Review on Image Steganographic technique based On curvlet transform for data hiding

Mr. Chougule Vrushabh N., Prof. Mrs. P. P. Belagali
Dr. J.J.Magdum college of Engineering

***Abstract*— Steganography is the new scheme in order to hide a secret data in cover images which uses transform domain to increase its robustness and security. transform represents edges better than wavelet, transform offers an effective solution to the problems associated with Image Steganography using wavelets and DCT (Discrete Cosine Transform). In this method size of cover image and secret image is same while in other methods secret image is half the sizes of cover image, also the stego image and extracted images are closer to original image than other methods.**

***Index Terms*— Steganography, curvelet transform, security, privacy, Discrete Cosine Transform, cover image**

I. INTRODUCTION

In last few years there is rapid growth in the internet world; attacker takes different ways to hack our secret data on the network. So our secret data is now not safe on network, in order to provide security to our secret data we have to take some steps. One solution to this problem is data hiding. Data hiding is method of hiding secret message in which we hide our secret data into a cover medium so that unwanted users will not aware of even existence of the hidden messages. This is achieved by steganography.

There are two types of Steganography they are Fragile and Robust.

A. Fragile: In Fragile steganography, if the file is modified, then the secret information is destroyed. For example the information is hidden the BMP file format. If the file format is changed into JPEG or some other format the hidden information is destroyed. The advantage of fragile is required to be proved when the file is modified.

B. Robust: In robust steganography the information is not easily destroyed as in frangile steganography, but robust steganography is difficult to implement than fragile. Information hiding system is featured by three different aspects, which includes security, capacity and robustness as shown Fig (a).

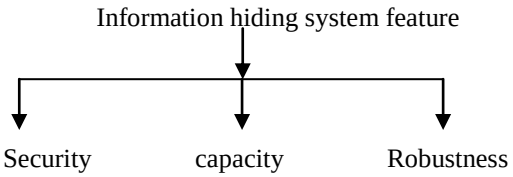

Fig (a)

Security refers to hacker's inability to even detect the presence of hidden information, Capacity means the ability of cover medium to hide the information, Robustness is the ability of stego medium to handle the modification before hackers or other user destroy information.

II. PROPOSED WORK

Steganography is applicable to all data objects that contain redundancy; in this research work we use only JPEG images. In daily life we use internet, users communicate with each other by sending digital images via email or other communicating medium and for that JPEG is one of the most common type that users use. Also steganography system with the JPEG format is not affected by visual attacks. The proposed method contains the following steps.

Step 1: Image Statistics-aware Test:

Input to this step is cover image, during this step we test the cover image if the cover image contains unrecognizable patterns and passes the histogram test then the cover image is accepted otherwise search for another cover image.

Step 2: Image Pre-Processing and Correction:

Input to this step is tested cover image from previous step; during this step three corrections will be done. First for each pixel in the cover image apply level

correction. Second for each pixel in the cover image apply contrast correction; and finally for each pixel in the cover image apply colour balance correction.

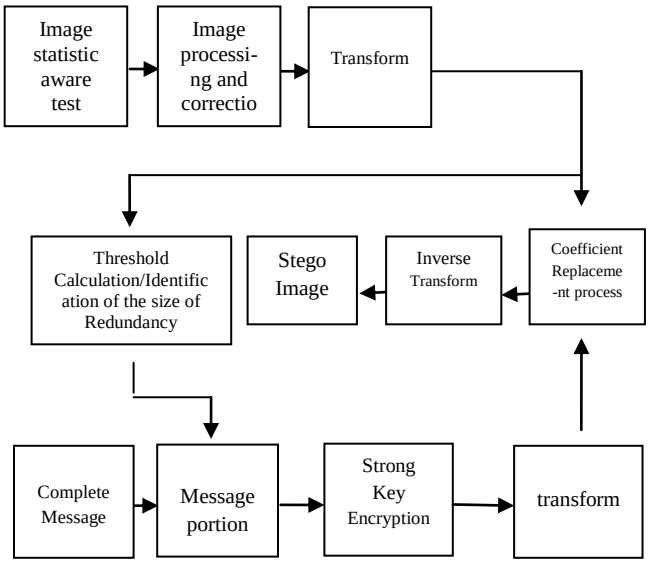

Fig (b)

Step 3: FDCT-FW Transformation:

During this third step pre-processed cover image is converted to domain through 2D transform FDCT-FW.

