A NOVEL WAVELET TRANSFORM METHOD BASED STEGANOGRAPHY FOR TRANSMITTING IMAGES

Mrunalini M.Chaudhari[1], Kanaksing N. Pawar[2]

[1] *P.G. Department of Electronics Engineering, S.S.V.P.S's B.S.D COE, Dhule, M.S. (India)*
[2] *H.O.D, P.G Department of Electronics Engineering, S.S.V.P.S's B.S.D COE, Dhule, M.S (India)*

ABSTRACT

The art of passing information in a manner that the very existence of the message is unknown is known as steganography. The detection of steganographically encoded packages is called steganalysis. Many different carrier file format can be used for steganography but now mostly preferred carrier is digital image because of their frequency on the communication medium such as internet. In this paper a novel steganographic technique using Stationary Wavelet Transform (SWT) for transmitting pictures is discussed. Two different techniques are proposed one using three level wavelet decomposition, taking a single plane of the cover image for embedding and processing the image as 4 x 4 blocks with swapping and second using single level wavelet decomposition.

Keywords: Discrete Wavelet Transform (Dwt), Stationary Wavelet Transform (Swt), Steganography, Steganalysis

I. INTRODUCTION

Modern steganography is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures, video, audio and even typeset text. This makes sense for a number of reasons. First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and extract messages. Secondly, extraction itself can be automated when the data is electronic, since computers can efficiently manipulate the data and execute the algorithms necessary to retrieve the messages.

Electronic data also often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages. Steganography is the study of techniques for hiding the existence of secondary message in the presence of a primary message. Steganography is the art and science of hiding the fact that communication is taking place. The primary message is referred to as the carrier signal or carrier message and the secondary message is referred to as the payload signal or payload message. Generally, in steganography the following operations are performed:

•Write a non-secret cover message

•Produce a Stego-message by concealing a secret message embedded on the cover message by using a stego-key send the stego-message over the insecure channel to the receiver.

•At the receiver end, on receiving the stego-message, the intended receiver extracts the secret embedded message from the stego- message by using a pre-agreed stego-key.

The detection of steganographically encoded packages is called steganalysis [2]. The simplest method to detect modified files, however, is to compare them to the originals. To detect information being moved through the

graphics on a website, for example, an analyst can maintain known-clean copies of these materials and compare them against the current contents of the site.

The differences, assuming, that the carrier is error free, will compose the payload. In general, using an extremely high compression rate makes steganography difficult, but not impossible; while compression errors provide a good place to hide data, high compression reduces the amount of data available to hide the payload in, raising the encoding density and facilitating easier detection, in the extreme case, even by casual observation [3].

The exchange of information is greater today than at any other time in history, and with the way technology is improving, this exchange will only become greater. The threat of a group or individual misusing standard channels of communication to send stolen information, or communicate a plan against a nation, is more likely now than ever [4]. Due to the nature of these communications, the need for a means to hide them is ever present; this is where steganography comes into play. Through the use of steganography, information can be transmitted while being disguised within another piece of data. Significant amounts of data can be moved through common means of electronic communication, with little threat of detection.

This data can be transmitted with the hidden information included, and travel across networks looking like normal traffic. Any third party that intercepts the data will not expect it to contain such a secret. Implementation of steganography is not hard to achieve, and there are multiple variations of programs that will encode and decode information. Hiding data through steganographic means has become easier due to the availability of free programs online. In addition, the number of technologically adept individuals is increasing on a daily basis. The ability to deal with steganography will become a more crucial skill in future information flows.

II. IMAGE STEGANOPGRAPHY

1. During the cold war two the Microdot technology developed by Germans which prints the clear good quality photographs shrinking to the size of a dot.

2. In Greece they select a person to send message by shaving their heads off. They write a secret message on their head and allow growing up their hair. Then the intended receiver will again shave off the hair and see the secret message.

3. During the world war two the secret message was written in invisible Ink so that the paper appears to be blank to the human eyes. The secret message is extracted back by heating the liquids such as milk, vinegar and fruit juices.

A new Image Steganography scheme is proposed in this paper. Based on different requirements of applications. According to the simulation results, the PSNR and MSE are still a satisfactory value even the highest capacity case is applied. This is due to the different characteristics of SWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the original image).

In the near future, the most important use of steganographic techniques will probably lie in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down [5].

