International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 9, No 2, 2021, pp 1-6
https://doi.org/10.18510/ijsrtm.2021.921

AN ENHANCED IMAGE STEGANOGRAPHY TECHNIQUE FOR HIGH-SECURITY COMMUNICATION

Apoorv Mahajan[1*], **Arpan Singh Rajput**[2]
[1*,2]Computer Science and Engineering Department, Electronics Engineering department, Jabalpur Engineering College, Jabalpur, M.P, India.
Email: [1*]apoorvmahajan3@gmail.com, [2]arpansinghrajput@gmail.com

Article History: Received on 26th February 2021, Revised on 5th April 2021, Published on 12th April 2021

Abstract

Purpose of the study: We propose an approach to hide data in an image with minimum Mean Squared Error (MSE) and maximum Signal-to-Noise ratio (SNR) using Discrete Wavelet Transform (DWT).

Methodology: The methodology used by us considers the application of Discrete Wavelet transform to transform the values of the image into a different domain for embedding the information to be hidden in the image and then using Singular Value decomposition we decomposed the matrix values of the image for better data hiding.

Main Findings: The application of the SVD function gave the model a better performance and also RED pixel values with the High-High frequency domain are a better cover for hiding data.

Applications of this study: This article can be used for further research on applications of mathematical and frequency transformation functions on data hiding. It can also be used to implement a highly secure image steganography model.

Novelty/Originality of this study: The application of Discrete Wavelet Transform has been used before but the application of SVD and hiding data in the H-H domain to obtain better results is original.

Keywords: *Discrete Wavelet Transform (DWT), Signal To noise ratio (SNR), Mean Square Error, Least Significant Bit, Steganography.*

INTRODUCTION

Steganography is a data hiding (Maiti C., Baksi D., Zamider I., Gorai P., Kisku D.R. (2011)) technique that conceals data in an image, video, and audio. This technique provides data confidentiality from malicious users. Steganography can be considered as a technique that provides a stealthy camouflage to hide the data in an image. Steganography is hiding the existence of data whereas cryptography is encrypting the data. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender (Qadir, A. M., and Varol, N. (2019)), whereas Steganography relies on the ability of the image to conceal a particular data within it, the attributes of the image that might affect the ability of an image to hide the data are frequency, intensity and colour combinations. This paper provides an image steganography technique that conceals the data in a covering of an image without disturbing its attributes.

There are two types of domains in steganography that consist of the implemented cover image i.e. spatial domain & frequency domain (Daneshkhah, A., Aghaeinia, H. and Seyedi, S. H. (2011)). In the spatial domain, pixel values of the image are directly processed whereas in the frequency domain, pixel values are transformed and then the transformed coefficients are processed. Currently, there are a plethora of methods to achieve image steganography, one of the most common ones is Least Significant Bit (LSB). Least Significant Bit technique provides an easy way to hide data in a cover image, the cover image is known as the image that is used to hide the data within it, but that leads to the identification of data in the image through the identification of Least Significant Bit as the person intending to know the hidden values can easily identify the data by identifying the values in the Least Significant Bit and combining them to form meaningful data, therefore it is not an ideal method to use as data can be identified by knowing the Least Significant Bit of the data. Mathkour, et. al. describes the recent techniques and also propose a method of hiding data with many advantages and fewer limitations (Mehboob, B. and Faruqui, R. A. (2008)). Rao Thota, et. al., 2008 explained and implemented the basic JPEG compression using only basic MATLAB functions in steganography (Mathkour, H., Al-Sadoon, B. and Touir, A.(2008)). Aneesh Jain, et. al. has described a method that hides given text information in a bitmap image, and in this scheme, there is no perceptible difference between the original image and the stegano image and it is also free from JPEG compression techniques (Jain, A and Gupta, I. S. (2007)). Dr. Walia, et. al in their paper explained the analysis of Least Significant Bit (LSB) based Steganography with Discrete Cosine Transform (DCT) based Steganography techniques (Walia, E., Jain, P., Navdeep (2010)). A highly secure encryption mechanism is required to hide data using steganography. A highly secure encryption mechanism may depend on various attributes of the cover image which can also be used in coordination with the alternative domain features to form a highly secure steganography mechanism. The DWT approaches exist but to enhance the hiding capacity of the image we have also used the H-H frequency domain with red colour pixel values to hide the data as it has proved to be more efficient than the pre-existing approaches of steganography.

PARAMETERS

The embedding of huge data in a cover image makes some alterations in the image, these alterations lead to a distorted image and therefore certain parameters should be considered during the process.

