Lab Project Report on:

Hiding a Message in an Image using Steganographic Techniques

Report Submitted by:

Sitara Kumbale (16EE248)
Adarsh Malapaka (16EE129)

Under the guidance of
Dr. Krishnan CMC

Department of Electrical and Electronics Engineering
National Institute of Technology, Karnataka
17th March 2019

ACKNOWLEDGEMENT

The final outcome of this project required a lot of assistance from many people and we are privileged to have gotten this all along the completion of our project. We are profoundly grateful to Dr. Krishnan C.M.C, Dept. of Electrical & Electronics Engineering, for his expert guidance and continuous encouragement from the commencement to the completion of the project and the lab sessions to ensure that we gain immense knowledge from them.

Finally, we would like to take this opportunity to thank our families for their constant support throughout the work. We sincerely acknowledge and thank the Teaching Assistants who have assisted us during the conduction of our regular lab experiments.

ABSTRACT

In this report, various steganographic algorithms for hiding a given message in an image have been analysed and surveyed out of which two such algorithms, the Least Significant Bit (LSB) Manipulation technique and the Discrete Wavelet Transform (DWT) technique have been implemented on MATLAB. The report first introduces the reader to the concept of steganography and its applications after which a literature survey of various algorithms is presented. Finally, the techniques are implemented and the results are compared for different image sizes and the image compression qualities.

In the LSB approach, the message is broken into individual components which are converted into 8-bit binary values, encrypted using an XOR encryption key and then encoded into the image by changing the least significant bit of the pixels sequentially. In the DWT approach, the message to be hidden is embedded in high frequency coefficients resulting from the Discrete Wavelet Transform and the low frequency coefficients are unaltered for better quality. The corresponding size of the output altered image (in Kb), execution times for both encoding and decoding processes and the Peak Signal-Noise Ratio (in dB) are tabulated and compared for both LSB and DWT approaches.

Keywords - *Steganography, Cryptography, LSB technique, Discrete Wavelet transform*

TABLE OF CONTENTS

1. Introduction

With the rapid advancement of the Internet, information processing technologies and the development of communication, it has become necessary to share information safely and reliably. Security of information is one of the most important factors of information technology and communication because of the huge rise of the World Wide Web and the copyrights laws. Cryptography was originated as a technique for securing the confidentiality of information. It is concerned with concealing the content of the message, so it becomes difficult to comprehend. Unfortunately, it is usually not enough to keep the contents of a message secret. Here is where keeping the existence of the message a secret is of paramount importance!

Steganography is derived from the Greek words *Steganous* meaning 'covered' and *graphy* meaning 'writing'. Steganography is a technique which is used to hide a message so as to prevent the detection of the hidden message. Image Steganography (hiding text in an image/ hiding images in an image) is the most popular method.

The history of steganography dates back to 440 B.C. in Ancient Greece. The Greek used to shave slaves' head, write a secret message and send them to their allies after their hair had grown back. Steganography was also used by the Germans during the World War I and II. During the American Revolution, invisible ink was used by the revolutionaries for communication purposes. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information.

The basic terminologies used in the steganography systems are: cover message, secret message, secret key and embedding algorithm.

- ➔ The **cover message** is the carrier of the message. It may be an image, video, audio, text or some other digital media.
- ➔ The **secret message** is the information which has to be hidden in the suitable digital media.
- ➔ The **secret key** is usually used to embed the message depending on the hiding algorithms.
- ➔ The **embedding algorithm** is the technique that is used to embed the secret information in the cover message.

Applications of Steganography:

- ➔ Confidential Communication and Secret Data Storing
- ➔ Protection of Data Alteration
- ➔ Access Control System for Digital Content Distribution
- ➔ E-Commerce
- ➔ Feature Tagging Elements
- ➔ Digital Watermarking
- ➔ Database Systems
- ➔ Copyright Protection Mechanisms

Steganographic Algorithms:

- ➔ Steganography using Least Significant Bit (LSB)
- ➔ Edge Adaptive Steganography
- ➔ Fractal Based Image Steganography
- ➔ Steganography using DCT (Discrete Cosine transform)
- ➔ Steganography using DWT (Discrete Wavelet Transform)

In this project, we have explored two techniques - Steganography using Least Significant Bit (LSB) and Steganography using Discrete Wavelet Transform (DWT).

2. Literature Review

In the year 2012, Das, R. and Tuithung, T. [1] proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel intensities of cover image. Peak Signal to Noise Ratio (PSNR) of steganographic image with cover image shows better result in comparison with other existing steganography approaches.

In the year 2013, Akhtar, N.; Johri, P.; Khan, S., [2] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. The inversion bit pattern is stored and this is used to obtain the original message. RC4 algorithm has been implemented to improve robustness. This method randomly disperses the bits of the message in the cover image and thus makes it harder for unauthorized people to extract the original message. The presented method is an enhancement to Least Significant Bit technique as it improves security and image quality.

