High Secure Image Steganography in BCBS Using DCT and Fractal Compression

K. Munivara Prasad[1] V.Jyothsna[2] S.H.K. Raju[3] S.Indraneel[4]
[1]*Department of CSE,SVEC,Tirupati,*
[2]*Department of IT,SVEC,Tirupati,*
[3]*Department of CSE, Narayana Engineering College, Nellore,*
[4]*Department of CSE, St.Ann's college of engineering and Technology,chirla,*

ABSTRACT
We propose a new approach to steganography for hiding secret images in the digital media. Steganography differs from digital watermarking because both the information and the very existence of the information are hidden. We refer it as Blind Consistency based Steganography, which provides high imperceptibility and security for information from subterfuge attack. The Existing Steganographic approaches are unable to handle the Subterfuge attack i.e, they cannot deal with the opponents not only detects a message ,but also render it useless, or even worse, modify it to opponent favor. The advantage of BCBS is the decoding can be operated without access to the cover image and it also detects if the message has been tampered without using any extra error correction. To improve the imperceptibility of the BCBS, DCT is used in combination to transfer stego-image from spatial domain to the frequency domain. The hiding capacity of the information is improved by introducing Fractal Compression and the security is enhanced using by encrypting stego-image using DES. Finally the Embedding and Extraction process are detailed in the paper, along with the analysis on capacity, security and imperceptibility. The experimental results are provided as well.

Keywords:
Steganography, Data Hiding,BCBS, DCT and Fractal Compression

1. Introduction

The word *steganography* literally means *covered writing* as derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not. The area of steganography has a long history. It can be traced back to techniques like invisible ink and microdots used by spies [4]. Common approaches to hide information in digital images include least significant bit insertion (LSB), masking (in a manner similar to paper watermarks), and information hiding in transformations (DCT, FFT, WT, etc.) [5,6]. While they all have different advantages for specific applications, they also suffer a similar problem: such systems are unable to deal with subterfuge attacks (collusion and forgery) [8], that is, they cannot deal with the opponents who not only detect a message, but also render it useless, or even worse, modify it to the opponent's favor.

Data hiding methods for images are generally classified into two categories. One embeds the images into the spatial domain [7], such as the method of changing the least significant bits (LSB) and the texture block coding method. The other embeds the images into the frequency domain such as the spread spectrum methods, the wavelet-based embedding methods, and the DCT-based embedding methods. Generally speaking, we can embed larger amounts of data in the spatial domain than in the frequency domain, but hiding information in the frequency domain is more robust than in the spatial domain.

In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Most Significant Bits (MSB) of the image to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the human eye. This is mainly used in watermarking

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

techniques. In the transform based method, the spatial domain is transformed to frequency domain using DCT, Fast Fourier Transforms (FFT), and Wavelets etc.

A new approach in steganography, referred to as blind consistency-based steganography (BCBS). At the sender's side, the message is hidden in specific columns/rows of an image. After a slightly global blur operation, those columns/rows are discarded and replaced by their neighboring pixels chosen randomly in order to make the marked columns/rows unpredictable. Locations of those message hiding places and the blur kernel are the two stego-keys. The decoding process is an ill-posed problem. We proposes the separable deblurring based consistency method to decode the message at the receiver's side, which transforms the illposedness to a well-posed one by using separable blur kernel and integer-type cover images. Therefore, exact and unique solution can be guaranteed in the decoding process. The breakthrough of the BCBS approach is that it not only decodes the message exactly, it also detects if the message has been tampered without using any extra error correction. The detection is integrated into the process of decoding. Another advantage of the BCBS approach is that the decoding process can be operated *blindly* without access to the cover image, which enhances the imperceptibility. That is, it eliminates the possibilities of malicious attackers obtaining both the cover image and the stego image and does a bit-by-bit comparison to discover the potential existence of hidden messages.

2. Related Work

Chin-Chen Chang [2] has proposed a model in which the data is embedded into the cover image by changing the coefficients of a transform of an image such as discrete cosine transform. The high compression rate is one of the advantages of fractal image compression. Another advantage is the good image quality, after enough iteration for decompression. But the computation time required to encode an image might be very long due to an exhaustive search for the optimal code. And DES encryption is used to provide the security to the data, but it is unable to protect the Stego-Image from *subterfuge attack*. Which means the attacker not only detect a message, but also render it useless or even worse, modify it to the opponent's favor.

