ISSN 2349-9842, Volume 1, Issue 1, March 2014

International Journal of Innovative Trends and Emerging Technologies

A MODIFIER DIGITAL IMAGE STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM

V.RAJKUMAR

Department of Computer science and Engineering, Dhaanish Ahmed College of Engineering

E-mail :rajkumarvmecs@gmail.com

***Abstract*--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 can be achieved by hiding the existence of information within seemingly harmless carriers or cover the carriers may be text, image, video, audio, etc. In this project, we proposed hiding large size of secret images in to the small size of cover image; we modified secure and high capacity using steganography for hiding the images. Arnold transform is performed to scrambles the secret image. Discrete Wavelet Transform (DWT) is executed in both secret and cover images which followed by Alpha blending process. The Inverse Discrete Wavelet Transform (IDWT) is applied to get the stego image. We have inquired the performance of our scheme by comparing various qualities of the stego image and cover image. The result shows it is highly secured with certain strength and good perceptual invisibility.**

Key words: Steganography, DWT, Arnold Transform, Alpha Blending.

1.INTRODUCTION

Steganography is the act of secret communications, which means only the sender and receiver are aware of the secret communication. To achieve this, the message is typically hidden within innocent-looking objects known as cover object. The objective is to embed a secret message so that its very presence in the stego object that cannot be proved, the main requirement of steganography is undetectability, which involves communicating secret data in an appropriate multimedia carrier, e.g., video, audio,image files etc. The purpose of steganography is not to keep others from knowing the hidden information it is to keep others from thinking that the information even exists. If this steganography method causes someone to suspect the carrier medium, then the method has failed. Encryption and steganography attain separate goals. The encryption encodes data such that an unintended recipient cannot determine by its intended meaning. Steganography does not alter data to make it unusable to an unintended recipient. Instead, the stenographer attempts to prevent an unintended recipient from suspecting that the data is there.

The wavelet transform has an emerged as a cutting edge technology, within the image compression. The wavelet based coding provides significant improvements in image quality at higher compression ratios. For the past few years, a variety of powerful and difficult wavelet-based schemes for image compression have been developed and implemented. Further those Schemes are being designed to address the requirements of very different kinds of applications such as internet, remote sensing, mobile applications, digital library, military application, medical imagery and e-commerce etc.,

2 *Related Work*

The Recent researches are using the discrete wavelet transform (DWT) is applied in image compression format (JPEG) 2000 and Motion photographic group (MPEG)-4. Chen.P et al., [1] have proposed secrete message is embedded in the high frequency co-efficient of the wavelet transform by leaving the low frequency co-efficient sub-band unaltered.

Raja.K.B et al., [2] have proposed a novel image steganographic technique in integer wavelet transform domain. Babita Ahuja, et aI., [4] proposed for more hiding capacity achieved by Filter Based scheme in Steganography. Jan Kodovsky and Jessica Fridrich [3] worked out the specific design principles in Steganographic scheme for the JPEG format and their security.

Mohamed Ali Bani Younes, et. aI., [5] proposed a steganographic approach for hiding. This approach hides the least significant bits insertion to hide the data within encrypted image data. Chang-Chu Chen, et al., [6] have proposed that data hiding scheme was a modification of the LSB based Steganography using the rule of reflected gray code.

In this paper we presents a new method of data hiding in the discrete wavelet transform coefficients of the cover image to maximize the hiding capacity to overcome the drawback. The Arnold transformation is performed to scramble the secret image to hide into the wavelet coefficients in the low frequency to increase the system security.

In chapter three we discuss about the proposed method, DWT and IDWT, Arnold transformation and implementation of steganography model, Noise Attacks, Chapter four describes the experimental results and analysis for the proposed steganography method and noise attacks. In Chapter five the conclusion of the paper and suggests for the future improvements of the system.

3 PROPOSED SYSTEM

In our proposed method, we use three types of process. The first method is encoding and second method is decoding process, the third method is Noise Attacks, in encoding process the cover image and scrambled secret image in order to increase the security level by using DWT. The alpha blending matrix is obtained for the cover image and secret image to improve the system security, then Apply Arnold transform with secret key on secret image and get the scrambled secret image. It gives the more security and robustness to our process. After the Alpha blending operation is done, we apply the IDWT to get the stego image. The decoding process is the reverse process of the encoding model, in decoding process the DWT is performed on the stego-image and known cover image. Then alpha blending performed on both images and it applies the IDWT on Alpha blend image and gets the scrambled secret image. We perform Arnold transformation with secret key to recover the original secret image from the stego image. The encoding and decoding process clearly exposed idea about our model.The noise attack is performed to retrieving the secret image from the affected stego image.

