Cyber Times International Journal of Technology & Management

Vol. 10 Issue 2, April 2017 – September 2017

TABLE OF CONTENTS

FRACTAL COMPRESSED IMAGE HIDING TECHNIQUE IN DCT DOMAIN

Pournima Jungle
Asst. Prof., TMV, Pune
pournimakj@rediffmail.com

ABSTRACT

Cryptography is used to hide information from enemy. Now a days there are advancements of technology and we can send quickly information to anywhere across the globe, but this also alarmed us that it can be tempered, read by anyone, unauthenticated person. So here we need some more advance technique like BCBS and DCT which used to compress an image under a big or small image so intruder/ enemy cannot even open the image and remain unknown. Here we used combination of aforesaid technique in three step and get the result of hiding big image under cover of small image.

KEYWORDS: *BCBS, Cryptography, DCT Domain, Steganography.*

I. INTRODUCTION

Steganography

Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography can be illustrated as, “The art of communicating in a way which eliminate the existence of the real values. In contrast to Cryptography, intruder is allowed to come, take piece of info to play and about ready to temper the real information.”

The goal of steganography is to hide messages inside other messages in a way that does not allow anyone to even assume that there is second message present.”

Information hiding Techniques-

Information can be hidden by several ways of which following two are the major key player;

1. Water marking
2. Cryptographic

Watermarking

- Watermarking concept is used to prevent piracy in digital media to identify owner ship of content.
- This can be done by adding some additional data like metadata to existing information that become undetectable by infringer and in case of illegal use this plays a vital role for ownership identification.
- Watermarking is done by making a image/Signal + added metadata= Final Image/Signal to distribute over network for free/ subscription use.

Cryptography

Cryptography or cryptology is a term derived from Greek language having sense of hiding some information from others. Hiding can be done by any of the method like;

1. Drawing of an image and hid information in it.
2. Developing of protocol which is unknown to all other third parties so

they are unable to understand even if they get this.

3. In modern we use several algorithms to hid actual information when we spread that over the network.
4. Cryptography basically used to conceal information of vital in nature for the state.

Fractal Compression

Fractal compression is technique where an image is broken into small pieces of several images having some relation in all between, is called Fractal code, that help to re-join the images on receiving. Fractal compression works on breaking and re-joining concepts.

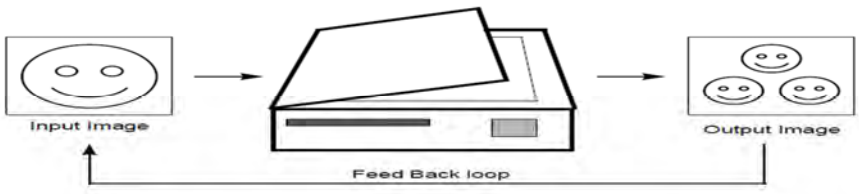

Figure 1: Block Diagram of Fractal Compression

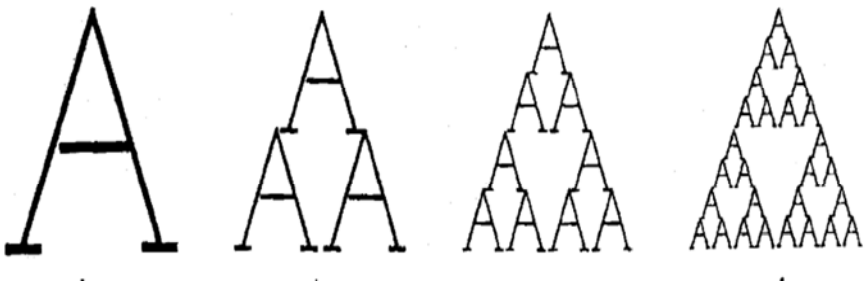

Figure 2: Example of Fractal Compression

Forward DCT

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

for $u = 0,..., N-1$ and $v = 0,..., N-1$

where $N = 8$ and $C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$

Inverse DCT

$$f(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

for $x = 0,..., N-1$ and $y = 0,..., N-1$ where $N = 8$

II. LITERATURE SURVEY

K. Munivara Prasad [1] in his paper presented an approach to steganography for overlapping secret images in the digital media. The others stenographic approaches are unable to handle the Subterfuge attack i.e., If one get the image, modified it and get

back send to you again with data of his favor then how to identify that this information is not been tempered by any one or if it is then it should not be decrypted as it is.

