A SURVEY: IMAGE STEGANOGRAPHY USING DIFFERENT METHOD

[1] Gayakwad Sonal, [2] Hiren Mer
[1] Student, [2] Asst professor
[1]Master of computer engineering,
[1]Atmiya Institute of Science and Technology, Rajkot, India

Abstract— [1] Steganography is the art and science of writing hidden messages in such a way that, apart from the sender and intended recipient, no one suspects the existence of the message, a form of security through the state of being unknown. The main two famous schemes used for image steganography are spatial domain embedding and transform domain embedding. In this paper five method [1][2][3] Huffman Encoding and Transform Domain Method, DWT based, dual wavelet transform, Wavelet Transforms and [4][5] Hybrid Wavelet Transforms, DWT and Artificial bee colony optimization have been used for the image steganography.

Keywords— Image steganography, DWT, Huffman encoding, Dual wavelet transfer, Hybrid wavelet transfer, Artificial bee colony optimization

I. INTRODUCTION

[3] STEGANOGRAPHY IS THE PROCESS OF HIDING OF A SECRET MESSAGE WITHIN AN ORDINARY MESSAGE AND EXTRACTING IT AT ITS DESTINATION. ANYONE ELSE VIEWING THE MESSAGE WILL FAIL TO KNOW THAT IT CONTAINS SECRET/ENCRYPTED DATA. THE WORD COMES FROM THE GREEK WORD "STEGANOS" MEANING "COVERED" AND "GRAPHEI" MEANING "WRITING". [1] THE MAIN TWO FAMOUS SCHEMES USED FOR IMAGE STEGANOGRAPHY ARE SPATIAL DOMAIN EMBEDDING AND TRANSFORM DOMAIN EMBEDDING. THE MAIN AIM OF DWT IS USED TO TRANSFORM ORIGINAL IMAGE (COVER IMAGE) FROM SPATIAL DOMAIN TO FREQUENCY DOMAIN. [6] THE SECRET INFORMATION CAN BE EMBEDDED IN VARIOUS TYPES OF COVERS. IF INFORMATION IS EMBEDDED IN A COVER TEXT (TEXT FILE), THE RESULT IS A STEGO-TEXT OBJECT. SIMILARLY, IT IS POSSIBLE TO HAVE COVER AUDIO, VIDEO AND IMAGE FOR EMBEDDING WHICH RESULT IN STEGO-AUDIO, STEGO-VIDEO AND STEGO IMAGE RESPECTIVELY.

[7] 1.1. TYPE OF STEGANOGRAPHY

- Image steganography
- Text steganography
- Video steganography
- Protocol steganography
- Audio steganography

1.1.1. Image Steganography: Taking the cover object as image in steganography is known as image steganography. In this technique pixel intensities are used to hide the information.
1.1.2. Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc.*, where protocol is used as carrier, is known as network protocol steganography.
1.1.3. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information.
1.1.4. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity.
1.1.5. Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and *etc.* is used to achieve information hiding.

[7] 1.2. IMAGE STEGANOGRAPHY TERMINOLOGY

Image steganography terminologies are as follows:

- **Cover-Image**: Original image which is used as a carrier for hidden information.
- **Message**: Actual information which is used to hide into images. Message could be a plain text or some other image.
- **Stego-Image**: After embedding message into cover image is known as stego-image.
- **Stego-Key**: A key is used for embedding or extracting the messages from cover-images and stego-images.

II.LITERATURE REVIEW

1. METHOD OF IMAGE STEGANORAPH

[1] 1. Huffman Encoding and Transfer Domain Method

A. Embedding Algorithm
Input: An Ml*Nl carrier image and a secret image.
Output: A stego-image.

1. Obtain Huffman table of secret message/image.
2. Find the Huffman encoded binary bit stream of secret image.
3. Decompose the image by using wavelet transform.
4. Calculate size of encoded bit stream in bits.

5. Divide the carrier image into non overlapping blocks of size 8*8 and apply DWT on each of the blocks of the cover image.
6. Repeat for each bit obtained in step 3
(a) Insert the bits into LSB position of each DWT coefficient of 1st 8*8 block found in step 4.
7. Decompose the encoded bit stream of secret message/image obtained in step 2 into 1-D blocks of size 8 bits.
8. Repeat for each S-bit blocks obtained in step 6
(a) Change the LSB of each DWT coefficient of each 8*8 block (excluding the first) found in step 4 to a bit taken from left(LSB) to right(MSB) from each S bit block B.
9. Repeat for each bit of the Huffman table
(a) Insert the bits into LSB position of each DWT coefficient
10. Apply inverse DWT using identical block size
11. End.