K.B.Raja[3] has proposed a model which uses LSB ,but LSB provides poor security ,and DCT for converting objects in spatial domain to frequency domain. This model uses only raw Images because of *subterfuge attack*. The JPEG, BMP and GIF image formats, the header contains most of the image information. This leads to the problem of insecurity and therefore the payloads from such images can be easily identified.

Hairong Qi *[1]* has proposed a model BCBS, the advantage of the BCBS approach is that the decoding process can be operated *blindly* without access to the cover image, which enhances the imperceptibility. And that it not only decodes the message exactly, it also detects if the message has been tampered without using any extra error correction. The drawback is the amount of data to hide is very less because he is selected only one row / Column to hide with one bit per pixel. And also the security is provided only for the Stego-Image not for the data that can be improved by using DES.

3. Proposed Work

In this section we define the Fractal Image compression, BCBS (Blind Consistency Based Steganography) and, Discrete Cosine Transformation (DCT) with Examples. Here the Cover Image is a carrier of embedded image; Secret Image is an image which is to be embedded in the cover image .Stego-Image is the combination of Cover Image and Secret Image. The Secret Image is compressed with Fractal image Compression method with high compression rate by preserving the decompressed image closed to that of original Image. BCBS is used to hide the data and it not only decodes the message exactly, it also detects if the message has been tampered without using any extra error correction and DES is used to encrypt the BCBS stego-image to provide the security. Discrete Cosine Transformation (DCT) is used to convert stego-object in spatial domain into stego-image of frequency domain. The reverse process is carried out at receiver end.DES encoded data is retrieved from the Stego-Image by using IDCT and it can be decrypted by using DES. The stego image is extracted from the BCBS Extraction and extracted data can fractal decompressed to get the original secret Image. Here the images referred to as raw images, JPEG or GIF.

3.1. Fractal Compression

Fractal image compression is a lossy image compression [16] technique to achieve high level of compression while preserving the quality of the decompressed image close to that of the original image. The method relies on the fact that in a certain images, parts of the image resemble other parts of the same image (self-similarity). But the computation time required to encode an image might be

very long due to an exhaustive search for the optimal code. Fractal-based compression methods do not require gridding, segmentation, or modeling stages as most of the specialized methods require, although using such techniques along the fractal image compression algorithms results in a better quality image with the higher compression ratio.