These parameters are:

A. Mean Square Error

The mean squared error denotes the difference between the input data (cover image) and the received image data. (Neeta, D., Snehal, K. and Jacobs, D. (2007))

It can be represented as:

$$MSE = \sum_{i=1,j=1}^{M,N} [IM(xi,yj) - IM2(xi,yj)] ** 2$$

M*N

Where IM is the first image and IM2 second image, M = number of rows and N = number of columns.

B. Peak Signal-to-Noise Ratio

PSNR (Peak Signal-to-Noise ratio) is the ratio of the maximum possible power of an image to the power of the corrupting noise that distorts the quality of the image. In order to estimate the PSNR (Chen, P, and Lin, H (2006)) of an image we need to compare the image to an ideal clean image that has the maximum power.

PSNR is represented as:

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

Capacity

It is the number of bits that can be embedded within the cover image without changing image quality or altering its features. (Chan, K, and Cheng, L. M. (2004))

CONVENTIONAL LSB BASED METHOD OF STEGANOGRAPHY

The LSB method (Chan, K, and Cheng, L. M. (2004), Dey, S., Abraham, A. and Sanyal, S. (2007) consecutively replace the bits of cover image with information bits to conceal data in the image. It may change some of the bits or may alter all the eight bits of the image, to conceal the information in the image so that the information is not visible to human perception. It is the most common spatial domain technique (Daneshkhah, A., Aghaeinia, H. and Seyedi, S. H. (2011)). The capacity for embedding the information in a colored image is thrice of that of a grayscale image because when using a colored image, the LSB of each of Blue, Red, and Green can be used to encrypt the data. When all the bits of information file are embedded in all the bytes of the cover image then it becomes non arguably easy to detect information and extract the message from the received image. A somewhat secure method includes random orientation of data bits in the cover image with the secret key (Anand, J. V., and Dharaneetharan, G. D. (2011)) between the transmitter and the receiver to indicate the locations of the hidden data in the image.LSB is extremely vulnerable to attacks during transmission. LSB techniques implemented in 24-bit formats are difficult to identify contrary to 8-bit formats (Thota, N. R., Devireddy, S. R. (2008)).

DISCRETE WAVELET TRANSFORM

A discrete wavelet transform (DWT) is a transform that decomposes a given signal into a number of sets, where each set is a time series of coefficients describing the time evolution of the signal in the corresponding frequency band (Hosseinzadeh, M.(2020)). The discrete-time Fourier transform X(e**ij) of a discrete-time sequence X[n] is a representation of the sequence in terms of the complex exponential sequence e(jwn), where ω is the real frequency variable, and is defined as (Skodras, A. N. (2015)):

$$\boxed{X(e^{j\omega}) = \sum_{n=-\infty}^{\infty} x[n]e^{-j\omega n}}$$

As in the case of Fourier Transform, the Wavelet Transform has been discretized and is known as a discrete wavelet transform (DWT) and is advantageous over traditional Fourier transform. The WT decomposes a signal into several scales of different frequency bands, and, at each scale (Ramos, R, Valdez-Salas, B., Zlatev, R., Wiener, M. S., Rull, J. M. B. (2017)).

PROPOSED TECHNIQUE

In recent times, many methods are used to encrypt data in an image, some of those methods use a mixture of LSB with different transform functions such as discrete cosine transform (DCT), discrete wavelet transform (DWT) (Zhang D. (2019)). In this method, we have used an advanced approach to hide data in the cover image. In this method, we distinguish the RGB channels then we use one of the channels and perform discrete wavelet transformation (DWT) and transform it into four frequency components Low-Low (LL), High-Low (HL), Low-High (LH), and High-High (HH). Now, since the high-high frequency component is less sensitive to the human eye, it serves as perfect camouflage for the data. So, after we select the optimal frequency component, we perform SVD(singular wave decomposition) (B, Mr & N, Ms &Michahial, Stafford. (2016)) operation to make data more secure and then we apply LSB steganography to create the final file. We have also used various metrics for the comparison of our approach with the pre-existing approaches we have calculated the mean squared error between the actual image and the stegano image, which gave us the idea of the error in the bit values in the embedded image, we have also used PSNR(peak- signal- to – noise- ratio as a metrics to calculate the ratio between the noise and the signal of the transmitted image. Figure 1 depicts the proposed work in a block diagram.

