International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IMAGE STEGANOGRPHY USING MODIFIED DWT TECHNIQUE

N. BrahmaNaidu[1], Associate Professor, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Kandimalla RamaKrishna[2], **Keerthi Diyyala**[3], **Manne Sai Swaroop**[4], **Kolla Sandeep**[5]
[2,3,4,5] UG Students, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1] nbnaidu1208@gmail.com
[2] kandimallaramakrishna123@gmail.com, [3] keerthidiyyala2002@gmail.com ,
[4] saiswaroop.msai@gmail.com , [5] sandeepkolla100@gmail.com

Abstract

The modern computing world revolves around the word "DATA", but just what is so intriguing about it? In today's world, data is the power and business start realizing it because data can predict customer trends potentially, get increased sales, and help the organization to achieve newer heights. The technology has become so advanced and our topmost priority is to secure data. Here in this project, the high frequency coefficients produced by the discrete wavelet transform contain hidden messages. To enhance the quality of the images, low frequency sub-band coefficients are kept intact. Before embedding, some elementary mathematical operations are performed on the secret messages. These operations prevent messages from being stolen or destroyed by unauthorized internet users, and they do so while also providing adequate security.

Keywords: DWT (Discrete Wavelet Transform), LSB (Least Significant Bit), IDWT(Inverse Discrete Wavelet Transform)

Introduction

The process of hiding a secret message within a larger one so that the contents or presence of the hidden message could not be known to anyone and this process is known as steganography. Steganography serves the main purpose which is to provide secret communication between two groups. Cryptography which can conceals only the contents of a secret message but steganography can able to conceal the fact that a message is communicated. Though there are some differences between steganography and cryptography, there are many analogies between them and some authors categorize steganography as a type of cryptography because hidden communication is a type of secret message. We can perform steganography on different transmission media like images, video, text, or audio. Image Steganography is a technique used to hide data in an image

that can be used for secure data exchange. One of the famous algorithms that are used for image steganography is DWT(Discrete Wavelet Transform).Implementation of DWT is tricky and has many issues such as decimal and negative values which cannot be stored in an image. To solve this there are many proposed solutions with some drawbacks . In this paper, we explore one such solution to address the implementation issues of DWT.

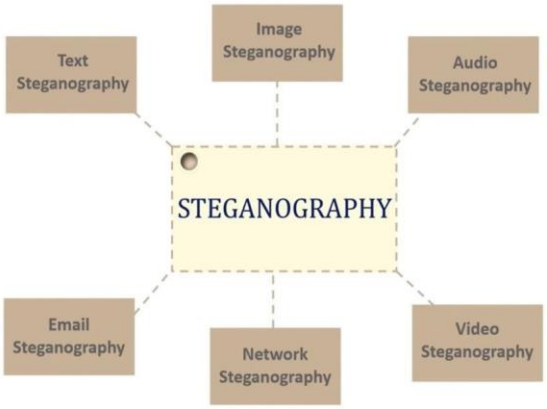


Fig.1. Steganography techniques

Literature Survey

Various researchers have made significant contribution in the area of steganography few of them have been discussed in this paper.

It provides an overview of various steganography techniques, methods, standards, benefits, and drawbacks. The paper also explains a method that can use any type of image file without converting it to a bitmap and without using more memory than is necessary. [1].It gave an overview of different steganographic techniques and its major types and classification of steganography. It tells about the types of steganography which are image, audio, video, text. Here it gave the description of the techniques and comparison between the techniques, it tells about the terminology required for performing the steganography technique on the images [2].For providing security for the text which is being embedded into the image that is implemented by using cryptography technique such as DES algorithm .By using this technique the text which is embedding is encrypted so that security for the image is increased[3].It tells about steganography and cryptography together initially the information using des algorithm and hide inside the image before hiding the image is converted from partial to frequency domain. It uses 2-d HAAR dwt horizontal procedure, vertical position for embedding data. The LSB of wavelet can be replaced by message signal. It uses DES algorithm for encrypting data which is a 8-bit algorithm and key is 64-bit. The various stages are key transformation, expansion Permutation, S-box substitution, p-box permutation , XOR and swap[4].In this paper they discussed about HAAR algorithm of dwt in which the cover image is disintegrated into three colour planes, red, green, blue in order to embed secret images into each colour plane. Each colour plane is decomposed into four sub bands LL, LH, HL and HH. On each plane n-level dwt is applied the results of these three-planes is given as an input to extraction algorithm to get three secret images. It

programmed in MATLAB with some 64 -bit operation and execution time is 50 seconds. The stimulation results suggest that this technique maintains good image quality and it is robust with in comparison with different image processing operations. The average pear signal-to-noise ratio (PSNR) value obtained for stego-image is 55.53, average Mean Square value (MSE) value is around 5 to 10 [5].