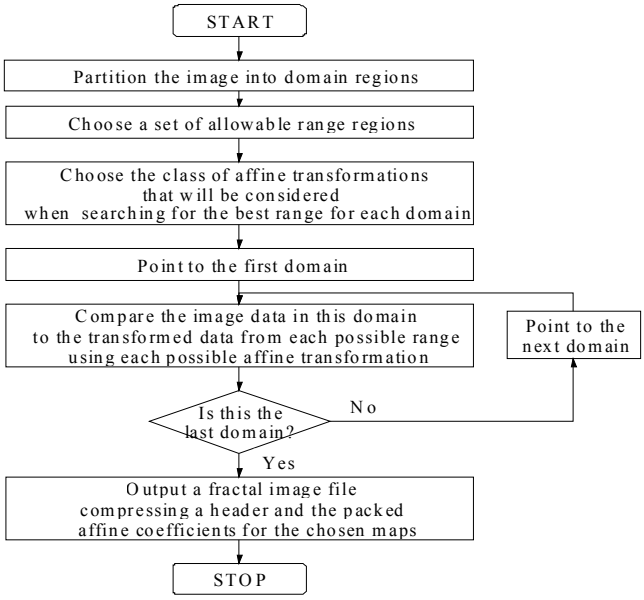


Fig 1(a).An algorithm for the fractal compression

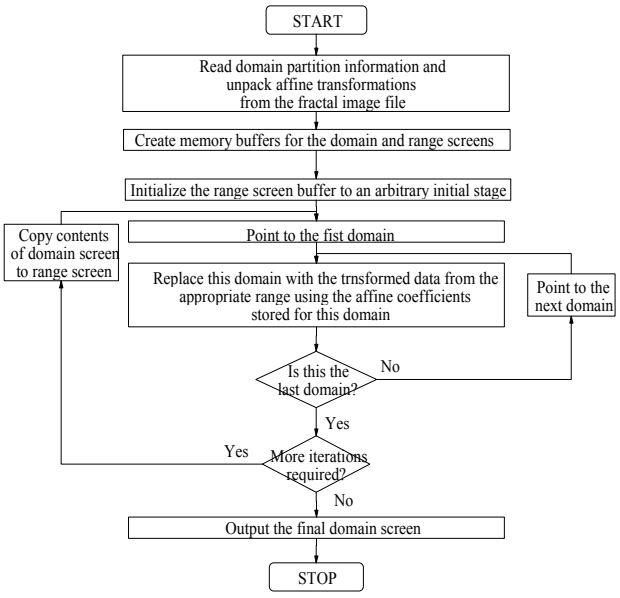
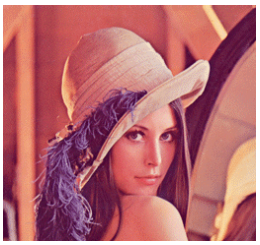


Fig 1(b).An algorithm for the fractal decompression

Example the Lena Image can be compressed as



Original Lena image (184,320 bytes)

FIF-min. quality (3,924) comp. ratio: 46.97:1

Fig 2.Compression of Lena Image with Fractal Compression

3.2. Blind Consistency Based Steganography (BCBS):

For purposes of this explanation,[1] message (c) is hidden in specific columns of the cover image (f), which is then undergone a slightly blur operation. In the resulting image, the message hiding columns are replaced by pixels chosen randomly from their neighbors to generate the stego image (g). In the decoding process, separable deblurring based consistency method is designed to convert the ill-posed decoding problem to a well-posed one in order to uniquely extract the hidden message. The message hiding columns and the blur kernel are the two stego keys used at the receiver's side for decoding.

Figure 4: (a) Cover Image (b) Secret Image (Bit map)

(c) Stego- Image after applying BCBS

(d) Retrieved Image

3.3. Descreate Cosine Transformation (DCT):

The DCT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain[14]. Many digital image and video

compression schemes use a block-based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images [9]. In the transform-based method there are two types (i) the large number of coefficients are modified slightly to accommodate data of the payload, (ii) replacing the smaller number of insignificant coefficients by the data of the payload. Here the data is embedded into the cover image by changing the coefficients of a transform of an image such as discrete cosine transform coefficients. The two dimensional DCT is applied on blocks of 8x8 pixels. This transforms 8x8 pixels blocks into 64 DCT coefficients.

Formulae for DCT and inverse DCT:

DCT:

$$F(u,v) = \frac{\Delta(u)\Delta(v)}{4}\sum_{i=0}^{7}\sum_{j=0}^{7}\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16}f(i,j)$$

IDCT

$$F(i,j) = \frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}\Delta(u)\Delta(v).\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16}.F(u,v)$$

$$\Delta(\varepsilon) = \begin{cases} 1/\sqrt{2} & for\ \varepsilon = 0 \\ 1 & otherwise \end{cases}$$

4. Proposed Model

In our model the combination of two steganographic algorithms are used namely BCBS and DCT.BCBS algorithm used to provide the security for the stego-object from Subterfuge Attack. In BCBS [1]at the sender's side, the message is hidden in specific columns/rows of an image instead of selecting major portion of the pixels in the cover image. To make the hidden columns unpredictable global blur operation is applied. Locations of those message hiding places and the blur kernel are the two stego-keys. The decoding process is an ill-posed problem. The separable deblurring based consistency method to decode the message at the receiver's side.

In our model BCBS can be applied for both column and row depends upon the amount of data to be hidden in the cover image. But the algorithm is repeated for column and row separately, this does not degrade the performance of the algorithm; it will increase the channel capacity.

The DCT method is used to transform the image Stego-image from special domain into frequency domain.DES algorithm is used to encrypt the stego-image (stego image from BCBS) before applying DCT.

