[1]

Steganography Using Discrete Wavelet Transform

Hala Abualsaud, Mia Gonzalez

I. ABSTRACT

STEGANOGRAPHY is a secure and imperceptible technique used in the Information Security field. It works by hiding various types of information in other platform media where the information existence cannot be detected by normal vision (i.e. the information transmission is concealed). Previous work has accomplished this using the haar wavelet. Our approach includes hiding the messages in the components of various discrete wavelet transforms (Daubechies, Biorthogonal). The first factor to consider when validating each wavelet type is the integrity of the message transmitted. Another factor is to keep the transmission concealed by having a non-distinguishable stego image from the original one.

II. INTRODUCTION

A. Background

Information security is an extremely important challenge for every organization and is used to protect confidentiality. There are various security techniques to protect communications. Conventionally, Cryptography used to be a popular approach to transfer information in a secure way that it would be hard to decipher. Steganography has evolved to replace Cryptography to make communication impossible to be detected by anyone else other than the sender and the receiver as hidden messages will be embedded inside another medium (i.e. the cover object).

Cryptography	Steganography
It works by using Encryption algorithms	It works by hiding stego information in a cover object (embiddes the message in a different medium)
Protects messages contents	Protects messages existence
A secure information security technique. It relies on parameters such as keys	A more secure and imperceptible information security technique. It doesn't rely on any parameter

Table 1: Comparison between cryptography and steganography techniques

[1]December, 14 2019

B. Conventional Approaches

Previously steganography was accomplished using the following methods: Least Significant Bit, Least Significant Bit Watermarking, and Haar Discrete Wavelet Transforms.

The most popular steganography method is the Least Significant Bit (LSB) technique. It works by reading the values of each pixel in an image, converting it to its binary format, and finally replacing the least bits of each byte with the bits of the hidden message. The drawback of this method is that the stego object is easy to corrupt which makes it a relatively insecure method.

Least Significant Bit Watermarking works by applying watermarks after replacing the least significant bits of the cover object with the message bits in order to distort the existence of information. This method is more secure than the LSB technique but the stego object can be seen in the transmission image.

In order to increase the security when transmitting hidden data, discrete wavelet transform method has been evolved to make communication harder to be detected. In this method, wavelet coefficients of the cover object are replaced by the hidden message bits instead of the least significant bits mentioned earlier. Haar wavelet transform has been explored by researchers earlier.

C. Wavelets

Haar wavelet is a simple, fast, memory efficient wavelet. It is symmetric and not continuous; it resembles a step function,. However, Haar window is only two-elements wide which means in Haar transform, big changes from even to odd values won't be reflected in the high frequency coefficients.

Daubechies Wavelets are orthogonal easy implemented easy invertible wavelets. Moreover, the filter length of Daubechies wavelets is more than two which makes them smoother wavelets than Haar. Also they use overlapping windows so high frequency coefficient spectrum reflects all high frequency changes. We will be using Level 2 and Level3 Daubechies in this paper (db2, db3)

Biorthogonal Wavelets are symmetric invertible wavelets. The family of biorthogonal wavelets uses two wavelets, one for decomposition and one for the reconstruction. We will be using biorthogonal 1.3 (bior1.3) and biorthogonal 2.2 (bior2.2) in this paper.

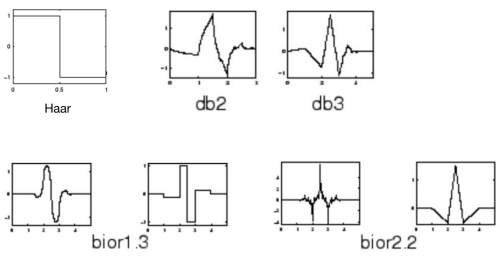

Figure 1: Haar, db2, db3, bior 1.3 wavelets [2]

III. PROPOSED METHOD

The focus of our research was Discrete Wavelet Transforms in Steganography technique. We used images as our cover objects and text as our hidden message and the implementation was done without using a key. Our base comparison is against the 2D Haar Discrete Wavelet Transform. We have explored the Daubechies and biorthogonal wavelets. From there we varied the type of cover image used, image manipulation, and increasing the length of the message. Discrete Wavelet Transform is used to decompose images into Low-Low (LL), Low-High (LH), High_Low (HL), and High-High (HH) sub images that have the same size as the original image.

