ISSN 2286-4822
www.euacademic.org

EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 1/ April 2015

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

Image Compression and Decompression Technique Based on Block Truncation Coding (BTC) And Perform Data Hiding Mechanism in Decompressed Image

NASRUL ALAM
Assistant Professor in Computer Science & Engineering
BCARE Institute of Management & Technology
West Bengal, India

Abstract:

Data compression is important in storage and transmission of information. Various compression techniques have been proposed in recent years to achieve good compression. In this paper mainly discuss a well known Image compression technique based on Block Truncation Coding (BTC), where less computational complexity. By using this technique we are performing compression of gray scale/monochrome image data. It is one-bit adaptive moment-preserving quantizer that preserves certain statistical moments of small blocks of the input image in the quantized output.

In this paper we also concern about data hiding mechanism and information security based on stegoanalysis technique. Important information is firstly hidden in a host data, such as text, image, video or audio, etc, and then transmitted secretly to the receiver. Finally stego image is formed by combining different stego objects and transmit to the receiver side. At the receiving end different opposite processes should run to get the back the original secret message.

This paper mainly discuss about Image compression and decompression technique based on Block Truncation Coding (BTC) and perform data hiding mechanism in decompressed image and also discuss to retrieve the minimum pixels image such as 8×8 pixels, 16×16 pixels and so on, up to original cover image size through the divided by 2×2 pixels and perform data hiding in retrieve image.

Key words: Image compression, Block Truncation Coding, lossy compression, Cover Image, Steganography, Information hiding / Embedding.

Introduction

With the development of the Internet, information processing technologies and the rapid development of communication, it is necessary to share information resources, and the network has becoming the main means of communication. Nevertheless, the Internet is an open environment so; information security has becoming increasingly important. Today, information security technology has two main branches are cryptography and information hiding. Cryptography is concerned on concealing the content of the message, so it becomes difficult to understand. Information hiding is divided into steganography and digital watermarking.

"Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured."

Steganography is the art of hiding information in such a way that prevents the detection of hidden messages. The message is the data that the sender wants to remain confidential. It can be in the form of text, image, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded. It serves to hide the presence of the message. We can use gray images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as a cover image. It is important to note that the hidden data is not detectable in the stego-image.

Image Processing

Image Processing and Analysis can be defined as the "act of examining images for the purpose of identifying objects and judging their significance". Image analyst study the remotely sensed data and attempt through logical process in detecting, identifying, classifying, measuring and evaluating the significance of physical and cultural objects, their patterns and spatial relationship.

Analyzing and manipulating images with a computer. Image processing generally involves three steps:

1. **Import** an image with an **optical scanner** or directly through **digital photography.**
2. **Manipulate or analyze** the image in some way. This stage can include **image enhancement** and **data compression**, or the image may be analyzed to find patterns that aren't visible by the human eye. For example, meteorologists use image processing to analyze satellite photographs.
3. **Output the result**. The result might be the image altered in some way or it might be a report based on analysis of the image.

Image processing is the application of **signal processing** techniques to the domain of **images** — two-dimensional **signals** such as **photographs** or **video.** Image processing does typically involve **filtering** an image using various types of filters.

Digital image processing has been demonstrated in this chapter using examples of Landsat images that are available in digital form. It is emphasized, however, that any image can be converted into a digital format and processed in similar fashion. The three major functional categories of image processing are:

1. ***Image restoration*** to compensate for data errors, noise, and geometric distortions introduced during the scanning, recording, and playback operations.
2. ***Image enhancement*** to alter the visual impact that the image has on the interpreter, in a fashion that improves the information content.
3. ***Information extraction*** to utilize the decision-making capability of the computer to recognize and classify pixels on the basis of their digital signatures.

Image Processing classify as three type

1) Low level image processing (Noise removal, image sharpening, contrast enhancement).
2) Mid level image processing (Segmentation).
3) High level image processing (Analysis based on output of segmentation).