In the year 2013, Prema, G.; Natarajan, S.,[3] Investigated on Image steganography for secure data hiding and transmission over networks. The proposed system provides the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. Genetic Algorithm is used to modify the pixel location of stego image. Visual Cryptography is used to break the image into two shares based on a threshold. The performance of the proposed system is evaluated by calculated the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

Khosravi, M.; Soleymanpour-Moghaddam, S.; Mahyabadi, M.,[4] investigated a novel steganographic method is proposed which is based on the spatial domain: Least Significant Bit (LSB). The LSB matching method proposed by Mielikainen utilizes a binary function to reduce the number of changed pixel values. While in this paper a bipolar evaluating system is proposed to assess the performance of different orders for LSB matching. Afterward a genetic algorithm strategy is employed to search for an optimal solution among all the permutation orders. The experimental outcomes show that by employing the proposed bipolar evaluating system, the distortion of the stego-image is reduced while the probability of detection is decreased.

In the year 2012, Thenmozhi, S. and Chandrasekaran, M., [5] presented a novel scheme that embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. An optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms other steganography techniques based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

In the year 2012, Hemalatha, S, Acharya, U.D. and Renuka[6] used integer Wavelet Transform (IWT) to hide the key. In this method the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands. This Technique is very secure and robust because the hidden data cannot be lost due to noise or any signal processing operations. Results shows very good Peak Signal to Noise Ratio.

In the year 2011, Mandal, J.K.; Khamrui, A.,[7] proposed a study of Image steganography that. In this paper a Genetic Algorithm based color image authentication/data hiding technique through steganographic approach, in frequency domain using Discrete Fourier Transform (DFT) termed as GASFD, has been proposed. 2×2 masks are taken from the source image in row major order where DFT is used to transform original image (cover image) block from spatial domain to frequency domain. Three bits of the hidden image are embedded per byte of the source image onto the rightmost 3 bits of each pixel excluding the first byte of each mask, as a effect large volume of message/ image is embedded in frequency domain. 2×2 embedded image mask is transformed from frequency domain to spatial domain using inverse DFT. Resulting image mask of size 32 bits are taken as initial population. New Generation and Crossover are applied on the initial population to obtain stego image.

In the year 2013, Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), [8] Investigated on a generalization of the classical Fourier transform. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key.

3. Theory

Least Significant Bit Technique (LSB)

The least significant bit is the bit which is farthest to the right in a binary representation and holds the least value. It is usually employed in hash functions, checksums and pseudorandom number generators. The Least Significant Bit (LSB) Manipulation technique makes use of this lower significance of the bit within each pixel of an image. An image is a collection of pixels with each pixel storing three eight bit integers corresponding to the red, blue and green components respectively. The human eye often cannot identify the subtle differences between colours (refer to Fig 3.1.1) and so by replacing the LSB in each of these colours, hiding of a message is possible.

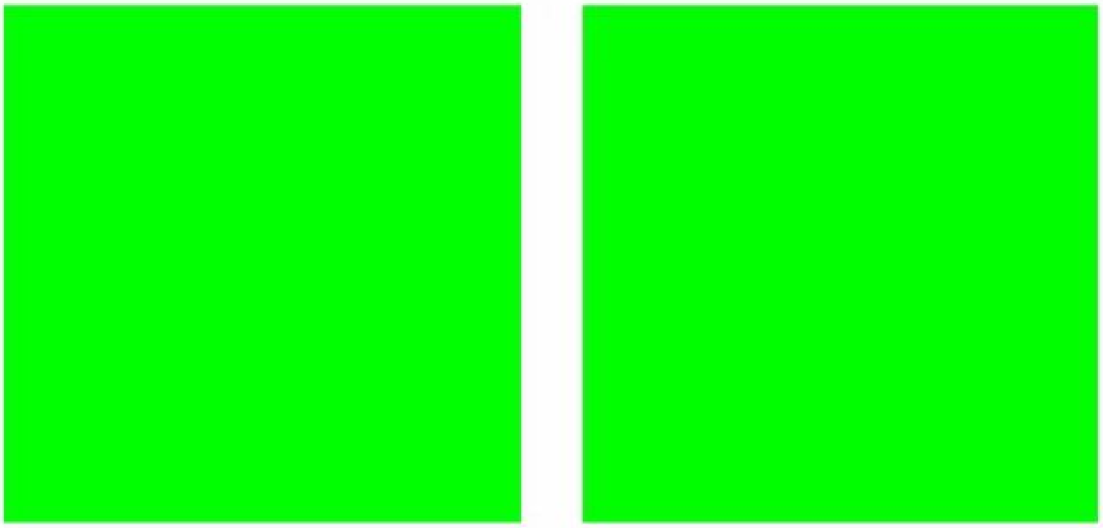


Figure 3.1 Unidentifiable subtle difference between colours

In Fig 3.1, the green square on the left has RGB components of (0,255,0) whereas the square on the left has RGB components of (0,254,0). Despite the difference of 1, there is no observed visible difference between the two.