Step 4: Threshold Calculation/Identification of the size of redundancy:

This step calculates the threshold (T) that is used to define what is the size of the redundancy in the cover image, that can be used to embed the message or part of the message.

$$T = \frac{\alpha}{N}\sum^{N}|J_w| \quad (1)$$

Where Jw is the coefficients of the FDCT-FW for the cover image, N is the number of coefficients. It was found that this equation should be scaled by a correction factor α (between 0 and 1).If the value of the FDCT-FW coefficient <T, then store the index of the coefficient, s=s+1.Where s is the size of the information.

Step 5: Message Partitioning:

Input to this step is secret message, value of s. During message partitioning step the secret message is converted into 1D bit stream.

Step 6: Strong Key Encryption:

This step encrypt the 1D bit stream of the message from the previous step with RC4,key length=56.

Step7: Encrypted Message FDCT-FW Trans - formation:

Encrypted 1D bit stream of the message during previous step is transformed to domain during this step.

Step 8: Stego Image Formation:

Input to this final step is FDCT-FW of the cover image, FDCT-FW transform of the encrypted message. During stego image formation step place the FDCT-FW coefficients of the encrypted message in the location specified previously in the FDCT-FW of the cover message. Inverse FDCT-FW transforms the result.

At the receiver side to obtain original message and cover image following steps are used.

Step1:

At the receiver side obtained stego image is decompressed to obtain the coefficients of curvelet transformed cover image and curvelet transformed encrypted bit stream of the message.

Step2:

In this step applying inverse curvelet transform to both coefficients to obtain cover image and encrypted bit stream.

Step3:

Encrypted bit stream is decrypted using same key to obtain the bit stream of the message, we get the hidden message and cover image

III. .PARAMETERS OF EVALUATION:

[1] PSNR:

The invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio (PSNR)

$$PSNR=10Log10(S2/MSE) \quad (2)$$

Where,

$$S^{2}=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{j-1}^{n}J^{2}(i.j) \quad (3)$$

[2] MSE:

The MSE is the Mean Square Error defined as,

$$MSE=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[J(i,j)-J'(i,j)]^{2} \quad (4)$$

Where J' is the pixel in the stego image the result of the steganography.

[3] RMSE :

The Root Mean Square Error (RMSE) is used also as a measurement criterion.

$$\text{RMSE}=\sqrt{MSE} = \sqrt{\frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[J(i,j) - J'(i,j)]^2} \quad (5)$$

REFERENCES:

[1] N. Provos, and P. Honeyman, "Hide and seek: An introduction To steganography," IEEE Security and Privacy Magazine, IEEE Computer Society, May-June pp. 32-40, 2003.

[2] R. Poornima and R.J.Iswarya, " An Overview of Digital Image Steganography "International journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.

[3] Tamer Rabie, "High-Capacity Steganography" 2013 6th International Congress on Image and Signal Processing (CISP 2013)

[4] T. Peining, S. Dexter, and A. Eskicioglu, "Robust digital image watermarking in curvelet domain," Proceedings of SPIE, International Society for Optical Engineering, ISSN 0277- 786X , Vol. 6819, pp. 1- 12,2008.

[5] E. Candès, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," Tech Rep., Appl. Comput. Math., California Institute of Technology, 2005.

[6] J. Fridrich, M. Goljan, D. Soukal, and T. Holotyak, "Forensic steganalysis: Determining the stego key in spatial domain steganography," Proceeding of EI SPIE, Vol. 5681, pp. 631- 642, SanJose, CA, 2005.

[7] N. Provos, and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE Security and Privacy Magazine, IEEE Computer Society, May-June pp. 32-40, 2003.

[8] M. Naor, and O. Reingold, "On the construction of pseudo random permutations," Journal of Cryptography, Vol. 12, No. 1, pp. 29-66, 1999.

[9] A. A. Al-Ataby, and F. M. Al-Naima, "A modified high capacity image steganography technique based on wavelet transform," Int Ara Journal of Information Technology (IAJIT), Vol. 7, No. 4, pp. 358-364, 2010.