Image Compression

Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more images to be stored in a given amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages.

Types of Image Compression

There are two different types of compression

- Lossless Compression
- Lossy Compression

Lossless and lossy compression

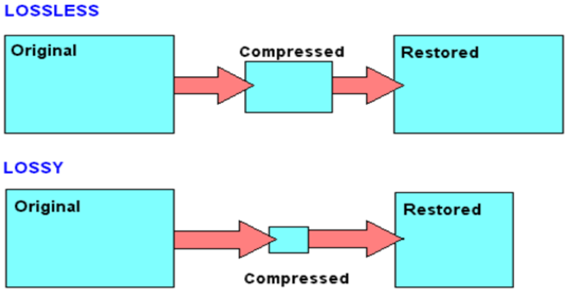


Fig. 1 : Diagram of Lossless and Lossy Compression

Basis of the Project Design Work

The Project design work stands on three bases 1) Compression Technique 2) Compression and Decompression 3) Block Truncation Coding (BTC).

Compression Technique

Compressing an image is significantly different than compressing raw binary data. Lossless compression involves with compressing data which, when decompressed, will be an exact replica of the original data.

Error Metrics

Two of the error metrics used to compare the various image compression techniques are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The MSE is the cumulative squared error between the compressed and the original image, whereas PSNR is a measure of the peak error. The mathematical formulae for the two are

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2$$

$$PSNR = 20 * \log10 (255 / \text{sqrt}(MSE))$$

where I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction. So, if you find a compression scheme having a lower MSE (and a high PSNR), you can recognize that it is a better one.

Compression is one of the techniques used to make the file size of an image smaller. The file size may decrease only slightly or tremendously depending upon the type of compression used.

Image Compression and Decompression

The compression system model consists of two parts: the compressor and the decompressor.

Compression process:

- **Uncompressed image → compressed file**

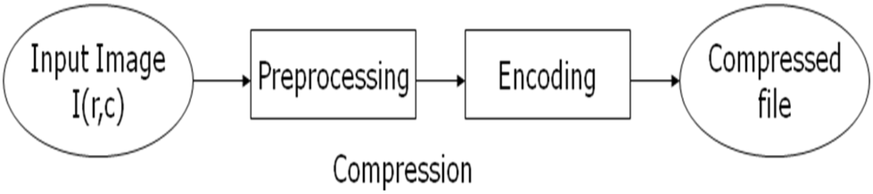


Fig. 2.a : Diagram of Compression Technique

Decompression process:

- **Compressed file → decompressed image**

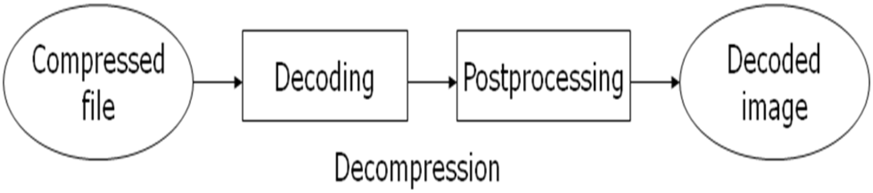
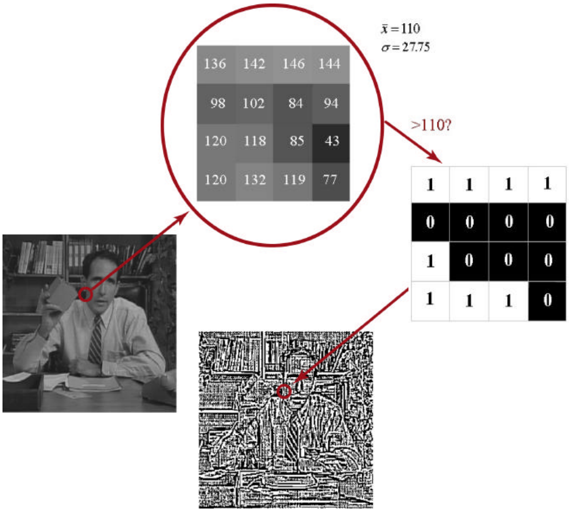