2.1 Discrete Wavelet Transform

Discrete wavelet transform is a multi-resolution decomposition of a signal[6]. The low pass filter applied along a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal. The two-dimensional wavelet transform that we describe can be seen as a one-dimensional wavelet transforms along the x and y axes. Mathematically the wavelet transform is convolution operation, which is equivalent to pass the pixel values of an image through a low pass and high pass filters. The image is represented by two dimensional signal functions; wavelet transform decomposes the image into four frequency bands, namely, the LL1, HL1, LH1 and HH1 bands. H and L denote the high pass and low pass filters respectively. The approximated image LL is obtained by low pass filtering in both row and column directions. The detailed images, LH , HL and HH contains the high frequency components. To obtain the next coarse level of wavelet coefficients, the sub Â band LL1 alone is further decomposed and critically sampled. Similarly LL2 will be used to obtain further decomposition. By decomposing the approximated image at each level into four sub-images forms the pyramidal image tree. These results in two-level wavelet decomposition of image, the two-level DWT decomposition is shown in Fig.1.

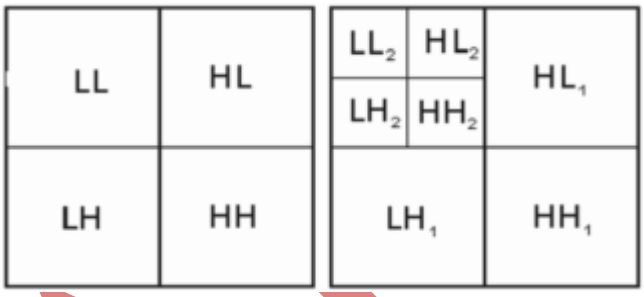

Figure 1: scale and 2-scale2 dimensional discrete wavelet transform.

2.2 Stationary Wavelet Transform

The Stationary wavelet transform (SWT) [7] is a wavelet transform algorithm designed to overcome the lack of translation-invariance of the discrete wavelet transform (DWT). Classical DWT suffers a drawback; the DWT is not a time- invariant transform. This means that, even with periodic signal extension, the DWT of a translated version of a signal X is not, in general, the translated version of the DWT of X. Translation-invariance is achieved by removing the down samplers and up samplers in the DWT and up sampling the filter coefficients by a factor of $2^{(j-1)}$ in the j^{th} level of the algorithm. In SWT the output at each level contain the same number of samples as input, hence the SWT is inherently redundant scheme. This algorithm is more famously known as "*algorithme à trous*" in French (word *trous* means holes in English) which refers to inserting zeros in the filters. It was introduced by Holschneider et al. [8].

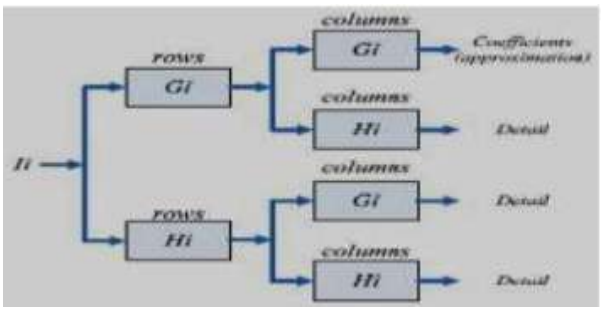

Figure 2: 2d SWT decomposition scheme

The 2D Stationary Wavelet Transform (SWT) is based on the idea of no decimation. It applies the Discrete Wavelet Transform (DWT) and omits both down-sampling in the forward and up-sampling in the inverse transform [9]. More precisely, it applies the transform at each point of the image and saves the detail coefficients and uses the low frequency information at each level. The Stationary Wavelet Transform decomposition scheme is illustrated in Fig.2 where Gi and Hi are a source image, low pass filter and high-pass filter, respectively. Fig.2 shows the detail results after applying SWT to an image using SWT at 1 to 4 levels. A few applications of SWT are, signal denoising and pattern recognition.

III. METHOD-1 SINGLE LEVEL WAVELET DECOMPOSITION

3.1 Embedding Process

In this embedding process we embed the secret image or stego image on to the cover image. The cover image is made up of three channels Red(R), Green (G), Blue (B). And for embedding we are dealing with G channel.

3.1.1 Embedding Algorithm

The secret image embedding algorithm as follows,

Input:

The colors image I and Secret Image S.

Output:

The Stego image I'.

1. As we are dealing with color image and are made up of three channels we need to separate these channels and take G channel.
2. Apply single level decomposition using wavelet transform on G channel and produce sub bands coefficients {LL, LH, HL, HH}.
3. Take secret image which is to be embedding.
4. Now embed the secret image S into the sub band to get stego image.
5. Apply inverse wavelet transform on stego image to get embedded cover image I'

3.2 Extraction Process

The Extraction algorithm is as follows.