B. Extraction Algorithm

Input: An Ml*Nl Stego-image.

Output: Secret image.

1. Divide the stego-image into non overlapping blocks of size 8*8 and apply DWT on each of the blocks of the stego-image.
2. The size of the encoded bit stream is extracted from 1st 8*8 DWT block by collecting the least significant bits of all of the DWT coefficients inside the 1st 8*8 block.
3. The least significant bits of all of the DWT coefficients inside 8*8 block (excluding the first) are collected and added to a 1-D array.
4. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
5. Construct the Huffman table by extracting the LSB of all of the DWT coefficients inside 8*8 blocks excluding Fust block and the block mentioned in step 3.
6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
7. End.

[2] **2. DWT Based Perfect Secure and High Capacity Image Steganography Method**

A. Embedding Algorithm

1. Apply the same level DWT on both the message data and the cover image data. Hence, Four *CCA* (approximation), *CCH* (horizontal), *CCV* (vertical) and *CCD* (diagonal) coefficients are generated as of the transformed cover image data. Similarly, *MCA*, *MCH*, *MCV* and *MCD* coefficients are generated as of the transformed pictorial message data.
2. Divide the *CCA* and *MCA* coefficients into 4*4 blocks which can be called as:
MCA= {Mai, 1<i< nm}
CCA= {CAj,1<j<nc}
where MAi and CAj are the ith and jth blocks of the MCA and CCA and nm and nc are the total number of 4× 4 blocks of the MCA and the CCA coefficients.
3. Find the most similar 4 × 4 blocks of the CCA and the MCA using RMSE pattern matching distance criterion, Save the most similar blocks numbers as key K and do this to find all the most similar blocks.
4. Apply inverse DWT on the cover image DWT coefficients.

B. Extraction Algorithm

1. Apply the same level DWT to the received cover image data.
2. Divide the *SCA* (approximation coefficients) coefficients into 4 × 4 blocks.
3. Using keys Ks, extract the approximation message DWT coefficients from the approximation cover image DWT coefficients.
4. Considered the high frequency message DWT coefficients as zero value.
5. Apply inverse DWT on the message DWT coefficients.

[3] **3. Dual Wavelet Transform Used in Color Image Steganography Method**

A. Embedding Algorithm

Step 1: Read the cover image as C. and check with size, contrast, brightness and etc.,
Step 2: Apply pre-processing on cover image C.
Step 3: C can be Separated into Channels R, G, B planes. (CR, CG, CB) Channels.
Step 4: Read the secret image as S. and convert the secret image into gray scale image as SG.
Step 5: By apply dual transform technique into CB and SG.
Step 6: Apply DWT/IWT extract the approximation coefficients of matrix A1 and detail coefficient matrices LH1, LV1, LD1 of level 1 of the CB as CB1.
Step 7: Apply DWT/IWT extract the approximation coefficient of matrix LA1 and detail coefficient matrices LH1, LV1, LD1 of level 1 of the SG as SG1.
Step 8: Perform fusion operation on image CB1 and SG1get fused image.
Step 9: Finally apply fused image with 2-D IDWT/IIWT and Band G Channels to form stego image as ST.

B. Extraction Algorithm

Step 1: Receive the stego image Perform a 2-D DWT/IWT at level of both stego image and known cover image.
Step 2: Apply fusion process on both stego image and cover image to get fused image.
Step 3: Separate the wavelet coefficients and take inverse DWT/IWT of fused image to reconstruct the scrambled image.
Step 4: Finally apply Modified Anti Arnold to Reconstruct the Secret Image.

[4] **4. Transforms, Wavelet Transforms and Hybrid Wavelet Transforms Method**

A. Embedding Algorithm

Step 1: apply transforms on cover image it results into transformed cover image.
Step 2: On the other hand, normalize the covert message to be hidden by normalization factor.
Step 3: Lower energy block of transformed cover image is used for embedding of covert message.
Step 4: Apply inverse transforms on improved cover image this will generate the stego image. Stego image same as cover image.

B. Extraction Algorithm

Step 1: First apply transforms on stego image.
Step 2: Extract the energy block where we embedded the covert message from transformed stego image.
Step 3: DE normalize the extracted data using normalize
factor.
Step 4: Results the retrieved covert message which is exactly same as covert message to be hidden.