Fig. 2.b : Diagram of Decompression Technique

Block Truncation Coding

Block Truncation Coding (BTC) is one of the lossy image compression techniques. The computational complexity involved in this method is very simple. In the proposed method, the feature of inter-pixel correlation is exploited to further reduce the requirement of bits to store a block. The proposed method gives very good performance in terms of bit-rate and PSNR values when compared to the conventional BTC.

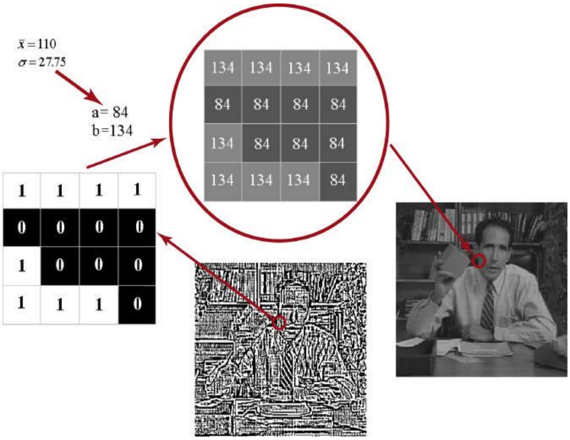


136	142	146	144
98	102	84	94
120	118	85	43
120	132	119	77

1	1	1	1
0	0	0	0
1	0	0	0
1	1	1	0

Figure 3. Illustration of the BTC compression process.

$$m_1 = \bar{x} = \frac{1}{k}\sum_{i=1}^{k} x_i \quad , \qquad (1)$$
$$m_2 = \frac{1}{k}\sum_{i=1}^{k} x_i^2$$



1	1	1	1
0	0	0	0
1	0	0	0
1	1	1	0

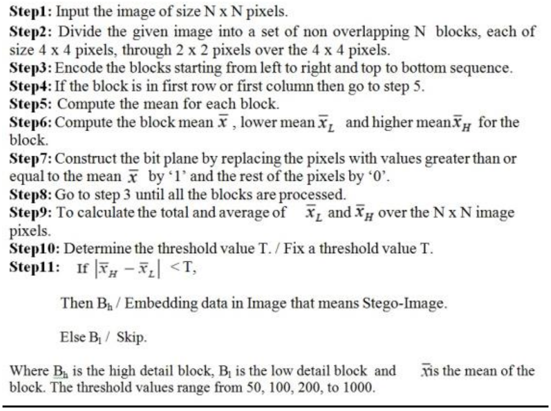
134	134	134	134
84	84	84	84
134	84	84	84
134	134	134	84

Figure 4. Illustration of the BTC decompression process.

The sample standard deviation σ is given by:

$$\sigma^2 = m_2 - m_1^{\ 2} \qquad (2)$$

Algorithm for BTC :



Step1: Input the image of size N x N pixels.
Step2: Divide the given image into a set of non overlapping N blocks, each of size 4 x 4 pixels, through 2 x 2 pixels over the 4 x 4 pixels.
Step3: Encode the blocks starting from left to right and top to bottom sequence.
Step4: If the block is in first row or first column then go to step 5.
Step5: Compute the mean for each block.
Step6: Compute the block mean $\bar{x}$, lower mean $\bar{x}_L$ and higher mean $\bar{x}_H$ for the block.
Step7: Construct the bit plane by replacing the pixels with values greater than or equal to the mean $\bar{x}$ by '1' and the rest of the pixels by '0'.
Step8: Go to step 3 until all the blocks are processed.
Step9: To calculate the total and average of $\bar{x}_L$ and $\bar{x}_H$ over the N x N image pixels.
Step10: Determine the threshold value T. / Fix a threshold value T.
Step11: If $|\bar{x}_H - \bar{x}_L| < T$,

Then B_h / Embedding data in Image that means Stego-Image.