Input:

Stego image I' Cover Image I

Output:

Secret image S

1. Take the embedded stego image I' and separate the tree channels Red, Green, and Blue and select G channel for further.
2. Apply the single level decomposition using wavelet transform on G channel to get appropriate sub bands coefficients.
3. Now apply the exact reverse process as we done for embedding.
4. After applying reverse process we get the secret image S.

IV. METHOD-II THREE LEVEL WAVELET DECOMPOSITION

4.1 Embedding Process

In this embedding process we embed the secret image or stego image on to the cover image using three level wavelet transform. The cover image is made up of three channels Red(R), Green (G), Blue (B). And for embedding we are dealing with G channel.

4.1.1 Embedding Algorithm

The secret image embedding algorithm as follows,

Input:

The colors image I and Secret Image S.

Output:

The Stego image I'.

1. From the color image I, separate the R, G, B channel and use G channel.
2. After getting G channel apply three level decomposition using wavelet transform on the G channel of the cover image I.
3. After applying the transform we get sub band coefficients as {LL, LH, HL, HH}.
4. Now take secret image S for embedding onto cover image.
5. Now we have secret image and G plane image sub band now apply embedding process to get stego image I'.
6. Now apply inverse wavelet transform on the stego image I'.

4.2 Extraction Process

In this process we reconstruct the original secret image S.

4.2.1 Extraction Algorithm

The Extraction algorithm is as follows.

Input:

Stego image I' Cover Image I

Output:

Secret image S

1. Take the stego image I' and separate the three R, G, B channels and select G for use.
2. Apply three level decomposition using wavelet transform on the stego image.
3. After applying wavelet transform we get sub band coefficients {LL, LH, HL, HH}.
4. Select the required sub band for extraction.
5. Apply the exact reverse process of embedding for extraction of secret image from stego image I'.
6. After this we get secret image S.

We checked the visual quality of the stego image i.e. the difference between original image and stego image. To calculate this we used two performance measure techniques Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Higher the value of PSNR and lower the value of MSE shows that the visual quality of the stego image is perfect.

MSE:

It is defined as the square of error between cover image & stego image. The distortion in the stego image can be measured using MSE. It is calculated as follows.

$$MSE = \frac{1}{n}\sum_{n=0}^{N}[x(n) - y(n)]^2 \quad \text{..... (1)}$$

Where x (n) represent cover image and y (n) represent stego image.

PSNR:

It is the measure of quality of stego image by comparing cover image with stego image. It is calculated as follows.

$$PSNR = 10\log_{10}\frac{\sum_{n=0}^{N}x(n)^2}{\sum_{n=0}^{N}[x(n) - y(n)]^2} \quad \text{..... (2)}$$

Where x (n) represent cover image and y (n) represent stego image.

V. DISCUSSION AND RESULT

5.1 Proposed Method I (Using Single Level Wavelet Decomposition):

5.1.1 Results using DWT (db1)

Figure 3: single level dwt embedding and extraction

5.1.2 Results using SWT (db1):

Figure 4: single level SWT embedding and extraction

In fig.3 and fig.4 we perform embedding process on the give input image for this first we first separate the G plane from color image. After this we transform G planec by three level decomposition using DWT/SWT for embedding the secret image onto decomposed G plane to obtain embedded G plane after obtaining the embedded G plane we reconstruct the G plane into colored stego image. After this embedding process we get the embedded colored stego image which is exactly same as cover input image. Now to obtain the secret image from stego image we have to use extraction process and after extraction we get the secret image as shown in figure.