A. **Scrambling Based on Arnold Transform:**

The Arnold transformation is proposed by V. J. Arnold in research of Random theory, it is a class of cropping transformation, here we take a digital image as a matrix, and it will become disordered after performing Arnold transform. The Arnold transformation of this matrix and then a new matrix can be obtained after the image scrambling processing. Set the image pixel coordinates. Consider N is the order of the image matrix, i, j € 0, 1, 2. . . N -1) and the Arnold transform is as in (1):

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \text{ (Mod N)} \quad (1)$$

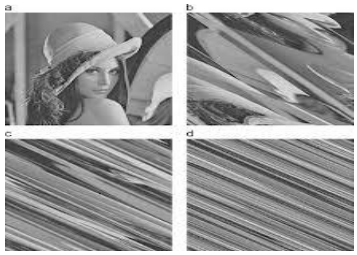


Fig 3.1. Arnold Transform scrambled image

The image can do many no of iteration each iteration number can be used as a secret key for extracting the secret image from the stego image. This transformation gives more security and robustness to our process.

B. Discrete wavelet transforms:

The Wavelet transform are defined over the finite interval having an average value as zero. The basic idea of the wavelet transforms which represent the random function as a superposition functions. The wavelet transform uses I-D sub band for decomposition process in which an I-D set of sample is converted into the low pass sub band (Li) and high-pass sub band (Hi).

The low-sub band represents the low-frequency of the cover image. The high-sub band represents remaining part of the original cover image. In 2-D sub band decomposition process is executed twice, first in horizontal direction, second in the vertical direction.

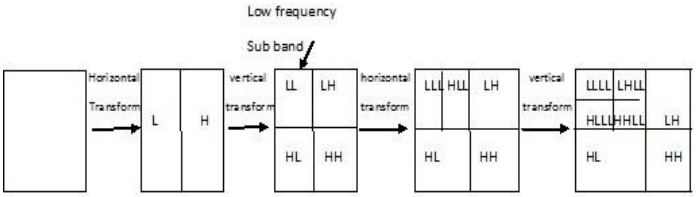


Fig: 3.2. DWT represents 2-D low level sub bands

For decomposing first 1-D level sub band is applied, then applying the 2-D sub band for

decomposition the existing Low Level sub band (LLi). This process done in multiple transform levels, the Low resolution sub band and high resolution sub band represents in horizontal, vertical and diagonal respectively (LHi, HLi, HHi) in the original cover image.

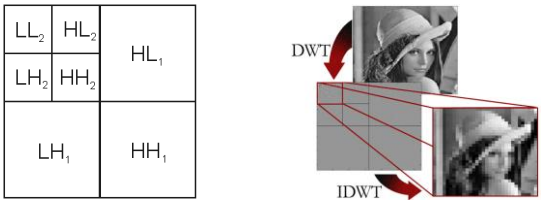


Fig 3.3 2D sub band.

C. Alpha Blending

Alpha blending is the process of combining a translucent foreground color with a background color, thereby producing a new range of color. The degree of the foreground color is transparency may range from completely transparent to completely unintelligible. If the foreground color is completely transparent, the new color will be the background color. Conversely, if it is completely transparent, the blended color will be displayed in front, the range between these extremes, in which case the blended color is calculated as a weighted average of the foreground and background colors. the graph which provides the alpha blending functions that work for RGB values, The alpha blending functions does not work when a 256-color virtual buffer is active.

D. Implementation of modified Steganography model

In the encoding process which includes DWT, Arnold transform and Alpha blending, IDWT is applied for receiving stego image. The Decoding process includes DWT, Arnold transform and Alpha blending, IDWT to receive the secret image, in Noise Attacks which retrieves the secret image from the attacked cover image.

I. Encoding process

In encoding process the small size cover image and large size scrambled secret image with secret key was reassigned by DWT transform and then by alpha blending process to increase the system security. IDWT was performed to reform the stego image.

The secured stego image was transfer to any communication media. The Architecture represents Encoding process in Fig: 3.4.

Algorithm for encoding process.

Step1: take small size cover image (N*N size) and large size secret image (2N*2N size) for pre position.