Else B_l / Skip.

Where B_h is the high detail block, B_l is the low detail block and $\bar{x}$is the mean of the block. The threshold values range from 50, 100, 200, to 1000.

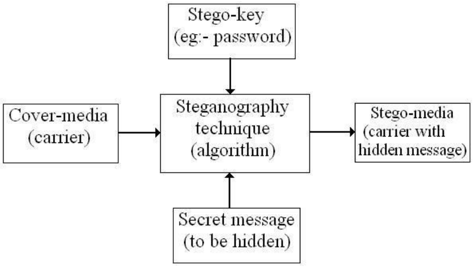
Steganography

Introduction:

Steganography, from the Greek, means covered or secret writing, and is a long-practiced form of hiding information. Although related to cryptography, they are not the same. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

More precisely,

> “the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present."



Different Steganographic Protocols:

There are basically three types of steganographic protocols:

1) Pure – key steganography: In this model, there requires no exchange of stego – key. This method is the simplest but is the most unsecured means to communicate secretly.

2) Secret – key steganography: In this model, both the sender and the receiver shares common secret – key before conveying messages.

3) Public – key steganography: In this model, two keys are required; one is public key and the other is private key. The public key is used for embedding message while the private key is used for extracting message.

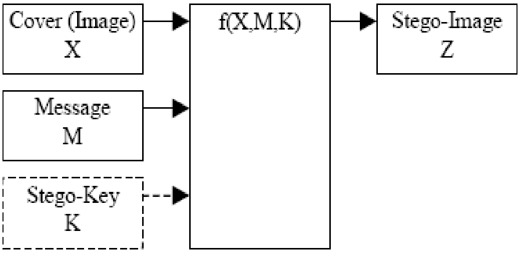
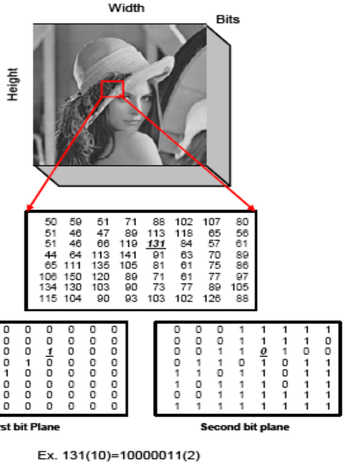


Figure 5: Basic Digital Steganography Encoder

Data Embedding Technique

Data Embedding Technique – BPCS (Bit Plane Complexity Segmentation) Steganography:



50	59	51	71	88	102	107	80
51	46	47	89	113	118	65	56
51	46	66	119	*131*	84	57	61
44	64	113	141	91	63	70	89
65	111	135	105	81	61	75	86
106	150	120	89	71	61	77	97
134	130	103	90	73	77	89	105
115	104	90	93	103	102	126	88

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	*1*	0	0	0
0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0

First bit Plane

0	0	0	1	1	1	1	1
0	0	0	1	1	1	1	0
0	0	1	1	*0*	1	0	0
0	1	1	0	1	0	1	1
1	1	0	1	1	0	1	1
1	0	1	1	1	0	1	1
0	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Second bit plane

Ex. 131(10)=10000011(2)

Figure 6: Bit Plane Slicing concept considering pixel having value 131.

Embedding Data:

Embedding data, which is to be hidden, into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the *cover image*. The second file is the message—theinformation to be hidden. A message may be plain text, ciphertext, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a *stegoimage*. A stego-key (a type of password) may also be used to hide, then later decode, the message.

