ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

A Survey on Secure and High Capacity Image Steganography Techniques

Usha B A[1], Dr. N K Srinath[2], Dr. N K Cauvery[3] Aditya Nanjangud[4], Abhineet M Deshpande[5], Anthony Rebello[6]

Assistant Professor, Department of CSE, R V College of Engineering, Bangalore, India [1]

Professor and Dean PG Studies, Department of CSE, R V College of Engineering, Bangalore, India [2]

Professor & HOD, Department of ISE, R V College of Engineering, Bangalore, India [3]

UG Final Year, Department of Computer Science & Engineering, R V College of Engineering, Bangalore, India[4,5,6]

Abstract: Steganography is the art of hiding data in plain sight. It is the science of "invisible" communication. In image steganography the embedding of data is done such that the Human Visual Syaytem(HVS) does not recognize that the image has a hidden message in it. A trade-off between security and capacity is often made in standard of steganographic techniques. In this paper some more Secure and High Capacity Image Steganography Techniques to explore their potentials and limitations are presented

Index Terms: Secure, DWT, IWT, BPCS, information-hiding, image processing, high capacity

I. INTRODUCTION

The word steganography has its origin from Greek words "steganos" which means "covered" and "graphei" meaning "writing", meaning concealed writing.

The data to be hidden is concealed as part of content in an image, audio or a video file. An information-hiding system is characterized by having three different aspects that contend with each other. These are, capacity, security, and robustness as shown in Fig. 1 [1].

Capacity refers to the amount of information that can be hidden in the cover medium. Security is the ability of the system to prevent an attacker to identify and extract hidden data. Robustness is the amount of changes the stego medium can withstand before an attacker can destroy hidden information. Achieving both high security and high capacity is often met with challenges as mechanisms for achieving high security.

It may not allow for high capacity and vice-versa. Having higher capacity may degrade the quality of the stego-image to an extent that it may be vulnerable to detection and steganalysis. High security always involves less data spread across the image so that the stego-image is secure when subject to steganalysis.

Steganographic methods are broadly classified into two categories spatial domain methods and transform domain methods. In spatial domain methods the image pixel values are processed to carry out steganographic operations.

Whereas in transform domain methods image is transformed into different domain and the processing is done by working on the transformed coefficients.

The advantage of the spatial domain

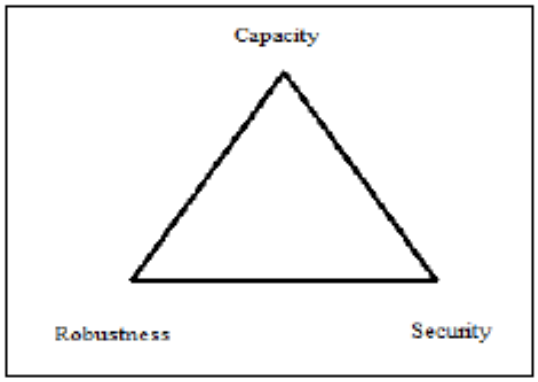

Fig. 1. Capacity Security Robustness Triangle

methods is simplicity. Transform domain methods are computationally complex when compared to spatial domain methods but more robust to signal processing operations.

Any steganographic technique's performance is measured by Peak Signal to Noise Reatio(PSNR) values. Higher PSNR values indicate that the performance of the system is better. In Any technique if the PSNR value above 30dB it is considered to be good technique.

II. INTEGER WAVELET TRANSFORM

One of the transform domain techniques is using Integer Wavelet Transform (IWT) for domain transformation. The Wavelet Transform provides a time-frequency representation of the signal. IWT is a more efficient approach to lossless compression. The coefficients in this transform are represented by finite precision numbers which allows for lossless encoding. This wavelet transform maps integers to integers. In case of Discrete Wavelet Transform, if the input consists of integers (as in the case of images), the resulting output no longer consists of integers. Thus the perfect reconstruction of the original image becomes difficult. However, with the introduction of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

Wavelet transforms that map integers to integers the output can be completely characterized with integers [2].

Hemalatha S et al. have come up with a novel idea of embedding two grey scale images of size 128x128. They are used as secret images in a color cover image of size 256x256 [2]. The following are the embedding and extracting mechanism:

Embedding:
(1) Represent the cover image C in YCbCr color space
(2) Obtain single level IWT of secret-images S1, S2 and Cb, Cr component of C.
(3) The resulting transformed matrix consists of four sub-bands corresponding to LL, LH, HL and HH sub bands.
(4) LL sub band of Cb is used to hide one secret image and LL sub band of Cr is used to hide another secret image. Then the two keys K1 and K2 corresponding to two secret images are obtained as follows:
(5) The sub-images CLL and SLL are subdivided into non-overlapping blocks BCk1 and BSi.
(6) Every block BSi, is compared with block BCk1. The pair of blocks which have the least Root Mean Square Error is determined. A key is used to determine the address of the best matched block BCk1 for the block BSi.
(7) Encrypt the key and store in the image.