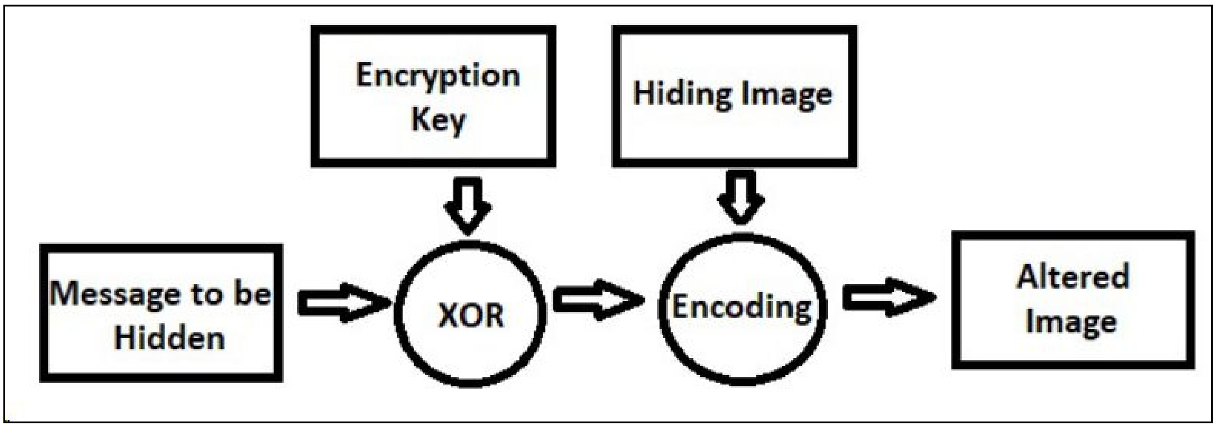


Figure 3.2 Flowchart of the LSB encoding process

In this method, the length of the message is attached to the beginning of the message to be able to reconstruct the message during decoding. A common encryption key for the encoding and decoding processes is used to encrypt the effective message using XOR operation. This encrypted text is encoded onto the 'hiding image' by replacing the LSBs in a sequential manner down along its column. Similar to the transposition of overhead electric cables to attain symmetry, each bit of the message is stored in a RGBBGRRG fashion. The decoding process is the exact opposite of the encoding process and the corresponding message is obtained. The Mean Squared Error is obtained by summing the absolute square of the difference of the Altered and Hiding images whole divided by the product of the number of rows and columns of the image. With this, the Peak Signal-Noise Ratio is found from the following equation where MAX is equal to 255 corresponding to 8-bit value.

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

Discrete Wavelet Transform Technique (DWT)

Discrete Wavelet Transform (DWT) is a Transform Domain Steganographic Technique. In this method, images are first transformed and then the message is embedded in the image. Steganography in the transform domain involves the manipulation of algorithms and image transforms, in this case, the DWT. These methods hide secret image in more significant areas of the cover image, making it more robust. For our project, we have implemented DWT Image Steganography in MATLAB. The diagram below shows the encoding process used to conceal text in an image using DWT technique.