Embedding Data into Images with Steganography:

With concerns of internet privacy growing tremendously over the last few years the usage of covert channels of digital communication is on the rise. Embedding hidden data into various other forms of data is by no means a new technology. People have been embedding hidden files into images, music files, and even TCP/IP packets for several years. Through the use of various steganography applications this process is becoming easier and easier for even those who are not technically savvy. One of the most common ways of embedding data covertly is to use what is called the least significant bit (LSB) methodology of injecting data into an image.

Hiding Information in Images:

> "Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured."

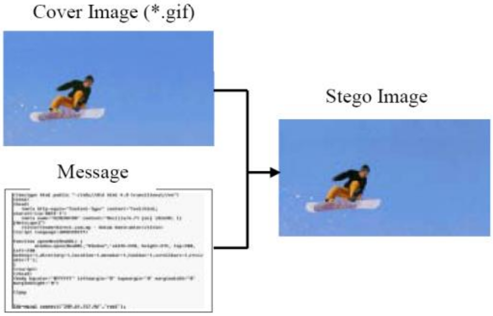


Figure 7: Stego-Image Process

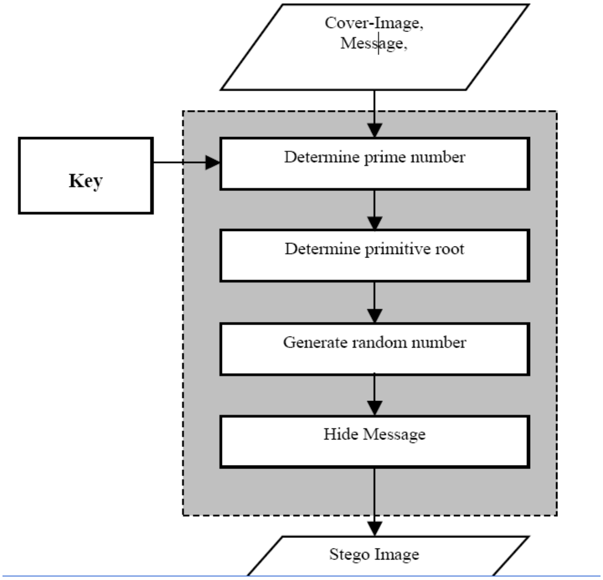


Figure 8: Flow Chart for SIHS

Embedding Algorithm:

Definition 1:

Given a cover image C and a message M to be hidden in C, then the private key steganography system can be defined as:

$$\mathbf{Fe: M\times K \rightarrow C}\text{, Such that } \mathbf{Fe\ (C,M,K) = C'}$$

and

$$\mathbf{Fr(\ Fe\ (C,M,K,),\ K) = Fr\ (C',\ K)}$$

Where

K is a secret key.

Fe is the embedding function.

Fr is the extracting function

C' is the stego-image.

This means that the message **M** can be embedded in **C** by the function **Fe** to generate the stego-image **C',** and the embedded message can be extracted by the extracting function **Fr** from **C'.**

Definition 2:

C: is a cover image partitioned into binary blocks of size 8×8{C1,..., Cy}.

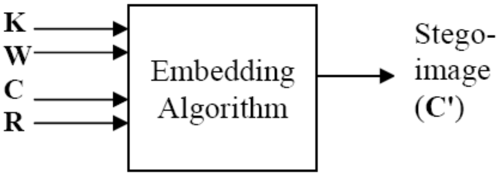
K: is a random binary block of size 8×8.