First of all, we use this symbol ***X*** to denote the secret image of size *N X N*. Let the cover image ***C*** be a image of size *M* X *M*. The secret image ***X*** can be defined as

$$X = \{x(i,j), 0 \le i < N, 0 \le j < N\},$$

Where $x(i,j) \in \{0,...,2^l - 1\}$, and l is the number of bits used in each pixel.
Likewise, the cover image ***C*** can be defined as
$C = \{c(i,j), 0 \le i < M, 0 \le j < M\}$,
Where $c(i,j) \in \{0,...,2^l - 1\}$, and l is the number of bits used in each pixel.
We use S1 symbol to denote the Stego-image1 which is the output of the first steganography algorithm BCBS.
The Symbol S2 is used to denote the Stego-image which is the output of the second steganographic algorithm DCT or it is the output of the embedding procedure of our model.

4.1. The Embedding Procedure

The Embedding procedure in our model embeds fractal compressed secret image (X) in two stages. Firstly the compressed stego image is embedded in the cover image (C) using BCBS,the output of the BCBS embedding is the stego image S1 act as a secret image in the stage2 and DES encrypted S1 is embedded with DCT.
The Embedding of the secret image (X) into the cover image in the proposed model has the following steps.

1. The secret image (X) is fractal compressed to achieve high level of compression while preserving the quality of the decompressed image close to that of the original image.
2. The compressed image is given as the input for the BCBS algorithm to avoid subterfuge attack.
3. The output or Stego-image S1 (output of BCBS Embedding) is encrypted using DES to provide the security to the data.
4. The encrypted data is transferred from spatial domain to frequency domain and embedded using DCT method.
5. The final stego-image S2 (output of DCT embed) is transferred over the noiseless channels.

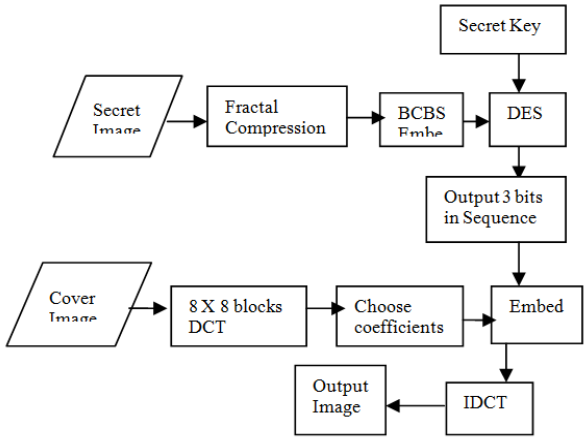


Fig 5(b).Block diagram for Embedding Procedure

4.2. The Extracting Procedure

At the receiving side after receiving the stego-image S2 again the two steganographic methods are used to extract the secret image (X).These are the following steps to follow while extracting the secret image (X)from the Stego-image S2.

1. The stego-image S2 is given as the input to the IDCT to extract the encrypted data.
2. The encrypted data is decrypted using DES decryption to get S1.
3. From stego-image S1 the compressed data is extracted using BCBS Extract or decoding.
4. Fractal decompressed the extracted data to get the Secret image (X).

The BCBS Extract from images is basically an *ill-posed* [10,11] problem, since a little change in the input data can dramatically affect the solution. In the decoding process of BCBS, by putting some restrictions on the cover image and the blur kernel, we are able to transform the ill-posed decoding problem into a well-posed one.

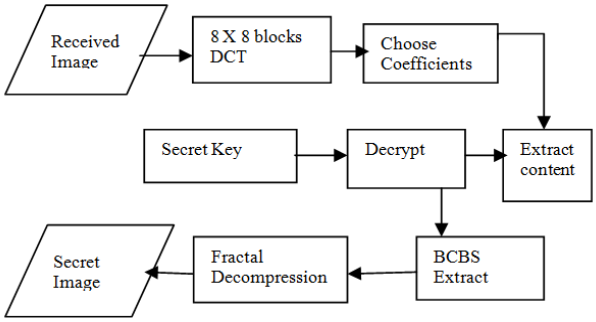


Fig 5(a).Block diagram for Extracting Procedure

We propose an algorithm for our model as Secure Blind consistency based Steganography with DCT (SBSDCT). The algorithm is given below.