A. Procedure

In this project, we used images as the cover objects and texts as the hidden object. Image can be in any format such as (.bmp), (.jpg). We used "Hello World" as our hidden text. We used two kinds of images as our cover object: a high detailed image and a simple one. The procedure is as follows:

Encoding: Hiding the signal within an image

1) Take the wavelet transform of the input image (choose from a various group of wavelets: Haar Wavelets 'haar', any of Daubechies wavelets, or any of Biorthogonal wavelets)
2) Find the coefficients below a threshold value
3) Replace these bits with the bits of the message to be hidden
4) Take the inverse transform
5) Store it as a regular image, in any standard format[2]

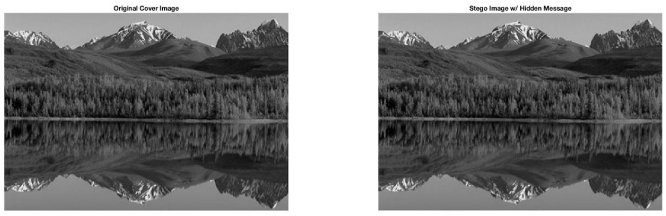

Figure 2: (a) Original Cover Image (b) Stego Image [Result of Encoding Step 5]

Decoding: Extracting the signal from the Stego image

1) Take the wavelet transform of the image
2) Find th[3]e coefficients that are below a threshold value
3) Extract the bits of data from these coefficients
4) Combine the extracted data bits into an actual message
5) Output the message or data

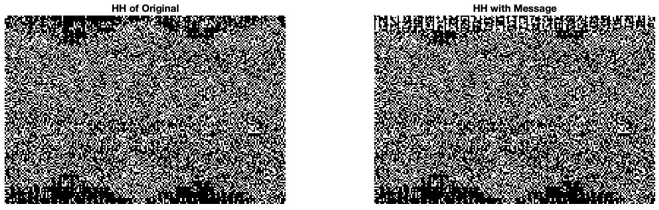

Figure 3: (a) The HH subband diagonal of Cover image
(b) Message in HH subband [Result from Encoding Step 3] [3]

B. Lifting Scheme

Lifting wavelet transform is a discrete wavelet transform that allows integer to integer wavelet transform. We used it in our project to avoid losing precision in coefficients as we write and read across the transforms and inverse transforms. Because our hidden message is written in binary to the image, any kind of perturbation severely affects the ability to recover the message. Preliminary implementations showed that we would not be able to recover the message without lifting at the Encoding and Decoding stages. We employed MATLAB's implementation of a 2-D lifting wavelet transform[7] for each type of wavelet.

C. Performance Measures

We compared the cover image and stego images using the following performance measurement tools:

- Mean Square Error (MSE) for y_i-$\hat{y}_i$ is the point-wise difference in the stego image from the original.

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2$$

- Peak Signal Noise Ratio (PSNR) is normalized to the number of bits used to represent pixel intensities in image

[2] *Introduction to Wavelet Families,* December 10, 2019, https://www.mathworks.com/help/wavelet/gs/introduction-to-the-wavelet-families.html#f3-1009152

[3] Implemented using the zipped code submitted

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\,\text{dB}$$

- Naturalness Image Quality Evaluator (NIQE)[3] is a general quality evaluator, low values indicate high quality, while high indicate low quality.
- Message Error (Msg Error) is the mean square error in the hidden message and the recovered message. It is 0.0 when the message is perfectly recovered, and can grow as large as the magnitude of the original message.