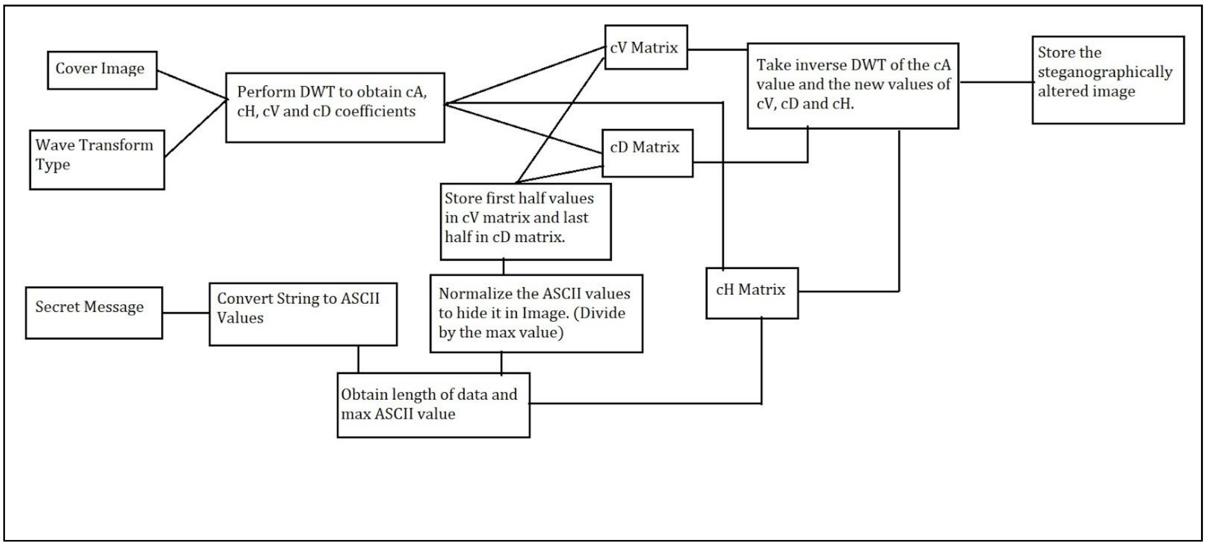

Cover Image
Wave Transform Type
Perform DWT to obtain cA, cH, cV and cD coefficients
cV Matrix
cD Matrix
Take inverse DWT of the cA value and the new values of cV, cD and cH.
Store the steganographically altered image
Store first half values in cV matrix and last half in cD matrix.
Secret Message
Convert String to ASCII Values
Normalize the ASCII values to hide it in Image. (Divide by the max value)
cH Matrix
Obtain length of data and max ASCII value

Figure 3.2 Comparison for a small size image using LSB

Encoding Process:

To implement the DWT algorithm, we first need three specifications or inputs:

- ➔ Cover Image to hide the data in.
- ➔ The Secret Message to hide the data.
- ➔ The Wave Transform type for DWT

The data to be hidden is first converted into its respective ASCII values. The maximum ASCII value is calculated and the data is normalized by dividing each of the values by the maximum ASCII value. The values must be normalized so that the match the image values. The image is then processed by performing Discrete Wavelet Transform on it, using the specified wave transform type.

When DWT is performed on the image, four distinct 'bands' or parts of the image are obtained. The size of data (length of string) and the maximum ASCII value are hidden in the cH matrix. The first half of the normalized string is stored in the cV matrix and the second half is stored in the cD matrix. The values in the cV and cD matrix are changed at certain positions such that the image quality is not affected. Inverse DWT is performed on the new values of cA, cH, cV and cD to obtain a steganographically altered image with the text hidden in the image.

Decoding Process:

The Decoding Process is exactly the opposite of the encoding process. The inputs you obtain in the decoding process are:

- ➔ Steganographically Altered Image
- ➔ Wave Transform Type

DWT is applied on the altered image so as to obtain the four 'bands.' From the cH matrix, the values of maximum ASCII and length of string concealed are obtained. From the cV and cD matrices, the first and second half of the normalized string is obtained. This normalized string is multiplied with the maximum ASCII value to obtain the ASCII values of the string characters. From the ASCII values, the original string that was hidden in the image is recovered.

4. Results

The Images shown below offer a comparison of Image Types when LSB and DWT Steganography Techniques are applied to them.