Algorithm SBSDCT:
Input: Cover Images (c1 &c2) and a Seecret Image (X)
Output: Encoded Stego Image(s)

Step 1: Fractal compression(X)
Step 2: Run BCBS( )
Step 3: Encrypt the S1 using DES;
Step 4: Compute DCT( ).
Step 5: The output of DCT is collected as Stego image(S2).

BCBS( )

The cover image c1 is of size M X N. The length of the secret image (After compression) X1 is of l_c bits. Without loss of generality, we assume X1 is hidden in one column (column i) or (row i) of c1 and that $l_c \leq M$. We also assume each pixel in the cover image c1 carries maximum three bits of the hidden message[1].

Step 1: Each pixel in column i (or row i) of cover image c1 is replaced with column i-1 (or row i-1) of the same image.

Step 2: Add the (j * 3) bits of the secret image (X1) to the least significant bits of the j^{th} column i (or row i) where j=1,2,……. l_c.

Step 3: Blur kernel h of finite size is used to blur the image generated from step 2. This process helps spread the message bits to the neighboring pixels.

Step 4: Discard column *i* (or row i) from the image generated by step 3, and replace it with neighbor pixel brightness value where the neighbor is chosen randomly. The resulting image from step 4 is called the stego image (S1).

we can formulate the message encoding process into Eq. 1, where c1 + X1 denotes that the message (S1) is hidden in the cover image (c1), *x* indicates the convolution with the blur kernel, and ±r denotes the further process on column *i (or row i)*described in step 4. The blur kernel h is discrete and of finite support.

$$S1 = (c1 + X1) \times h \pm r$$

(iv) DCT( )

1. Read a block of n *n pixels
2. Compute c2 = Δ (u) Δ(v) / 4
3. for(i =0; i<7; i++)
4. for(i=0; j < 7; j++)
5. Compute

F(u, v)=c2*cos ((2i+l)uπ /16)*cos ((2j+1)vπ /l6)*f(i, j)

The working of the algorithm is already explained as the model defined in the previous section. The procedure is adopted at receivers end.

5. Experimental Results and Steganalysis

The performance of our model includes compression, Imperceptibility, capacity; error computation and security of BCBS are analyzed based on these experimental results.

a. Compression:

Since Image requires large bandwidth, compression is useful to reduce the bandwidth. Here Fractal compression is used to compress the image. The comparison of Jpeg and Fractal compression is defined with example in fig 7.

b. Imperceptibility:

Imperceptibility takes advantages of human psycho visual redundancy. For image steganography imperceptibility can measured using two metrics Mean square Error (MSE) and Peak signal to noise ratio (PSNR).
The MSE is computed by performing byte by byte comparisons of the two images, since a pixel is represented by 8 bits and hence 256 levels are available to represent the various gray levels. The MSE will result in a meaningful value only when each byte of an image is compared with the corresponding byte of another image.

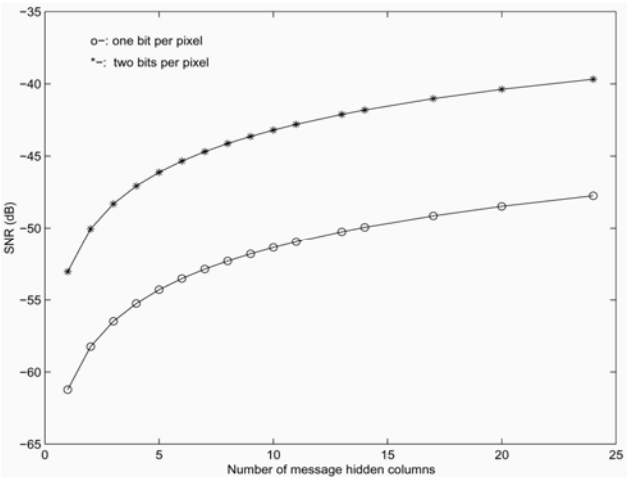
$$MSE = 1/ MN \sum^{M}_{i=1} \sum^{N}_{j=1} (f_{ij} - g_{ij})^2$$

