(I_c)}$$

Where, Numpix(Ic) is total pixels number of pixels in the cover image.

5.3 Bit Error Rate (BER)

If the communication channel is ideal and there are not attacks, the proposed steganography system successfully recovers the hidden data. However we must consider a real communication scheme, and then we have to measure the bit error rate (BER), which is computed as follow:

$$BER = \frac{Error\ bits}{Message\ bits}$$

VI. DRAWBACK OF BPCS-STEGANOGRAPHY

1.BPCS-steganography is based on complexity of image. For maximum embedding information, we require more and more complex image.

2. BPCS-steganography is not robust to even small changes in the stego image. I.e.to extract embed data from stego image correctly, there should not any change in stego image.

3. In some application, the presence of the embedded data may be known, but without the customization parameters, the data is inseparable from the image.

VII. CONCLUSION

The objective of this paper was to demonstrate our BPCS-Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans cannot see any information in the bit-planes of a color image if it is very complex. This technique provides higher capacity for hiding information. We can combine BPCS-steganography with encrypted embedded data for very strong information security. Future research will identify and formalizing the customization parameters and developing new applications.

REFERENCES

[1] Behroz A. Forouzan, “Cryptography & Network Security”, McGraw Hill Publication,2008, New Delhi.

[2] N.F. Johnson and S. Jajodia. “Exploring Steganography: Seeing the Unseen”. IEEE Computer, Volume 31: pages 26–34, 1998.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "*Information Hiding-A Survey*", Proc. of the IEEE, Vol.87, No.7, pp. 1062-1078, 1999.

[4] SeifedineKadry and Sara Nasr, "New Generating Technique for Image Steganography", LNSE, Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

[5] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan – University of Maine, Orono, Maine.

[6] Tao Zhang, Zhaohui Li and Peipei Shi, "Statistical Analysis Against improved BPCS Steganography", IEEE, 237 – 240, 27-29 March 2010.

[7] http://datahide.org/BPCSe/

[8] Kawaguchi, E. and Taniguchi, R., "Complexity of binary pictures and image thresholding – An application of DF-Expression to the thresholding problem", Proceedings of 8th ICPR, vol.2, pp.1221-1225, 1986.

[9] Kawaguchi, E. and Taniguchi, R., "The DF-Expression as an image thresholding strategy", IEEE Trans. On SMC,vol.19,no.5, pp.1321-1328, 1989.

[10] Kawaguchi, E. and Taniguchi, R., "Depth-First Coding for multi-valued figures using bit-plane decomposition", IEEE Trans. On Comm., vol.43, no.5, pp.1961-1995.

[11] HIOKI Hirohisa. "A data embedding method using bpcs principle with new complexity measures".http://www.i.h.kyoto-u.ac.jp/~hioki/research/DH/files/abcde_steg02_revised.pdf

[12] M. Goljan, J. Fridrich and R. Du, "Distortion-free data embedding", in Proc. of 4th Information Hiding Workshop, 2001, pp. 27-41.

[13] Mansi S. Subhedara, Vijay H. Mankarb, "Current status and key issues in imagesteganography: A survey", 2014 Elsevier Inc.

[14] SumeetKaur, SavinaBansal, R. K. Bansal, "Steganography and Classification of ImageSteganography Techniques", 2014 IEEE.

[15] Ratnakirti Roy, SuvamoyChangder, AnirbanSarkar, Narayan C Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", 2013 IEEE