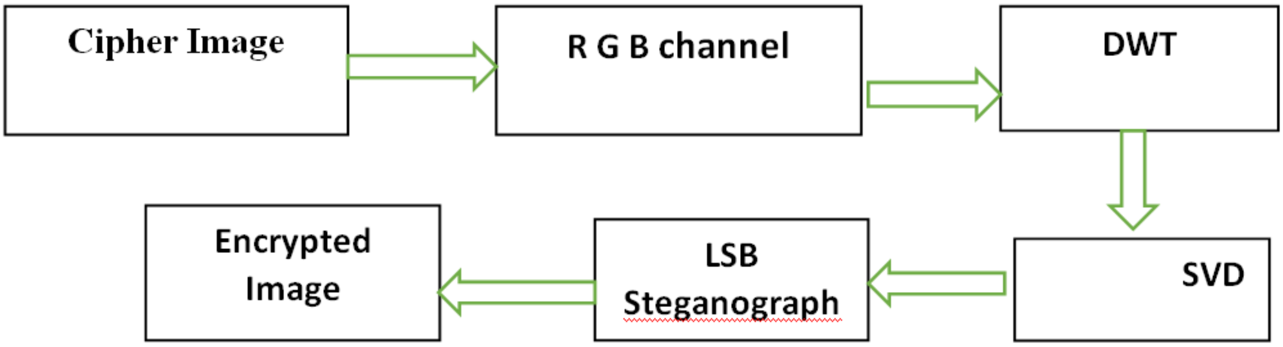


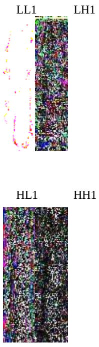
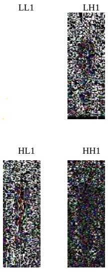
Figure 1: Block diagram of the proposed method

The same approach is used at the recipient end to extract hidden information from the encrypted image.

The encryption and decryption of data in an image are monitored through MATLAB, it is used to code and simulate the process of steganography. It provides information on MSE, the capacity of the cover image, PSNR, and encrypted data in the image.

EXPERIMENTAL RESULTS

The proposed method is implemented using the MATLAB software through which we used the Lena, Baboon, Peppers, and Sail Boat and tunnel image objects. All the cover images have .bmp image format and the same dimension of 512 × 512 and with the same size of 768KB of 24-bit-maps. We encrypted the data in all these images and compare the results in terms of MSE and PSNR to see how effective the proposed work. The Simulation results are mention in figure 2 given below:

Cover Image	DWT Extraction	Stegano Image	Cover Image	DWT Extraction	Stegano Image
					