Where M, N are the row and column numbers of the cover image, fij is the pixel value from the cover image, gij is the pixel value.(L=255 for 8 bit grey level image)
The **PSNR** of grey level image is specified as

$$PSNR = 10 \log_{10} L^2/MSE$$

c. Signal-to-noise ratio (SNR) is another way to quantify imperceptibility, where the message is regarded as the signal (σ^2_S / variance of the signal), and the cover image as the noise (σ^2_N - variance of the noise). Therefore, the higher the SNR, the more perceptible the message is.

$$SNR = \sigma^2_S / \sigma^2_N$$



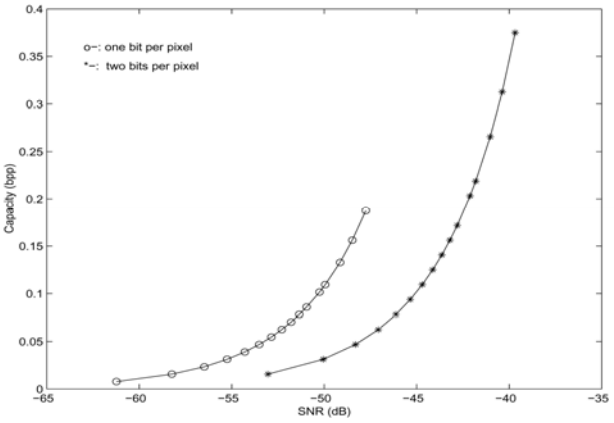
SNR vs. number of message hidden columns.

d. Channel Capacity:

Based on the conditioning analysis in [15], the size of the blur kernel needs to be greater than 3X3, and the distance between adjacent message hidden columns should be greater than twice the radius of the blur kernel. Therefore, we can quantize the capacity of BCBS as

$$(M \times ([N / sh] - 1) \times b) / (M \times N) \text{ bits / pixel}$$

Where b is the number of bits per pixel used to hide the message sh is the size of the blur kernel, M and N are the number of rows and columns in the cover image. A smaller sh will improve the imperceptibility.



Capacity vs. SNR.

The channel capacity of the BCBS is maximized with Compression before the embedding. Even the capacity is increased by selecting row and column together in BCBS embedding procedure. First BCBS embedding is

performed by selecting the row later based on the amount of data remain the BCBS is again applied by selecting the Column as the secret key. This process will improve the channel capacity and the security because of twice applying of the BCBS at embedding. The receiving side does it in reverse order.

e. Error Computation:

Bit error rate (BER): Here we compute the BER for two equal size images that is cover image and stego-image. BER is more accurate for error analysis when compared to MSE, because in BER we compute the actual number of bit positions which are replaced in the stego image.

f. Security:

In the JPEG, BMP and GIF image formats, the header contains most of the image information. This leads to the problem of insecurity and therefore the payloads from such images can be easily identified. In our model the security is provided for the image and data in two levels. Firstly the image is compressed and the compressed image is hidden in first cover Image used in BCBS. The stego object of BCBS is encrypted using DES then that is embedded into the Cover Image of DCT embed method. The security for the compressed image is provided using BCBS and DES encrypted DCT coefficients. Which also provide the security for the stego object from subterfuge Attacks.

6. Performance Analysis

Consider the two cover images C1 and C2 as baboon and boat and the secret image (X) is Lena are shown in Fig 6. Then we embed the compressed secret image (X1) Lena into the cover image baboon using BCBS and the second embedding of the encrypted stego-image S1 is embedded into the cover image (C2) boat is shown in Fig 6. The reverse operations, extraction of the images are shown in the Fig 6. The compression rate of the fractal image compression and the comparison with JPEG compression is shown in the fig 7. And the overall experimental results are shown in Table1. The sizes of the secret images are 512x512 pixels or larger. In [7], Wu and Tsai proposed an embedding method to embed a gray-level image of 256x256 in the spatial domain. And in Chin-Chen Chang [2] proposed an embedding to embed 512x512 images in the frequency domain. In *Hairong Qi [1]* proposed BCBS embed method for 128x128 images. We compare its results with ours, and this comparison is shown in Table 3 and Table 4. In K.B.Raja [3] proposed a method to embed secret image using LSB and DCT for raw images. Our PSNR values are slightly less than those in [2,7].