W: is a weight matrix of size 8×8, where

{Wi,j, i =1.. 8, j = 1..8}={1,2,...,63}

R: is the number of bits to be embedded in one block.

note that **r** ≤ $\lfloor$**log(mn+1)** $\rfloor$ **= 6**



Extracting Algorithm:

Input: C',W, K

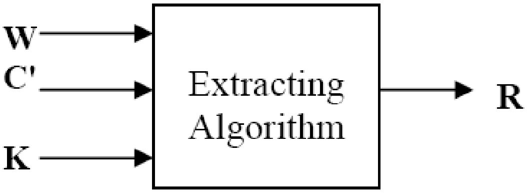
Output: R

BEGIN

FOR each block C'I

b1…br = (C'i ⊕ K) ⊗W mod2r

END



Mean Square Error (MSE) :

Mean Square Error (MSE) is an old, proven measure of control and quality [10]. MSE equals the mean of the squares of deviations from the target:

$$\mathbf{MSE} = \frac{1}{m}\sum_{i=1}^{m}(X_i - T)^2$$

This factor was applied to the stego-images generated from the proposed algorithm, modified algorithm and the LSB algorithm.

Peak To Signal Noise Ratio (PSNR) :

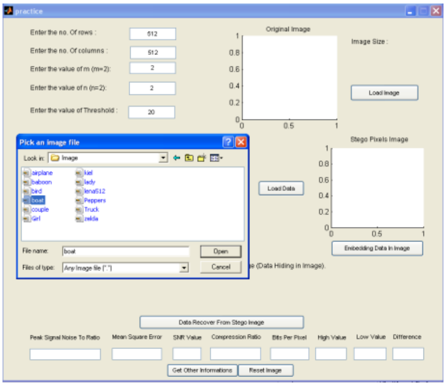
The Peak to Signal Noise Ratio **(PSNR)** is used to evaluate the image quality/error. The **PSNR** of a grey-image is defined as :

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

Where **MSE** is the Mean Square Error.

Project Demonstration (Screenshot)

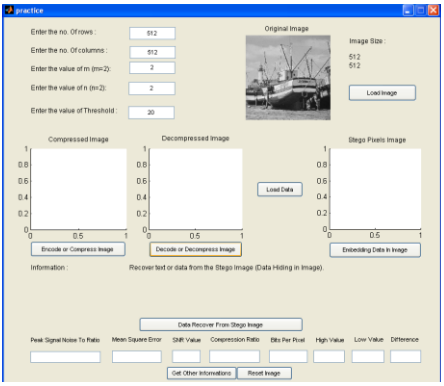
Step 1: Select the original cover gray image (input) from browser by the sender.



Enter the no. Of rows : 512
Enter the no. Of columns : 512
Enter the value of m (m=2): 2
Enter the value of n (n=2): 2
Enter the value of Threshold : 20

Pick an image file
Look in: Image
File name: boat
Files of type: Any Image file (*.*)

Step 2: Display the original cover image and actual image size 512 × 512 Pixels.


practice

Enter the no. Of rows : 512

Enter the no. Of columns : 512

Enter the value of m (m=2): 2

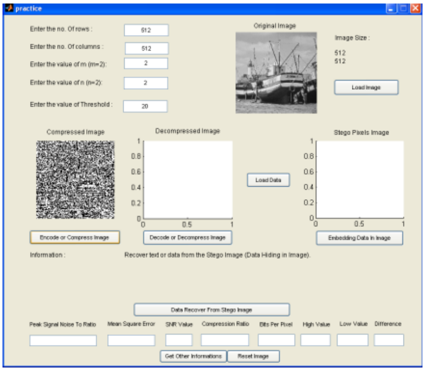
Enter the value of n (n=2): 2

Enter the value of Threshold : 20

Image Size : 512 512

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Step 3: Convert Original Cover Image to Encoded Image(Compress Image).


practice

Enter the no. Of rows : 512

Enter the no. Of columns : 512

Enter the value of m (m=2): 2

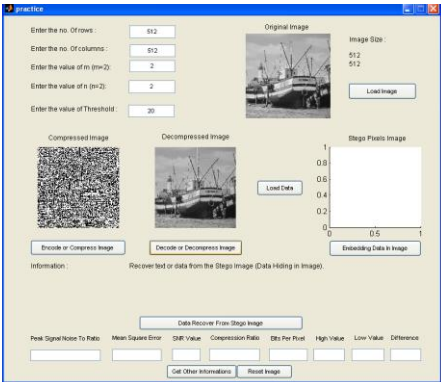
Enter the value of n (n=2): 2

Enter the value of Threshold : 20

Image Size : 512 512

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Step 4 : Convert Encoded Image(Compress Image) to Decoded Image(Decompress Image).