Small Size Image

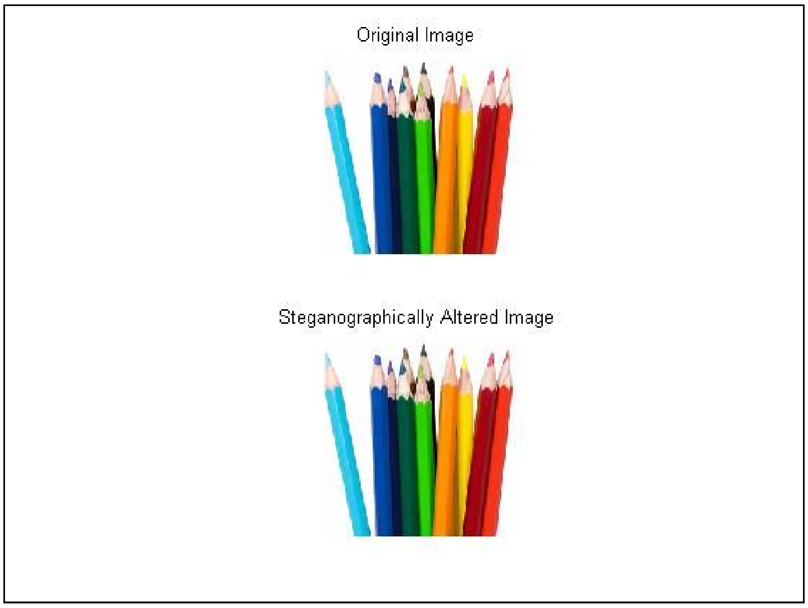


Figure 4.1 Comparison for a small size image using LSB

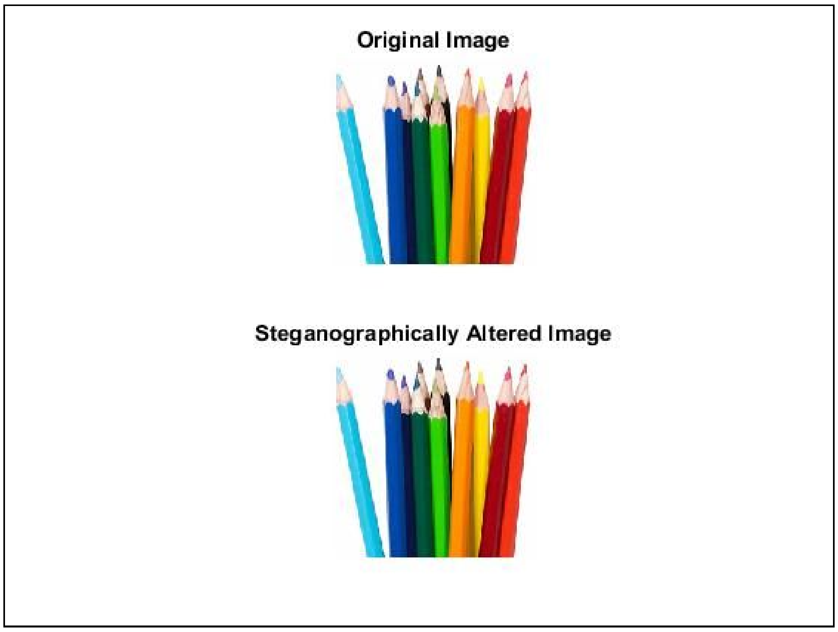


Figure 4.2 Comparison for a small size image using DWT

Medium Size Image

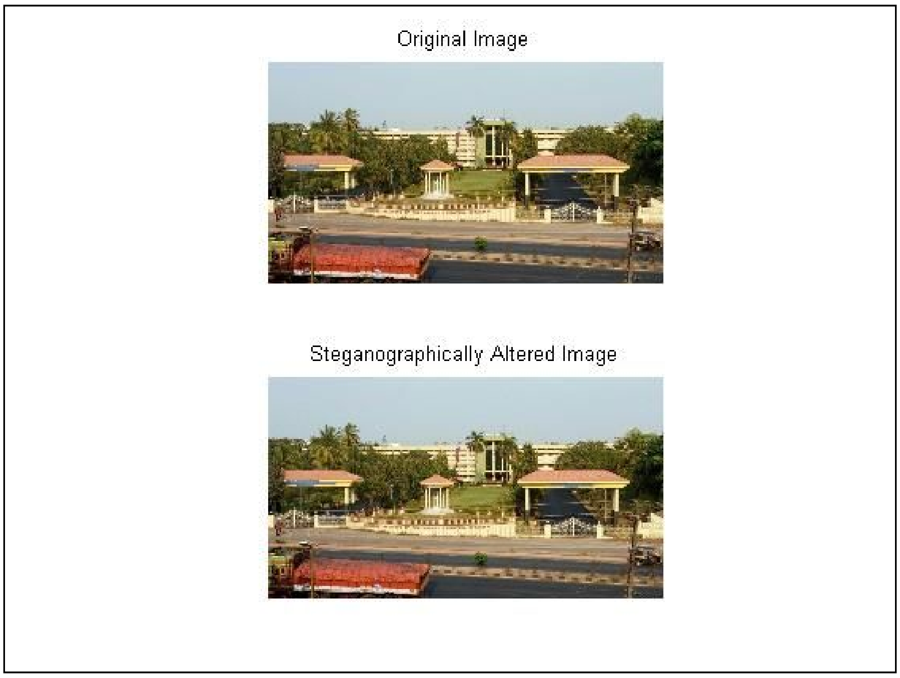


Figure 4.3 Comparison for a medium size image using LSB

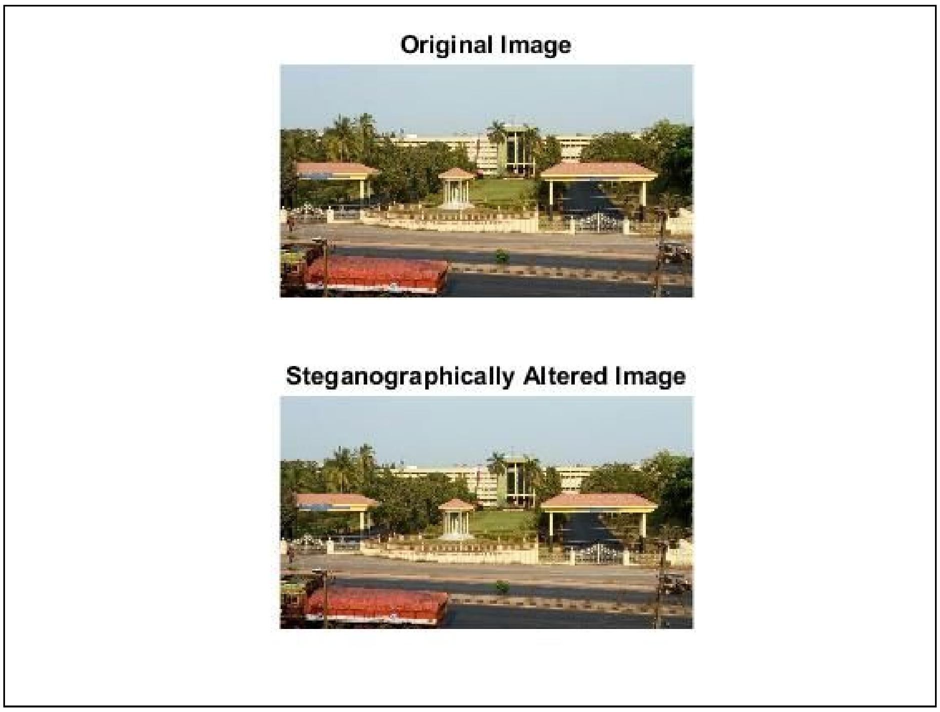


Figure 4.4 Comparison for a medium size image using DWT