[5] **5. Discrete Wavelet Transformation and Artificial Bee Colony Optimization**

A. Embedding Algorithm

Step 1: Read input image.
Step 2: Perform DWT to divide image into low and
high frequency coefficients.
Step 3: Create a mask of 4X4 matrix.
Step 4: For every 4 bit in the image if the pattern matches with any bit pattern in the mask then it would proceed to contour.
Step 5: The contour region is identified on the basis of a signed distance value. If the difference between two neighbouring pixels is greater than 10 then the bit is selected.
Step 6: The calculated bit sequence is then passed to ABC algorithm.
Step 7: The optimum solution is obtained using the value of fitness function.
Step 8: On each row at each position provided by ABC, one bit of binary pattern would be embedded.
Step 9: Calculate PSNR, MSE and Embedding Capacity.

B. Extraction Algorithm

Step 1: Use stego-image.
Step 2: For each position specified ABC perform step 3.
Step 3: Message= main_image (pos_bit).

2. A COMPARISON OF THE IMAGE STEGANOGRAPHY METHODS

Table 1 Comparison Table

Method	**Data hiding Capacity**	**Resistance To Attacks**	**Domain**	**Complexity**
Huffman Encoding and Transfer Domain	High	High	Frequency	Complex
DWT	High	Low	Frequency	Complex
Dual wavelet transfer	High	Low	Frequency	Complex
Method	Data hiding Capacity	Resistance To Attacks	Domain	Complexity
Transforms, Wavelet Transforms and Hybrid Wavelet Transforms	High	High	Frequency	complex
DWT & Artificial Bee Colony Optimization	High	Low	Frequency	Complex

Huffman Encoding and Transfer Domain method provide the higher embedding capacity, low distortion rate, good invisibility, high PSNR rate and also improve the image quality and security. This method is robust against any geometrical distortion such as rotation, translation, scaling, cropping etc. DWT Based Perfect Secure and High Capacity Image Steganography Method provide the higher embedding capacity, perfect security, high PSNR rate, low resistance attack. Using this method cover image data unchanged. Dual Wavelet Transform Used in Color Image Steganography Method provide high embedding capacity, low resistance, high security, high PSNR, more Imperceptivity and good quality image. Transforms, Wavelet Transforms and Hybrid Wavelet Transforms Method provide higher embedding capacity, High resistance to attack, good balance of imperceptibility and robustness. Discrete Wavelet Transformation and Artificial Bee Colony Optimization provide higher embedding capacity and increasing the visual image quality. It's also provide the higher resistance to attack. In image steganography using different method for secure invisible communication Huffman Encoding and Transfer Domain method provide the better result than other method

III. CONCLUTION

We have used five method Huffman Encoding and Transfer Domain, DWT, Dual Wavelet Transform Used in Color Image Steganography, and Discrete Wavelet Transformation and Artificial Bee Colony Optimization method for the invisible communication of image steganography. The result of Huffman encoding and transfer domain method and transform wavelet transforms method are almost same, but the Huffman Encoding and Transfer Domain method provide the higher embedding capacity, low distortion rate, good invisibility, high PSNR rate and also improve the image quality and security. This method is robust against any geometrical distortion such as rotation, translation, scaling, cropping etc. so, Huffman Encoding and Transfer Domain method is better than the other method.

IV REFERENCES

[1] M. Vijay, V. VigneshKumar, "Image Steganography Algorithm based on Huffman Encoding and Transform Domain Method ", IEEE Fifth International Conference on Advanced Computing (ICoAC) 2013.

[2] Mohammad Reza Dastjani Farahani, Ali Pourmohammad, "A DWT Based Perfect Secure and High Capacity Image Steganography Method", IEEE International Conference on Parallel and Distributed Computing, Applications and Technologies 2013.

[3] Prabakaran G, Dr. Bhavani R, Sankaran S, "Dual Wavelet Transform Used in Color Image Steganography Method", IEEE, International Conference on Intelligent Computing Applications 2014.

[4] Dr. Sudeep D. Thepade (Dean R & D, Professor), Mrs. Smita S. Chavan (Asst. Professor), "Vigorous Image Steganography with Transforms, Wavelet Transforms and Hybrid Wavelet Transforms" IEEE India Conference (INDICON) 2014.

[5] Amandeep Kaur, Rupinder Kaur, Navdeep Kumar, "Image Steganography using Discrete Wavelet Transformation and Artificial Bee Colony Optimization", 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.

[6] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.

[7] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013.