practice

Enter the no. Of rows : 512

Enter the no. Of columns : 512

Enter the value of m (m=2): 2

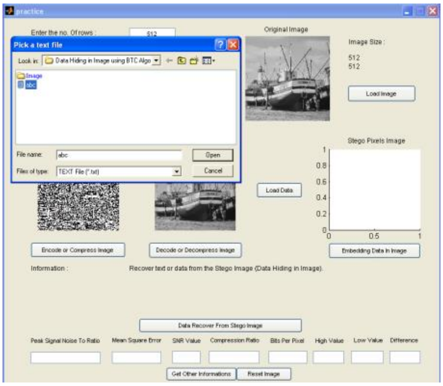
Enter the value of n (n=2): 2

Enter the value of Threshold : 20

Image Size : 512 512

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Step 5: Select the data or information which embedded with Decoded Image.



Pick a text file

Look in: Data Hiding in Image using BTC Algo

File name: abc

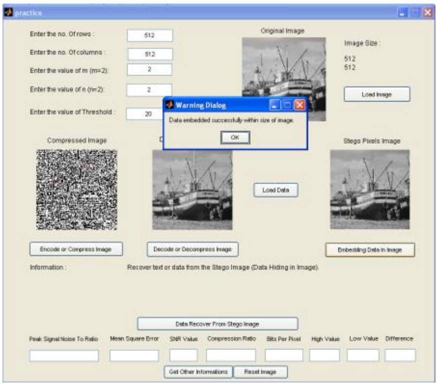
Files of type: TEXT File (*.txt)

Enter the no. Of rows : 512

Image Size : 512 512

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Step 6: Embedding data or information in Decoded Image which is the Stego Image.



Enter the no. Of rows : 512

Enter the no. Of columns : 512

Enter the value of m (m=2): 2

Enter the value of n (n=2): 2

Enter the value of Threshold : 20

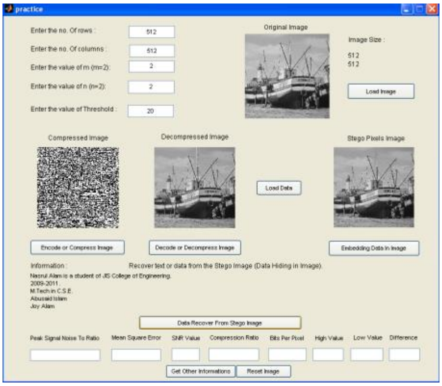
Image Size : 512 512

Warning Dialog

Data embedded successfully within size of image.

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Step 7: Extract Embedding data or information from Stego Image and receiver received the hiding data or information.



Enter the no. Of rows : 512

Enter the no. Of columns : 512

Enter the value of m (m=2): 2

Enter the value of n (n=2): 2

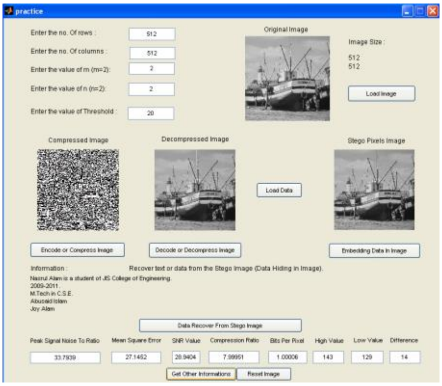
Enter the value of Threshold : 20

Image Size : 512 512

Information : Recover text or data from the Stego Image (Data Hiding in Image).