5.2 Proposed method 2 (Using Three Level Wavelet Decomposition):

5.2.1 Results using DWT (haar):

Figure 5: three level DWT embedding and extraction

5.2.2 Results using SWT (haar):

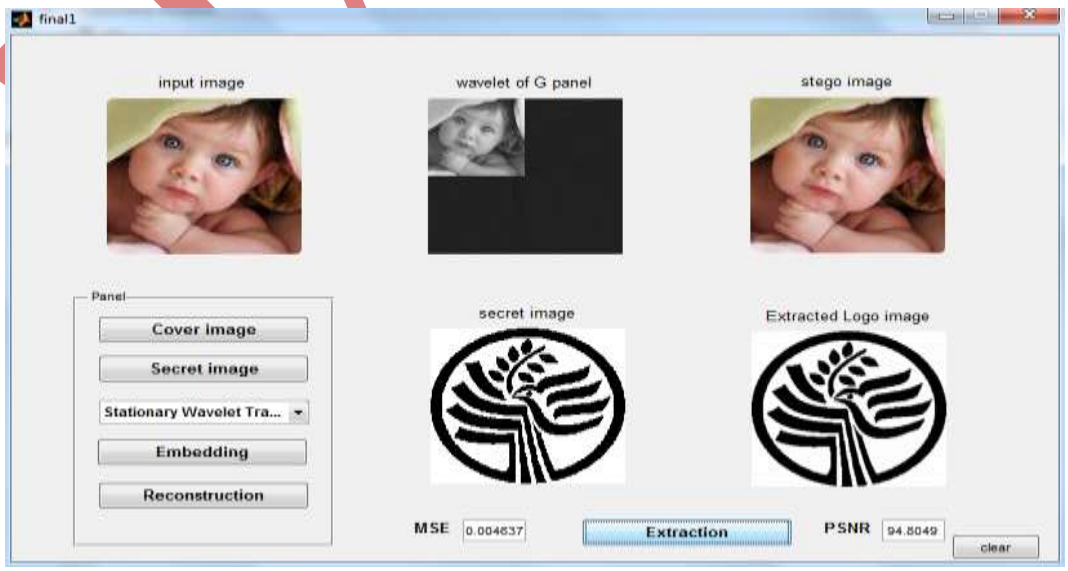

Figure 6: three level SWT embedding and extraction

The above fig.4 and fig.5 shows the result of the embedding and extraction process for single level decomposition using DWT and SWT.

Table1: MSE and PSNR for the different cover and secret images using single level decomposition

Cover image	Secret image	DWT		SWT	
		MSE	PSNR	MSE	PSNR
Baby	Tree	1.31877	46.9299	1.30375	46.9797
Man	IIT	1.21189	47.3397	1.2081	47.3538
Leena	Dots	1.62897	46.0571	1.62584	46.0666
Koala	QR	1.54765	46.2434	1.52999	46.2937
Zebras	ECG	1.02209	48.0665	1.01492	48.0979
Baboon	Ship	1.0819	47.7935	1.07509	47.821

Table2: MSE and PSNR for the different cover and secret images using three level decomposition

Cover image	Secret image	DWT		SWT	
		MSE	PSNR	MSE	PSNR
Baby	Tree	0.0046	94.698	0.0046	94.7982
Man	IIT	0.0061	92.323	0.0061	92.3238
Leena	Dots	0.0060	92.517	0.0060	92.517
Koala	QR	0.0051	93.846	0.0051	93.8465
Zebras	Che	0.0037	96.716	0.0037	96.7167
Baboon	Palm	0.0051	93.963	0.0051	93.9632

VI. CONCLUSION

In this paper, a new image data hiding technique based on stationary Wavelet Transform has been proposed. The stego-image is looking perfectly intact and has high peak signal to noise ratio value and low Mean Square Error value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image. In this paper two different techniques namely,

1. Using single level decomposition of Stationary Wavelet Transform and
2. Using three level decomposition of Stationary Wavelet Transform for hiding images has been proposed and implemented.

The main goal of this research work was embedding of secret image into cover image as a case of steganography. The two primary criteria for successful steganography are that the stego image resulting from embedding is perceptually indistinguishable from the host cover image, and the secret image is recovered correctly at the receiver. We successfully embed the cover image so we can say in some extent the target has been achieved.

REFERENCES

[1] Banoci, V.; Bugar, G.; Levicky, D. A novel method of image steganography in DWT domain", Radioelektronika, 2011-21 st International Conference.

[2] Wang, H, Wang, S, "Cyber warfare: steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[3] L. Tsung-Yuan, T. Wen-Hsiang, "A New Steganography method for data hiding in Microsoft Word documents by a Change Tracking Technique," IEEE transaction on Information forensics and security ,vol. 2, issue 1, pp.24-30, 20072 Wang, H, Wang, S, "Cyber warfare: steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[4] Goel, R., Garuba, M., Liu, C. , Nguyen, T. . The Security Threat Posed by Steganographic Content on the Internet.Information Technology, 2007. ITNG '07. Fourth International Conference on. 794-798 DOl 10.1109/ITNG.2007.192

[5] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.James E. Fowler: The Redundant Discrete Wavelet Transform and Additive Noise.

[6] T. Narasimmalou, Allen Joseph .R "Discrete Wavelet Transform Based Steganography for Transmitting Images" International Conference On Advances In Engineering, Science And Management, 2012.

[7] Kumar, V., Kumar, D, Performance evaluation of DWT based image steganography" , Advance Computing Conference (IACC),

[8] M. Holschneider, R. Kronland-Martinet, J. Morlet and P. Tchamitchian. Real-time algorithms for signal analysis with the help of the wavelet transform. In *Wavelets, Time-Frequency Methods and Phase Space*, pp. 289–297. Springer-Verlag, 1989.

[9] James E. Fowler: The Redundant Discrete Wavelet Transform and Additive Noise.