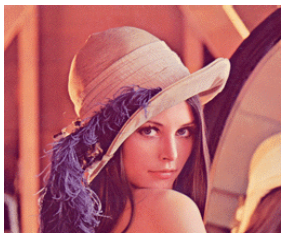
In our approach the cover image size is 512 X512 pixels. If the secret image size is 256X256 pixel and 66616 bytes, after fractal compression the image consist of 1419 bytes (Min.quality compression 46.97:1).According to the BCBS embed algorithm, it selects one column (or row) from cover image of size is 512x 512.The column consists of 512 pixels each can hold 3 bytes then 512X3 which is equals to 1536 bytes. The algorithm can also repeat two times for one column and row separately, in this 512x2+512x2 which is equals to 2048 bytes. If the secret image is 512x512 pixels and the size is 184320 bytes, then the compressed image is of 3024 bytes (Min.quality compression 46.97:1).If the BCBS embed algorithm repeats two times for one column and row the size is 512x3+512x3 which is equals to 3072 bytes. That is sufficient to embed a fractal compressed image.

In the DCT embedding procedure the BCBS stego-image (after embedding the secret image in the BCBS cover image) is encrypted using DES. DES encryption converts the BCBS stego- image into equal size cipher text. And it is embedded in to the second cover image of size 512x512 using DCT [2].

C1 C2 X

Fig 6(a).Cover Images(Baboon and Airplane)and the Secret image(Lena)

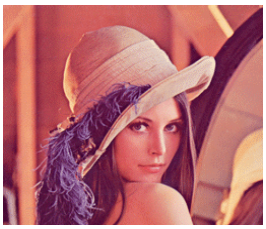
Fig 6(b).Stego-imge(S1),Stego-image(S2) and Extracted Secret image(X)



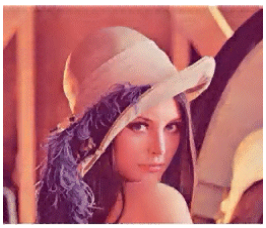
Original Lena image (184,320 bytes)

JPEG-max. quality (32,072)
comp. ratio: **5.75:1**

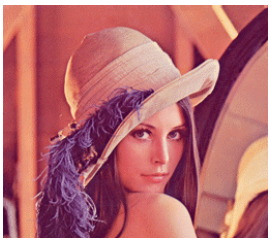
FIF-max. quality (30,368)
comp. ratio: **6.07:1**



JPEG-med. quality (11,278)
comp. ratio: **16.34:1**



FIF-med. quality (7,339)
comp. ratio: **25.11:1**



JPEG-min. quality (8,247)
comp. ratio: **22.35:1**

FIF-min. quality (3,924)
comp. ratio: **46.97:1**

Fig 7: Comparison of fractal and JPEG Compression Methods

Table 1: The image quality (PSNR) of the cover images after embedding into the BCBS cover image

The Secret Images	The cover images of size 512 x 512			
	Airplane	Boat	Lena	Toys
Baboon	32.96	33.14	32.86	30.01
Barbara	33.55	33.17	33.18	30.92
Girl	35.72	35.85	35.87	33.16
Lena	34.02	34.74	34.23	31.08
Peppers	34.62	34.81	34.38	31.42

Table 2: The image quality (PSNR) of the BCBS extracted images

Baboon	Barbara	Girl	Lena	Peppers
33.01	33.12	33.04	35.72	36.48

Table 3: The comparison results of the PSNRS of secret images of size 256 ×256

The cover images	The secret images 256x256					
	Peppers			Lena		
	Proposed	**	*	Proposed	**	*
Baboon	37.12	37.50	41.12	36.87	37.28	41.00
Airplane	34.97	35.42	41.58	34.89	35.22	39.29

*The method proposed by Wu and Tsai [7]
**The method proposed by Chin-Chen Chang[1]

Table 4: The comparison results of the PSNRS of secret images of size 512 ×512

The cover images	The secret images 512x512			
	Peppers		Lena	
	Proposed	**	Proposed	**
Baboon	35.07	35.36	34.84	35.14
Airplane	35.14	35.42	34.96	35.22