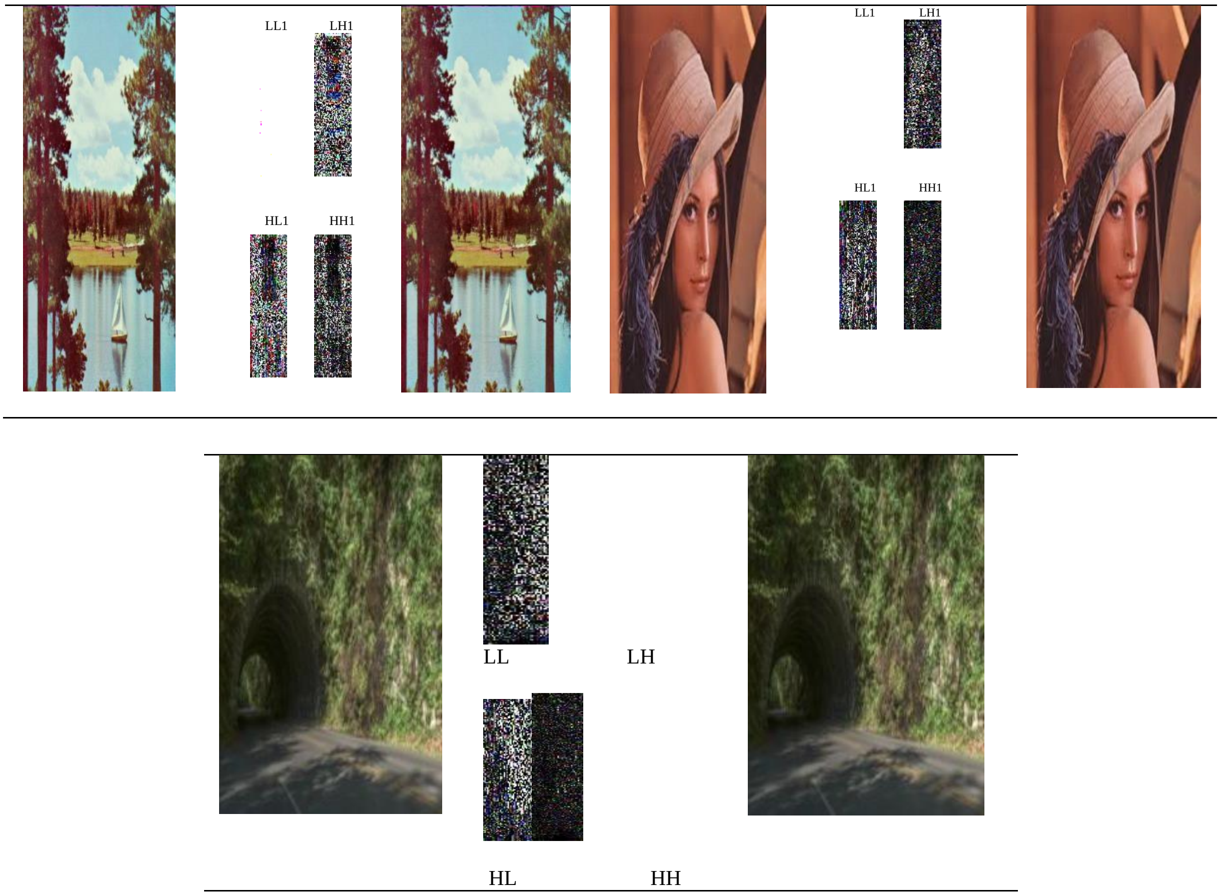


Figure 2: Column-wise Cover images, DWT extraction, and Stegano images peppers, sailboat, baboon, Lena, and tunnels.

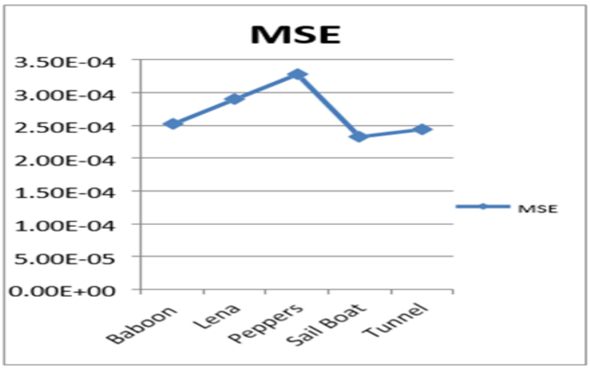


Figure 3: Comparison of MSE Values

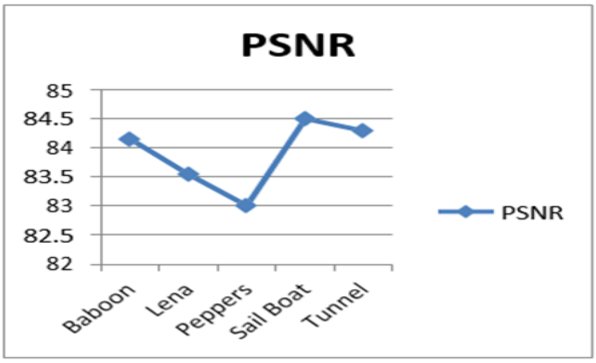


Figure 4: Comparison of PSNR values (dB)

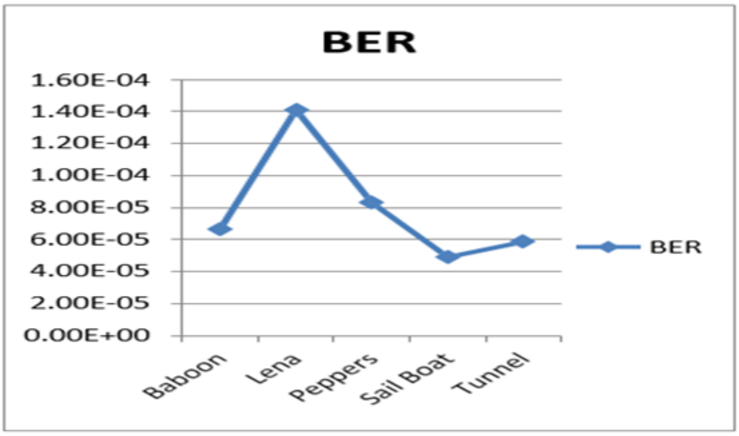


Figure 5: Comparison of BER values

Table 2: Stastical Measurement

Image Name	MSE	PSNR	BER
Baboon	2.5177e-004	84.1548	6.6757e-005
Lema	2.8992e-004	83.5421	1.4114e-004
Peppers	3.2806e-004	83.0052	8.2970e-005
Sail Boat	2.3270e-004	84.4969	4.9114e-005
Tunnel	2.4414e-004	84.2884	5.8651e-005

CONCLUSION

In this method, we proposed a highly secured method for encrypting data in the cover image. We have provided another layer of encryption to hide the data in the cover image using the properties of colored images and RGB channels. We used DWT, SVD, and then LSB steganography to achieve better results. We also analyzed the cover image as well as the Stegano image with respect to different parameters such as MSE, BER, PSNR, and the capacity of the cover image. It is a secure method that provides a secure method of encryption of data from malicious users.