Large Size Image

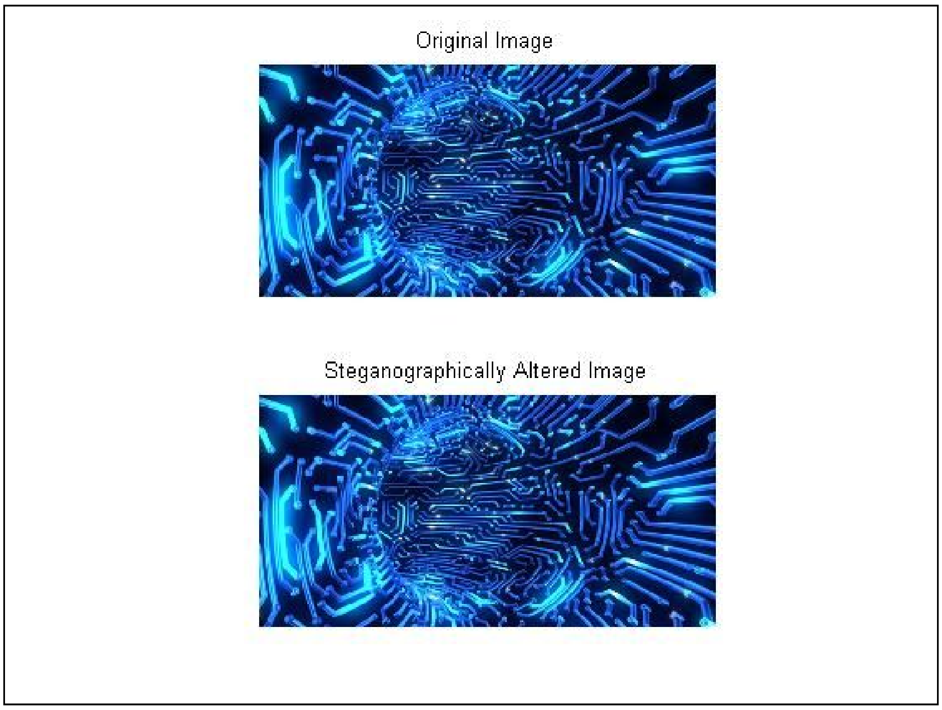


Figure 4.5 Comparison for a large size image using LSB

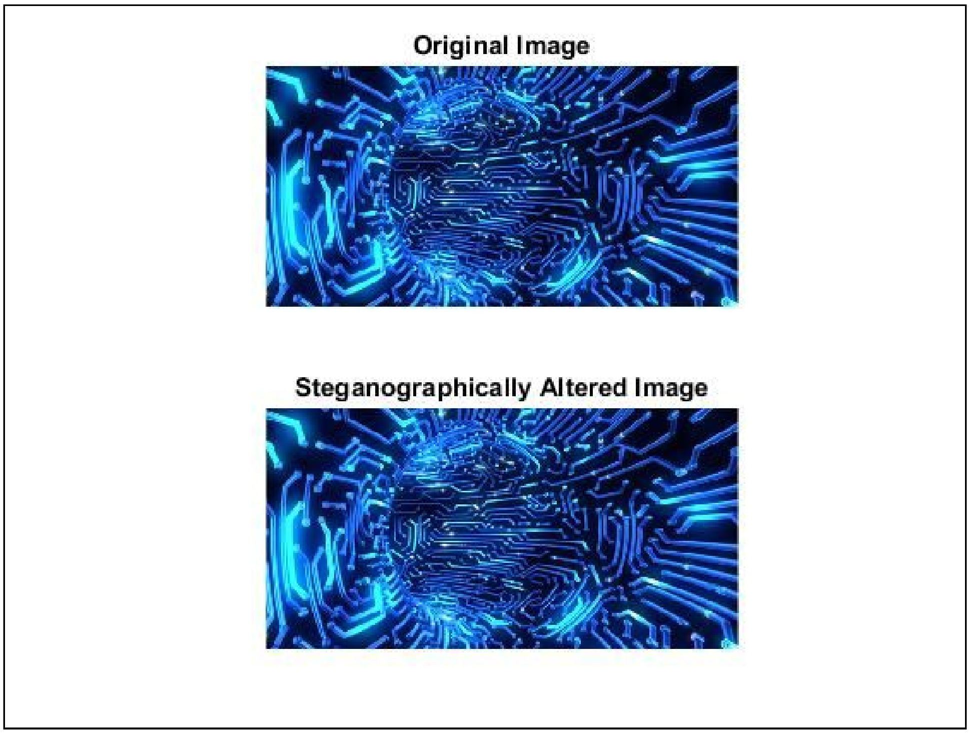


Figure 4.6 Comparison for a large size image using DWT

Size Comparison:

The table below shows the Sizes (Space Occupied) by the Steganographically Altered Images of different sizes when both the LSB and DWT Algorithm are applied.