**The method proposed by Chin-Chen Chang[1]

7. Conclusion

In this paper we have used the combination of BCBS algorithms and DCT transformation. We propose an approach to embed an image via fractal compression into the BCBS Image and the BCBS stego image into the DCT domain of the cover image. The stego-object in the spatial domain is transformed into frequency domain by applying DCT. Due to the high compression rate of fractal compression, we can embed a secret image larger than the cover image itself. BCBS is used to avoid subterfuge attack. More than one bit/byte of information can be added to each pixel in BCBS if it is imperceptible to the human visual system and can apply both for column and row if need. As for security, we encrypt the compressed data via DES so that we can prevent the eavesdroppers from getting the secret image.

REFERENCES

[1] Hairong Qi "Blind consistency based steganography for information hiding in digital media", International Conference on Images Steganography.
[2] Chin-Chen Chang "A DCT-domain System for Hiding Fractal Compressed Images" Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)
[3] K B Raja , C R Chowdary "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images "International conference on Image and Signal Processing ,2005.
[4] D. Kahn, "The history of steganography," in The First Workshop on Information Hiding, R. Anderson, Ed., vol.

1174 of Lecture Notes in Computer Science, pp. 1–5. Springer-Verlag, 1996.
[5] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. NOS 3&4, pp. 313–335, 1996.
[6] N.F. Johnson and S. Jajodia, "Exploring steganography, seeing the unseen," IEEE Computer, pp. 26–34, February 1998.
[7] WU, D.C. and TSAI, W.H.:-"Spatial-domain Image Hiding Using Image Differencing",IEE Proc.-vis. Image signal process., feb. 2000, 147(1), pp. 29-37.
[8] PFITZMANN, B: "Information Hiding Terminology", Proceedings of first workshop of Information Hiding May 1996 Cambridge, UK,pp.347-350.
[9] MARVEL, L.M., BONCELET, C.G., Jr., and RETTER, C.T.: " Spread Spectrum Image Steganography", IEEE trans. Image Process., 8(8), Aug 1999, pp.1075-1083.
[10] H.C. Andrews and Hunt B.R., Digital Image Restoration,Prentice-Hall, 1977.
[11] A.K. Katsaggelos, Digital Image Restoration, Springer-Verlag, 1991.
[12] C. Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations", Proceedings of the International Workshop Trends & Recent Achievements in IT, Romania, pp. 116-121, May 2002.
[13] K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Technical Report,Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, December 2004.
[14] H. Qi, A High-Resolution, Large-Area, Digital Imaging System,chapter 4, pp. 84–89, North Carolina State University,Raleigh, August 1999, Ph.D. Dissertation.
[15] FISHER, Y.: 'Fractal Image Compression: Theory and Application.' (Springer-Verlag, New York, 1995.)

Mr. K. Munivara Prasad received the M.E degree in CSE from Sathyabama University, Chennai. He is currently working as an Assistant Professor (SL) in the Department of Computer Science and Engineering in Sree vidyaniketha Engineering College ,Tirupati. His research interests are in Computer Networks ,Information Security and Image Processing.

Ms. V. Jyothsna received the M.Tech degree in IT from Sathyabama University, Chennai and she is doing her Ph.D in Intrusion Detection at JNTUH. She is currently working as an Assistant Professor in the Department of Information Technology in Sree vidyaniketha Engineering College ,Tirupati. Her research interests are in Computer Networks, Information Security and Intrusion Detection.

Mr. S.H.K.Raju received the M.E degree in CSE from Sathyabama University, Chennai and he is doing his Ph.D in Rayalaseema University. He is currently working as an Assistant Professor (SL) in the Department of Computer Science and Engineering in Narayana Engineering College,Nellore. His research interests are in Computer Networks, Information Security and Data Mining.

Mr. S.Indraneel received the M.E degree in CSE from Sathyabama University, Chennai and he is doing his Ph.D in Computer Networks and Security under the guidance of Dr C.H.D.V Subba Rao.. He is currently working as an Associate Professor in the department of Computer Science and Engineering in St.Ann's College of Engineering and Technology, Chirala. His research interests are in Computer Networks, Sensor Networks and Image Processing.