REFERENCES

1. Anand, J. V. and Dharaneetharan, G. D. (2011). New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security. In *Proceedings of the 2011 International Conference on Communication, Computing & Security* (*ICCCS '11*). Association for Computing Machinery, New York, NY, USA, pp. 474–476. https://doi.org/10.1145/1947940.1948038
2. B, Mr & N, Ms &Michahial, Stafford. (2016). Image Compression using Singular Value Decomposition. *IJARCCE, 5(12)*, 208-211. https://doi.org/10.17148/IJARCCE.2016.51246
3. Chan, K and Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*, pp. 469-474. https://doi.org/10.1016/j.patcog.2003.08.007
4. Chen, P and Lin, H (2006). A DWT Based Approach for Image Steganography. *International Journal of Applied Science and Engineering, 4(3)*, pp. 275- 290.
5. Daneshkhah, A., Aghaeinia, H. and Seyedi, S. H. (2011). A More Secure Steganography Method in Spatial Domain. *2011 Second International Conference on Intelligent Systems, Modelling and Simulation, Phnom Penh, Cambodia*, pp. 189-194. https://doi.org/10.1109/ISMS.2011.39
6. Dey, S., Abraham, A. and Sanyal, S. (2007). An LSB Data Hiding Technique Using Prime Numbers. *Third International Symposium on Information Assurance and Security, Manchester, UK*, pp. 101-108. https://doi.org/10.1109/ISIAS.2007.4299758
7. Hosseinzadeh, M.(2020). 4-Robust control applications in biomedical engineering: Control of depth of hypnosis. *Control Applications for Biomedical Engineering Systems*, pp 89-125. https://doi.org/10.1016/B978-0-12-817461-6.00004-4
8. Jain, A and Gupta, I. S. (2007). A JPEG compression resistant steganography scheme for raster graphics images. *TENCON 2007 - 2007 IEEE Region 10 Conference*, Taipei, Taiwan, pp. 1-4.
9. Maiti C., Baksi D., Zamider I., Gorai P., Kisku D.R. (2011). Data Hiding in Images Using Some Efficient Steganography Techniques. In: Kim T., Adeli H., Ramos C., Kang BH. (eds) Signal Processing, Image Processing and Pattern Recognition. SIP 2011. *Communications in Computer and Information Science, 260*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27183-0_21
10. Mathkour, H., Al-Sadoon, B. and Touir, A.(2008). A New Image Steganography Technique. *2008 4th*

International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, pp. 1-4. https://doi.org/10.1109/WiCom.2008.2918

11. Mehboob, B. and Faruqui, R. A. (2008). A stegnography implementation. *2008 International Symposium on Biometrics and Security Technologies*, Isalambad, Pakistan, pp. 1-5. https://doi.org/10.1109/ISBAST.2008.4547669
12. Neeta, D., Snehal, K. and Jacobs, D. (2007). Implementation of LSB Steganography and Its Evaluation for Various Bits. *2006 1st International Conference on Digital Information Management*, Bangalore, India, pp. 173-178. https://doi.org/10.1109/ICDIM.2007.369349
13. Qadir, A. M. and Varol, N. (2019). A Review Paper on Cryptography. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, pp. 1-6. https://doi.org/10.1109/ISDFS.2019.8757514
14. Ramos, R, Valdez-Salas, B., Zlatev, R., Wiener, M. S., Rull, J. M. B. (2017). The Discrete Wavelet Transform and Its Application for Noise Removal in Localized Corrosion Measurements", *International Journal of Corrosion*, 2017, pp. 7. https://doi.org/10.1155/2017/7925404
15. Skodras, A. N. (2015). *Discrete Wavelet Transform: An Introduction*.
16. Thota, N. R., Devireddy, S. R. (2008). Image Compression Using Discrete Cosine Transform. *Georgian Electronic Scientific Journal: Computer Science and Telecommunications,3 (17)*.
17. Walia, E., Jain, P., Navdeep (2010). An Analysis of LSB & DCT based Steganography. *Global Journal of Computer science & technology,10(1.0)*.
18. Zhang, D. (2019). Wavelet Transform. In: Fundamentals of Image Data Mining. Texts in Computer Science. *Springer*, Cham. https://doi.org/10.1007/978-3-030-17989-2_3