IV. COMPARISONS

The cover image is shown in Fig 1.a. and the hidden message is ‘hello world’. Received messages using Haar, db2, db3, bior1.3, and bior 2.2 wavelets are shown in the tables below (Tables 2,3,4). The results include using two types of images, a detailed one and a simple one. Liftwave Scheme technique was found to dramatically enhance the ability to recover text. Haar wavelet works better when using a high detailed image since Haar wavelet is not continuous such that small variation in the input does not result in a differentiable changes in the output. However, biorthogonal wavelets found to work much better when the cover image is simple (i.e. lacks details).

A. *Steganography with Natural Image*

Wavelet Type	*Haar*	*db2*	*db3*	*bior1.3*	*bior2.2*
Received Message	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*

Table 2: Comparison between wavelets for detailed image

Wavelet	*Msg Error*	*PSNR*	*MSE*	*NIQE*
Haar	0.0	81.1546	4.9845e-04	4.5888
db2	0.0	69.9812	0.0065	4.5951
db3	0.0	63.3480	0.0301	4.6148
bior1.3	0.0	75.4083	0.0019	4.5949
bior2.2	0.0	78.1443	9.9691e-04	4.6023

Table 3: Performance metrics for detailed image

All of the wavelets were able to recover the hidden message. The Haar had the best error (high PSNR and low MSE) for its stego image, compared to the original. This translates to imperceptibility (Table 3), which is important in steganography. The NIQE which provides overall quality, is negligibly the same for all the wavelets. The biorthogonal wavelets performed better than the daubechies (2,3). The reason behind this is because it has a component that is the Haar wavelet.

B. *Steganography with Filtered Image*

Next, we evaluated the performance of each wavelet in the case that the stego image was manipulated. Filtering the stego image, with a gaussian filter, σ=0.4, we were able to partially and perfectly recover the hidden message. The error measures: PSNR, MSE, NIQE are mainly an effect of the smoothing.

Wavelet Type	*Haar - smooth*	*db2 - smooth*	*db3 - smooth*	*bior1.3 - smooth*	*bior2.2 - smooth*
Received Message	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'è' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'¨' 'e' 'd' 'l' 'o' ' ' ' ' 'o' 'r' 'l' 'd'*	*'h' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*	*'è' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'*

Table 4: Comparison between wavelets for detailed image (with Gaussian smoothing)

Wavelet	*Msg Error*	*PSNR*	*MSE*	*NIQE*
Haar	0.0	44.4331	2.3430	4.3122
db2	1.4895e+03	44.4246	2.3476	4.3180
db3	1.7586e+03	44.3918	2.3654	4.3346
bior1.3	0.0	44.4305	2.3444	4.3282
bior2.2	1.4895e+03	44.4322	2.3435	4.3269

Table 5: Performance metrics for detailed image (with Gaussian smoothing)

C. *Steganography with Simple Image*

In our exploration, we examined how different images could serve as the cover object for our steganography. Natural images typically provide a lot of texture, and are unassuming - optimal for the purposes of steganography. To see how the various wavelets performed, we used Fig 3 as the cover object. This simple image has few components and fairly constant regions. The message ends up being a high frequency change when added to the transform. The db3 wavelet was significantly better than the others at recovering the message.

While the haar wavelet result had no semblance of the original message.

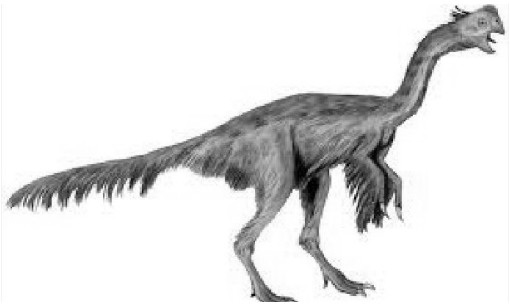

Figure 4: Simple Image as Cover Object

Wavelet Type	*Haar*	*db2*	*db3*	*bior1.3*	*bior2.2*
Received Message	' '	'è' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'	'¬' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'	'è' 'e' 'l' 'l' 'o' ' ' 'w' 'o' 'r' 'l' 'd'	'à' '¬' 'l' 'l' 'o' ' ' 'w' 'o' 'p' 'l' '¬'