Nasrul Alam is a student of JIS College of Engineering.
2009-2011.
M.Tech in C.S.E.
Abussaid Islam
Joy Alam

Step 8: To get other information from stego image.



Enter the no. Of rows : 512
Enter the no. Of columns : 512
Enter the value of m (m=2): 2
Enter the value of n (n=2): 2
Enter the value of Threshold : 20

Image Size :
512
512

Information : Recover text or data from the Stego Image (Data Hiding in Image).
Nasrul Alam is a student of JIS College of Engineering.
2009-2011.
M.Tech in C.S.E.
Abusaid Islam
Joy Alam

Peak Signal Noise To Ratio	Mean Square Error	SNR Value	Compression Ratio	Bits Per Pixel	High Value	Low Value	Difference
33.7939	27.1452	28.9404	7.99951	1.00006	143	129	14

Conclusion

In this paper, a new algorithm is introduced to hide data in a gray-scale image. The proposed algorithm can hide data in a block of 4×4 pixels, 8×8 pixels and actual size in a gray-scale image by changing a 2×2 pixels. Divide the given image into a set of non overlapping N blocks, each of size 4 × 4 pixels, through 2 × 2 pixels over the 4 × 4 pixels. Two versions of the algorithm were given: the first one selects the bits to be changed randomly, while the second version ensures that the modified bits to be changed are selected as close to the Least Significant Bit (LSB) as possible. This selection will ensure that changes made in the cover image can not be detected by a human observer.

Block truncation coding is an efficient compression technique while offering good image quality. Nonetheless, the blocking effect inherent in BTC causes severe perceptual artifact in high compression ratio applications.

This demonstrates the potential of the BTC based image compression technique. The advantage of this method is the flexibility in determining the percentage compression at the expense of image quality by choosing appropriate threshold.

This work motivates many more investigations in image compression based on BTC.

An efficient and secure data hiding approach based upon BTC.

Data hiding in compression image.

- JPEG
- GIF

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. A *stego-key* has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Finally, we have shown that steganography that uses a key has a better security than non-key steganography.

BIBLIOGRAPHY

E.J. Delp, O.R. Mitchell, "Image Compression using Block Truncation Coding", IEEE, Trans. Communications, Vol . 27, pp.1335-1342, September 1979

P. Franti, O.Nevalainen and T.Kaukoranta, "Compression of digital images by block truncation coding: a survey.", *The computer Journal*, Vol. 37 issue 4, pp 308-332, 1994

M. D. Lema, O.R.Mitchell, "Absolute Moment Block Truncation Coding and its Application to Color Image", IEEE Trans. Coomun., Vol. COM-32, No. 10, pp. 1148-1157, Oct. 1984.

E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," *IEEE Trans. Commun.*, vol. COMM-27, no. 9, pp. 1335–1342, Sep. 1979.

O. R. Mitchell, E. J. Delp, and S. G. Carlton, “Block truncation coding: a new approach to image compression,” *Proceedings of the IEEE International Conference on Communications,* vol. 1, June 4-7 1978, pp. 12B.1.1-12B.1.4.

M. Kamel, C. T. Sun, and L. Guan, “Image compression by variable block truncation coding with optimal threshold,” *IEEE Trans. Signal Process.*, vol. 39, no. 1, pp. 208–212, Jan. 1991.

B. V. Dasarathy, *Image Data Compression: Block Truncation Coding*, IEEE Computer Society Press, Los Alamitos, California, 1995.

O. R. Mitchell and E. J. Delp, “Multilevel graphics representation using block truncation coding,” *Proceedings of the IEEE*, vol. 68, no. 7, July 1980, pp. 868-873.

M. M. Amin, M. Salleh, S. Ibrahim, M.R Katmin (2003), “Information Hiding Using Steganography”, 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003, pp. 21-25.

R. J. Anderson. Stretching the limits of steganography. *Information Hiding, Springer Lecture Notes in Computer Science*, 1174:39–48, 1996.