Recovering:
(1) Represent the stego image G in YCbCr color space. Let it be GyGcbGcr
(2) Obtain IWT of Gcb and Gcr and obtain the keys K1 and K2.
(3) Divide GcbLL into non overlapping blocks of size 2x2
(4) Obtain the blocks that are nearest approximation to the original blocks of S1LL using K1
(5) Rearrange the blocks to obtain S1LLnew
(6) Obtain the secret image S1
(7) Similarly obtain S2 from GcrLL using K2

III. DISCRETE WAVELET TRANSFORM(DWT)

On applying DWT the four sub-bands of images separating the high frequency and low frequency information is obtained. and if the secret information is inserted in the high frequency coefficients of the sub-bands it is very difficult to detect the steganography in the stego-image. After applying 2D-Haar DWT on a 4 X 4 image we get the four sub-bands of the image each of size are 2 X 2 [3], these are

- LL: approximate area that includes information of the average of the image.
- HL: horizontal area that includes information about the vertical edges/details in the image.
- LH: vertical area that includes information about the horizontal edges/details in the image.
- HH: diagonal area that includes information about the diagonal details, e.g., corners, in the image

The proposed method is a color image steganography so when a color image (RGB) of size 512 X 512 is converted into its matrix formt the three classes of the color that is red,

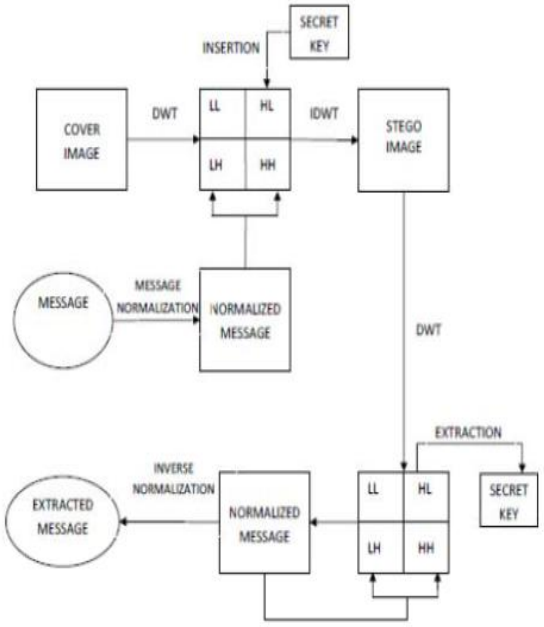

Fig. 2. DWT process

green and blue is obtained as a result of the matrix of coefficient of size 512 X 512 X 3. So when DWT is applied to a color image four sub-bands of image each of size 256 X 256 X 3 is obtained. In this proposed method a secret key is given for embedding message into the cover image, the exact key is needed for extracting the message from the stego-image. The information of the key is stored in the HL sub-band of the image. The message embedding and extracting procedures are described in Fig. 2.

Message embedding algorithm:
Step 1: Apply 2D-Haar DWT of the cover image, where we get the four sub-bands which separate the high and low frequency information.
Step 2: Calculating the length of the message (n) and save it to the sub-bands HL.
Step 3: Convert the each character of the message into its ASCII format.
Step 4: Normalizing the ASCII format of the message using the following formula Normalized message = ASCII value of each character/ n
where n is the length of the message
Step 5: Divide the Normalized message into two parts so that first part is to be inserted in the sub-band LH and the second part of the message in the sub-band HH.
Step 6: Message is inserted into all the color components of LH and HH sub-bands that are Red, Green and Blue color components. Message is inserted starting from the last column of each of the color components from top to bottom depending upon the length of the message.
Step 7: If the message length is larger than the No. of rows of each of the color components of each of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

the sub-bands then rest of the normalized message will go to the second last column of the each component, in this way all the normalized message is to be distributed.

Step 8: Insert the secret key in the HL sub-band.

Step 9: At the last step we have to take the Inverse Discrete Wavelet Transformation (IDWT) so that we can get the stego-image.

Message extraction algorithm:

Step 1: Apply 2D-Haar DWT to the stego-image so as to separate all the four sub-bands that are LL, HL, LH and HH

Step 2: Ask the user to inserting the secret key (k).

Step 3: Extract the secret key from the HL sub-band which was inserted at the time of stego-image.

Step 4: If the secret key (K) match with the saved key in the sub-band HL, then go to step 4 otherwise to step 8.

Step 5: Find the length of the message from the sub-bans HL so that we can calculate from which column to which row we can extract the coefficient of the color components of each of the sub-bands LH and HH.

Step 6: The inverse normalization is carried out by multiplying each of the extracted coefficients with the length of the message.