Table 6: Comparison between wavelets for a simple image

Wavelet	*Msg Error*	*PSNR*	*MSE*	*NIQE*
Haar	1.0803e+04	99	0.0	27.6890
db2	1.4895e+03	65.8708	0.0168	26.6722
db3	372.3636	58.2220	0.0979	26.5739
bior1.3	1.4895e+03	74.8154	0.0021	26.6217
bior2.2	1.4063e+03	78.8149	8.5426e-04	26.9364

Table 7: Performance Metrics for Simple Image

D. Longer Message

In order the understand the performance with a longer message, the following hidden message was sent with each of the wavelets:

"Nothing Gold Can Stay Robert Frost Nature's first green is gold, Her hardest hue to hold. Her early leaf's a flower; But only so an hour. Then leaf subsides to leaf. So Eden sank to grief, So dawn goes down to day. Nothing gold can stay."

The length of this message is 235 characters. Each character is converted to 8-bit binary representation, then stored in the diagonal subband of the cover image. For context, the message is 8% of the diagonal portion. The message is recovered with haar, db3 and bior2.2, so Message Error is zero. Db 2 and bior1.3 had a Message Error around $6x10^{1}$, which is relatively small.

V. CONCLUSION

Steganography can be accomplished with discrete wavelet transform techniques to conceal data transmission in order to enhance the security of communications. In this paper we addressed the technique of embedding a text message inside a cover image using wavelets coefficients to hide the data in. Different wavelets were tested with and without smoothing and with different cover images. Comparisons are made on the basis of different performance metrics to validate the results. Each wavelet has its own advantages and disadvantages based on the cover image used and the smooth added. The stego images generated with the biorthogonal wavelets had PSNR's close to that of haar, while perfectly recovering the message like haar. And considering a longer message bior2.2 performed better than bior1.3. The bior1.3 wavelet recovered the message from a smoothed stego image than bior2.2. The db3 wavelet was best at recovering the message from a simple image.

Future Modification: Future study could explore the best wavelet for a noisy channel simulated with Gaussian noise. The use of other types of hidden and stego objects could be investigated since the hidden information can vary based on the need or interests. One more possible modification to the work proposed in this paper is to allow users dynamically choose the bits for hiding data, and provide an encrypted file of those ones.

REFERENCES

[1] Hemalatha, S., et al. "Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image." Procedia Computer Science, Elsevier, 17 May 2015, www.sciencedirect.com/science/article/pii/S1877050915004755

[2] Shet K.S., Nagaveni, Aswath A.R. (2015) Image Steganography Using Integer Wavelet Transform Based on Color Space Approach. In: Satapathy S., Biswal B., Udgata S. Mandal J. (eds) Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Advances in Intelligent Systems and Computing, vol 327. Springer, Cham

[3] A. Mittal, A. K. Moorthy and A. C. Bovik, "No-Reference Image Quality Assessment in the Spatial Domain," IEEE Transactions on Image Processing , 2012.

[4] A. Mittal, A. K. Moorthy and A. C. Bovik, "Referenceless Image Spatial Quality Evaluation Engine," 45th Asilomar Conference on Signals, Systems and Computers , November 2011.

[5] A. Mittal, R. Soundararajan and A. C. Bovik, "Making a Completely Blind Image Quality Analyzer, " IEEE Signal Processing Letters , pp. 209-212, vol. 22, no. 3, March 2013.

[6] Strang, G.; T. Nguyen (1996), Wavelets and filter banks, Wellesley-Cambridge Press.

[7] Sweldens, W. (1998), “The Lifting Scheme: a Construction of Second Generation of Wavelets,” SIAM J. Math. Anal., 29 (2), pp. 511–546.
https://www.mathworks.com/help/wavelet/ref/lwt2.html