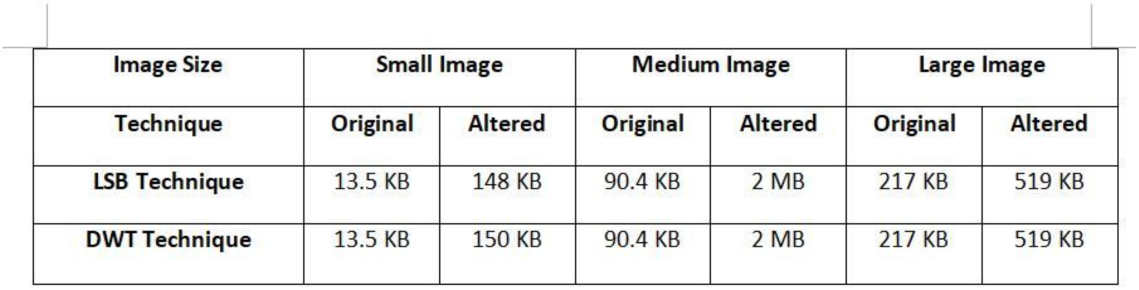


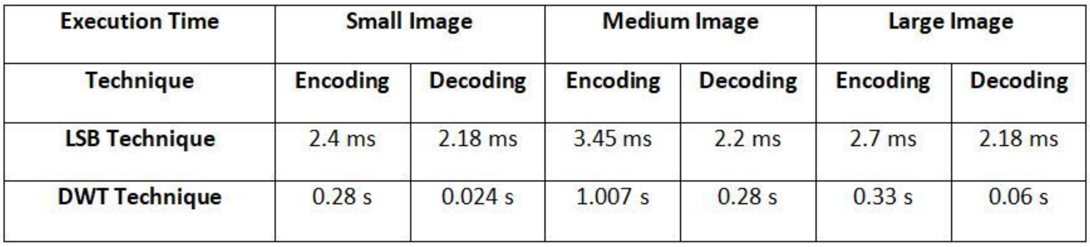
Image Size	Small Image		Medium Image		Large Image	
Technique	**Original**	**Altered**	**Original**	**Altered**	**Original**	**Altered**
LSB Technique	13.5 KB	148 KB	90.4 KB	2 MB	217 KB	519 KB
DWT Technique	13.5 KB	150 KB	90.4 KB	2 MB	217 KB	519 KB

Table 4.1 Comparison of Image Sizes for LSB and DWT Algorithms

From the table, it can be observed that the images that are steganographically altered by LSB Technique and the images that are steganographically altered by DWT Technique occupy nearly the same amount of space/ memory, that is, they are nearly of the same size. Hence, one algorithm is not better than the other with respect to the size of image (space occupied).

Encoding and Decoding Time Comparison:

The table below shows the Time taken to encode and decode the images when both the LSB and DWT Algorithm are applied.



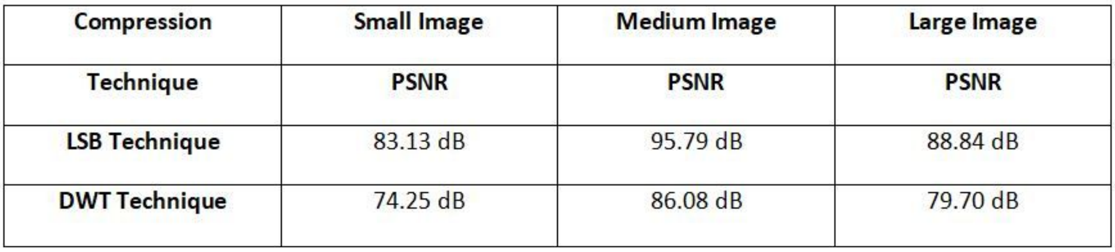
Execution Time	Small Image		Medium Image		Large Image	
Technique	**Encoding**	**Decoding**	**Encoding**	**Decoding**	**Encoding**	**Decoding**
LSB Technique	2.4 ms	2.18 ms	3.45 ms	2.2 ms	2.7 ms	2.18 ms
DWT Technique	0.28 s	0.024 s	1.007 s	0.28 s	0.33 s	0.06 s

Table 4.2 Comparison of Encoding and Decoding Time for LSB and DWT Algorithms

From the table, it can be observed that the images that the LSB Technique takes significantly lesser time to encode and decode images as compared to the DWT technique. Hence, the LSB technique performs better with respect to time efficiency as compared to the DWT technique. Hence, the LSB Algorithm is better than the DWT algorithm with respect to the encoding and decoding time.