Step2: Perform a 2-D DWT at level 1 of the Cover image (N/2 * N/2 size) for scrambling.

Step3: Apply Secret key with Arnold transformation

On image S and get the scrambled secret Image (SS).

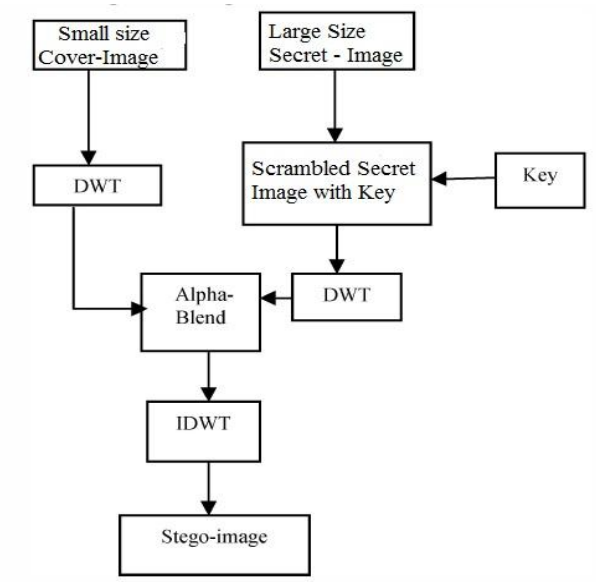


Fig: 3.4. Architecture of Encoding process.

Step4: Again perform a 2-D DWT at level 2 of the

Scrambled secret image SS (N/2 *N/2 size).

Step5: Again DWT is performed for the secret image to scramble the secret image (SS).

Step6: Apply Alpha blending operation on image C and image SS.

Step7: Finally, perform 2-D IDWT to form the Stego image (SI).

II. Decoding Process

The reverse process of the encoding is done with the stego image for retrieving the secret image using IDWT followed by alpha blending, DWT process.

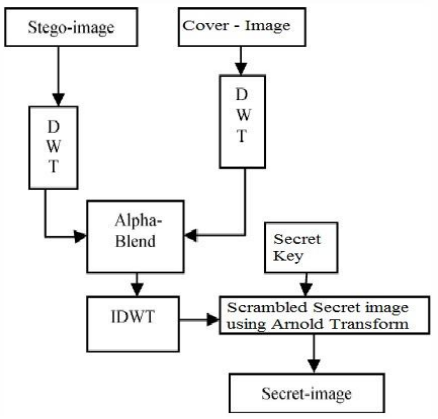


Fig: 3.5. Architecture of Decoding process.

The secret key was applied to get the original secret image. The representation of decoding process was given in the Fig 3.5.

Algorithm for Decoding Process.

Step1: Received the Stego image.
Step2: Perform a 2-D DWT at level 1 of the SI and known cover image.
Step 3: Apply Alpha blending on both image SI and image C.
Step 4: Next separate the wavelet coefficients and take IDWT to reform the SS.
Step 5: Finally perform the Arnold transformation with secret key and get the original Secret image S.

II. Noise Attacks

Noise Attack is a form of noise typically seen on images. The attacks may be in many forms, It represents itself as randomly occurring white and black pixels in salt and pepper attack and it represents as cropped images in cropping attacks etc., The secret image is hidden in low frequency of allover the cover image. Even the stego image is attacked by the hackers by using the discrete wavelet transform the secret image can be retrieved from the infected image and the original image can be identified by the receiver, the PSNR value will be measured it will be aroung 35 db.