The basic advantage of BCBS is that it also detects if the message has been tampered without using any extra error correction.

Huirong Qi Wesley E. Snydel; William A. Sunder [2] designed a blindness of BCBS which needs not to decrypt image again by disturbing the cover image.

Wang Xing-yuan, Li Fan-ping, Wang Shu-guo[3] detailed fractal image compression method based on
1. Spatial correlation and
2. Hybrid genetic algorithm.

This is two stage based algorithm. The first stage exploits by correlation of two images by neighboring blocks to recreate them when receiving. If it is not satisfied, the second stage of the algorithm is carried out in order to explore further similarities from the whole image.

This is to be keeping in mind always that in this method only relative positions are recoded in the first stage of the algorithm.

Vijayaratnam Ganeshkumar [4] said in his paper that if any eavesdropper gets attainted about information concealing then he will try and try to get out that original info which is hidden.

Now there is no 100 percent secure algorithm by which we can say that nobody can break it even try after try.

Now he suggest in his paper that hide an information in image/digital media in such a way that eavesdropper does not able to get attention, which make info untouchable by him and we can send it to destination even without single try to break it.

This is achieved by a three layered architecture which consists of:

1. Stegno Service,
2. Security Services using and
3. Data Services.

III. PROPOSED MODEL

The proposed model is try to combination of two steganographic algorithms namely-

- BCBS
- DCT.

BCBS algorithm used to provide the security for the stego-object from tricky 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 de-blurring based consistency method to decode the message at the receiver's side.

In these 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 (stego image from BCBS) before applying DCT.

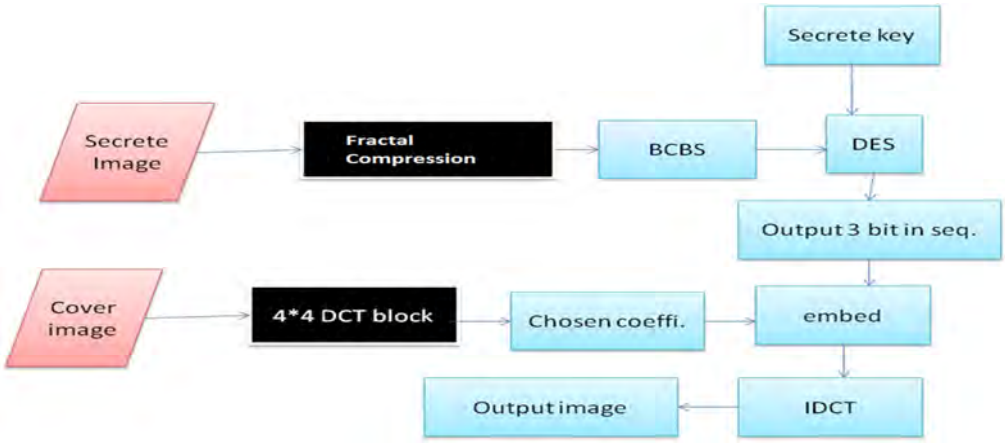

Figure 3: Block diagram for Embedding Procedure

IV. EXPECTED OUTCOME

The model proposes an approach to embed an image via

1. Fractal compression into the BCBS Image and
2. The BCBS stego image into the DCT domain of the cover image.
3. The stego- is transformed into frequency domain by u using DCT. Due to the high compression rate of fractal compression, proposed model is able to hide a bigger image under a small image without loss of any piece of information.

By adding one extra bit to every pixel in image fractal BCBS is able to avoid subterfuge attack. Finally received image can be encrypted using DES.

REFERENCES

[1] K. Munivara Prasad, V.Jyothsna, S.H.K. Raju, S.Indraneel "High Secure Image Steganography in BCBS Using DCT and Fractal Compression" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[2] Hairong Qi "Blind consistency based steganography for information hiding in digital media", International Conference on Images Steganography.

[3] Wang Xing-yuan, Li Fan-ping, Wang Shu-guo "Fractal image compression based on spatial correlation and hybrid genetic algorithm" J. Vis. Commun. Image R. 20 (2009) 505–510.

[4] Vijayaratnam Ganeshkumar, Ravindra L. W. Koggalage "Secured Communication using Steganography Framework with Sample RTF Implementation" Fourth Intemational Conference on Industrial and Information Systems, ICIIS 2009, 28·31 December 2009, Sri Lanka.