Image Compression Quality Comparison:

The table below shows the PSNR (Peak Signal to Noise Ratio) obtained when both the LSB and DWT Algorithm are applied.



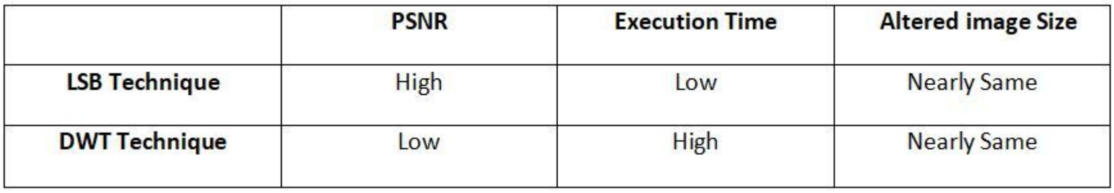
Compression	Small Image	Medium Image	Large Image
Technique	PSNR	PSNR	PSNR
LSB Technique	83.13 dB	95.79 dB	88.84 dB
DWT Technique	74.25 dB	86.08 dB	79.70 dB

Table 4.3 Comparison of PSNR for LSB and DWT Algorithms

From the table, it can be observed that the images that the LSB Technique produces images with slightly higher PSNR values as compared to the DWT Technique. Higher PSNR values are indicative of better quality images. Hence, the LSB algorithm is better than the DWT algorithm when the image quality is considered.

Comparison of LSB and DWT Algorithms:

The table below summarizes the observations and results obtained above and offers an overall comparison between the LSB and DWT Algorithms.



	PSNR	Execution Time	Altered image Size
LSB Technique	High	Low	Nearly Same
DWT Technique	Low	High	Nearly Same

Table 4.4 Comparison of Encoding and Decoding for LSB and DWT Algorithms

Conclusions

In this project, various steganography techniques to hide a text message in an image were studied and two of these techniques were implemented in MATLAB. The techniques implemented were the Least Significant Bit (LSB) Algorithm and the Discrete Wavelet Transform (DWT) Algorithm. The techniques implemented were extensively compared on images of various sizes, on parameters such as Space occupied by the steganographically altered image, encoding and decoding time and image compression quality (PSNR value).

From the results obtained, it was observed that the space occupied by the altered images were nearly the same in both the algorithms. The time taken for encoding and decoding the messages was found to be significantly lesser in LSB as compared to DWT. The PSNR values were found to be slightly higher in the case of LSB as compared to DWT. Overall, it was found that LSB performs better as compared to DWT with respect to the parameters that were considered for evaluation. However, references state that messages encrypted using DWT are often more difficult to detect as compared to those encrypted by LSB. DWT provides more 'invisibility' as compared to LSB.

In the future, the invisibility (the ability to hide messages better) of the two algorithms can be compared and more parameters can be used to compare the two algorithms.

References

1. Das, R.; Tuithung, T., "*A novel steganography method for image based on Huffman Encoding*," Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on , vol., no., pp.14,18, 30-31 March 2012.
2. Akhtar, N.; Johri, P.; Khan, S., "*Enhancing the Security and Quality of LSB Based Image Steganography,*" Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.
3. Prema, G.; Natarajan, S., "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application," Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.727,730, 21-22 Feb. 2013.
4. Khosravi, M.; Soleymanpour-Moghaddam, S.; Mahyabadi, M., "*Improved pair-wise LSB matching steganography with a new evaluating system*," Telecommunications (IST), 2012 Sixth International Symposium on , vol., no., pp.982,986, 6-8 Nov. 2012.
5. Thenmozhi, S.; Chandrasekaran, M., "*Novel approach for image stenography based on integer wavelet transform*," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on , vol., no., pp.1,5, 18-20 Dec. 2012.
6. Hemalatha, S.; Acharya, U.D.; Renuka, A.; Kamath, P.R., "*A secure image steganography technique using Integer Wavelet Transform*," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.755,758, Oct. 30 2012-Nov. 2 2012.
7. Mandal, J.K.; Khamrui, A., "*A Genetic Algorithm based steganography in frequency domain (GASFD)*," Communication and Industrial Application (ICCIA), 2011 International Conference on , vol., no., pp.1,4, 26-28 Dec. 2011.
8. Soni, A.; Jain, J.; Roshan, R., "*Image steganography using discrete fractional Fourier transform*," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 1-2 March 2013.
9. https://stanford.edu/class/ee103/lectures/steganography_slides.pdf
10. Stuti Goel, Arun Rana, Manpreet Kaur, "*Comparison of Image Steganography Techniques.*"
11. Po Yueh Chen and Hung Ju Lin, "*A DWT Based Approach for Image Steganography*," International Journal of Applied Sciences and Engineering, 2006