Step 7: Convert each of the extracted coefficients into character format to form the message.

Step 8: Display the message that the secret key did not match.

H S Manjunatha Reddy et al. have come up with a fusion based technique utilizing the DWT where cover image is used in extracting the embedded data [4]. The process of fusion of cover and secret image and the extraction of secret data is shown in Fig. 3 and Fig. 4 respectively.

IV. BIT-PLANE COMPLEXITY SEGMENTATION STEGANOGRAPHY (BPCS)

Palette based methods make use of a color palette which has all the colors required for an image stored as a combination of RGB or a color vector. Palette based methods are usually dependent on the order of the color vectors. Michiharu Niimi et al. mentions a BPCS steganography technique to palette-based images [5].

In BPCS, a complexity measure measures to what degree a binary image pattern contains significant information for the visual system. In this paper, we shows a method that does not sort the color vectors or depend on their order.

The brief steps of the technique is as follows:

Step 1: Produce R, G and B color component images from the original palette-based image.

Step 2: Apply BPCS-Steganography to the G image. We denote a G image with information embedded as a G', image.

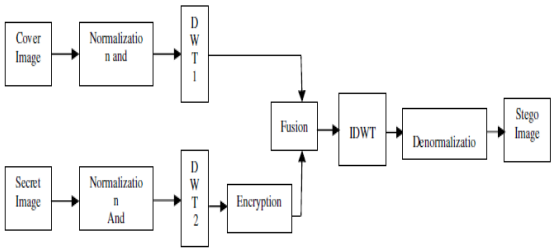

Fig 3. Encoding

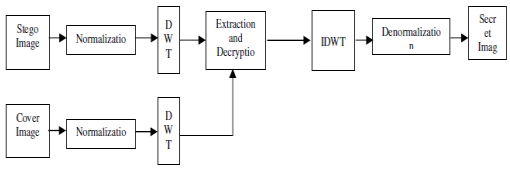

Fig 4. Extraction

Step 3: Produce a palette from the G', R, and B images. Color quantization operations are done after the above steps are carried out. BPCS is also used to find the capacity for embedding.

Payload encryption mapping is done between original payload and encrypted payload [6]. Drawback is that mapping table required at the decoding end.

III. CONCLUSION

Encryption provides data security by making data either inaccessible or even if accessible renders it useless to the intruder. Steganography takes data confidentiality and security to a new level as it introduces an element of uncertainty of where the data is hidden, Secret data is hidden is ordinary looking messages and files making the existence of the message undetectable. This paper reviews a few majorly used secure and high capacity image steganography techniques. The experimental results published in these papers show that these methods have relatively high PSNR values. Clearly IWT techniques are better in terms of image quality of the secret image as reconstruction of the images is better in IWT than in DWT. IWT technique gives a PSNR value of 44.7 dB [2]. DWT techniques are used more widely than IWT. DWT yields PSNR values of more than 50dB in multiple cases [3]. BPCS gives good PSNR values above 30dB in all cases [5]. These values show that the above mentioned techniques are all viable options for secure and high capacity steganography.

REFERENCES

[1] Ali A. Al-Ataby and Fawzi M. Al-Naima, "High capacity image steganography based on curvelet transform," Developments in E-systems Engineering (DeSE), 2011, 6-8 Dec. 2011

[2] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath, "A secure and high capacity image steganography technique," Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013

[3] Juned Ahmed Mazumder and Kattamanchi Hemachandran, "A high capacity and secured color image steganographic technique using discrete wavelet transformation," International Journal of Computer Science and Information Technologies, Vol. 4 (4) , 2013, 583 - 589

[4] H S Manjunatha Reddy and K B Raja, "High capacity and security steganography using discrete wavelet transform," International

Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)

[5] Michiharu Niimi, Hideki Noda, Eiji Ka Waguchi and Richard O. Eason, "High capacity and secure digital steganography to palette-based images," Image Processing. 2002. Proceedings. 2002 International Conference (Volume:2) on, 2002.

[6] K B Raja, Vikas , Venugopal K R, and L M Patnaik, "High capacity lossless secure image steganography using wavelets," Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on 20-23 Dec. 2006.

[7] Saeed Sarreshtedari and Shahrokh Ghaemmaghami, "High capacity image steganography in wavelet domain," Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE 9-12 Jan. 2010.

[8] M. Fahmy Tolba, M. AI-Said Ghonemy, Ismail Abdoul-Hameed Taha and Amal Said Khalifa "High Capacity Image Steganography using Wavelet-Based Fusion," Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on (Volume:1) 28 June-1 July 2004

[9] Rosanne English "Comparison of high capacity steganography techniques," Soft Computing and Pattern Recognition (SoCPaR), 2010 International Conference of 7-10 Dec. 2010.