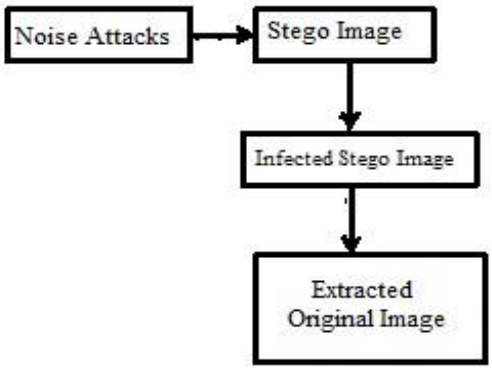


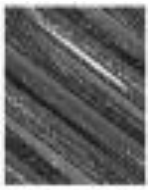
Fig: 3.6 Block Diagram of Noise Attacks

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

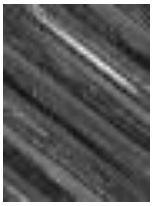
The performance of this method has been evaluated using Matlab R2007a. In our experiment, we have tested many sample images by using this proposed algorithm. With the representation we have given leaves.jpg (316X380) and Host.jpg (458x500) are consider as small size cover images and cman.jpg (560X560) is large size secret image. The leaves and Host images resize of 300x300 sizes and then cman.jpg resize of 600x600 sizes have been considered for our experiment. We have tested the various alpha values in between ranges from 0.05 to 0.01. to improve the embedding strength factor alpha and improve the quality level of stego-image. Then, we tested full secret load 600x600 was embedded into 300x300 size, which is obtained by apply 2 level DWT. The next level of DWT also performed but the approximation band is not clear in the level. The corresponding experimental results should be shown in Fig 4.1

Cover image (300X30 Secret Image (600X600) Arn – sec(600X600)





Stego Image Rec-Image (300X300) Orig- sec image (300X300)


Attacked stego Image

Retrieved secret image

Fig: 4.1 Shows a encoding, decoding process of cover image (Host.jpg) and secrete image (cman.jpg), secret image retrieved from noise attacked image.

A. Performance Analysis:

The quality of stego images is the most important property for steganography system, it is hard to detect by detectors and we use Peak Signal to Noise Ratio (PSNR) to measure the difference between an original cover image and stego image in db. The PSNR and MSE of cover image verses stego image respectively, the definitions are in (2) and (3)
Were

$$PSNR(dB) = 10 * \log(\frac{255^2}{MSE}) \qquad (2)$$

$$MSE = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{ij} - B_{ij}|)^2}{x * y} \qquad (3)$$

Table: 1 Comparison of various qualities of cover images and stego image with secret-images

Cover–image	Secret-image	MSE	PSNR
host.jpg316*380	cman.jpg458*500	0.7542	45.320
leaves.jpg786*1024	sec.jpg 300*450	0.3749	43.391
Lena.jpg 316*380	Camera.jpg 300*450	1.0440	45.943

PSNR values are measured in db

MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N. It is hard for the Human eyes to see the difference between original cover image and stego image when the PSNR ratio is larger than 30dB, The image quality factors MSE, PSNR and other quality measurement are measured, The effectiveness of the stego image formation proposed has been studied by calculating MSE and PSNR for the two digital images, The result data shows that for less MSE and High PSNR value,

The Optimal level of PSNR ranges from 35db to 45 db and MSE is as less as possible, the PSNR value is high when compare to the various methods it gives more robustness to our algorithm.

4 CONCLUSIONS

This paper deals with the techniques in discrete wavelet transform as associated to gray scale image. A new and secure steganography method for embedding large size secret image into small size cover image, in addition which gives more capacity and high security to transfer images in communication media. The experimental results show that this method gets stego-image with invisibility of secret image with high security and certain robustness, the PSNR value is around 35 to 45 db, this method is robust against various attacks such as salt and pepper noise, cropping attack, etc... even after the stego image is affected the PSNR value is aroung 35db which gives robustnes to the image.
In future this method can be tested with the various wavelet transform techniques with various image quality measurements and it can be tested with the various types of attacks.

REFERENCES:

[1] P.Chen, and H.Lin,"A DWT approach for image steganography", International Journal of applied Science and Engineering", volume.4, 3:pp 275:290,2006.

[2] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal,L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" International conference on Communication Systems Software", pp. 614-621, 2008.

[3] Jan Kodovsky, Jessica Fridrich "Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" Proceedings of SPIE, the International Society for Optical Engineering", vol. 6819, pp. 681902.1-681902.13, 2008.

[4] Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography,"

International Journal of Recent Trends in Engineering“, vol. I, no. I, pp.672-674, May 2009.

[5] Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," International Journal of Computer Science and Network Security", vol. 8, no. 6, pp.247-257, 2008.

[6] Chang-Chu Chen, and Chin-Chen Chang, "LSB-Based Steganography Using Reflected Grey Code, “The Institute of Electronics, Information and communication Engineers Transaction on Information and System, “, vol. E91-D (4), pp. 1110-1116, 2008.

[7] WWW.Wikipedia free encyclopedia, steganography, http://en.wikipedia.orglwiki/Steganography.

V.RAJKUMAR Received his Bachelor of Technology In SRM University and Master Of Engineering degree In Computer Science and Engineering from Anna University.. Currently he is serving for AIAIE’s.