Problem Identification

Dwt technique used for secure transfer of data from send to receiver in various approaches and each of them has certain pros and cons but this paper mainly focus on resolving certain cons of a particular methodology by modifying the dwt technique and adding two methods to the technique to achieve data security.

It mainly focus on embedding text inside a image and send image to client where the client decode the image to get required data

Methodology

DWT technique

One of the techniques to store the data in an Image while maintaining very little or no visible change in an Image is the LSB(Least Significant Technique) which stores the data in the last bit of an Image. But one can easily get the data just by looking into the image bits. This is solved by DWT using frequency coefficients. One of the DWT techniques is the Haar-DWT which is the simplest DWT.

A. HARR-DWT

In this method, 4 pixels are used to generate 4 coefficients. The 4 pixels are selected either by taking squares of 2X2 or in any other way such that each pixel is only taken once. The formulas that are used to calculate the coefficients d1, d2, d3, and d4 from the pixels p1, p2, p3, and p4 are as follows.

d1 = (p1+p2+p3+p4)

d2 = (p1-p2+p3-p4)

d3 = (p1+p2+p3-p4)

d4 = (p1-p2-p3+p4)

The process of calculating the coefficients is known as DWT. The data is embedded on these coefficients rather the pixels using techniques such as LSB. After embedding the data the coefficients are used to generate the pixel values to form the image this step is known as Inverse DWT. The new pixels P1, P2, P3, and P4 are calculated from the coefficients D1, D2, D3, and D4 using the formulas

P1 = (D1+D2+D3+D4)/4

P2 = (D1-D2+D3-D4)/4

P3 = (D1+D2+D3-D4)/4

P4 = (D1-D2-D3+D4)/4

Decoding is done by following the DWT step and extracting the coefficients from the embedded image and the required data is present in the LSB of the coefficients.

B. Problem with the above approach

A Black and white image pixel values range from 0 to 255 Integer values. As we

can see in the above image on calculating the new pixels P1, P2, P3, and P4 there is a clear chance of getting a fraction value. If we ignore the fraction value and just store the decimal value we cannot get the same coefficients from the pixels when extracting the data. This leads to errors in the extracted data, so we need to store the fraction values. Another issue we have is the possibility of a negative value that cannot be stored in an image. Ignoring the sign will lead to false data in extracting process. There is also a chance of exceeding the limit of 255.

Implementation

A. Existing Approach

In order to solve the discussed issues there are many techniques and tricks such as storing the decimal values separately in the form of the description of the Image or dividing the pixel value by 2 since the range of possible values goes from -256 to 256 dividing by 2 doubles the range. But it affects the quality of the embedded image significantly. Storing decimal values required additional memory. In order to address the said issues effectively we propose the following solution.

B. New Approach

In this approach in order to solve the possibility of negative values we use a different set of formulas as follows.

d1 = p1 + p3 + p4 - 2*p2

d2 = p2 + p4 + p1 - 2*p3

d3 = p3 + p1 + p2 - 2*p4

d4 = p4 + p2 + p3 - 2*p1

The above set of formulae is used for calculating the coefficients. After embedding the data the following formulas perform Inverse DWT to generate an Image from new coefficients D1, D2, D3, and D4.

P1 = (D1 + D2 + D3) / 3

P2 = (D2 + D3 + D4) / 3

P3 = (D3 + D4 + D1) / 3

P4 = (D4 + D1 + D2) / 3

When performing LSB the pixel value is changed by at most 1 which is not visible to the naked eye. Since the Inverse DWT formulas don't contain a negative sign we can safely rule out the possibility of a negative value. We still have the fraction values as we are dividing the sum by 3. To solve this issue we use a simple trick to store the fraction data within the pixel itself. To solve the fraction issue we first divide the pixel value by 3 before calculating the coefficients. The division is a floor division. Let p1, p2, p3, p4 be the pixels and np1, np2, np3, np4 be the pixel values after the division by 3. i.e np1=p1/3 and so on. Since we have pixels divided by 3 we can safely remove the division by 3 in the IDWT step. But we still need to calculate the coefficients while extracting the data which requires the pixel values to be the same when calculated by the IDWT formula. In order to save the fractional value we remove the division by 3 from IDWT and recalculate them to the divided version when calculating the coefficients.

1. Embedding step

np1 = ⌊p1/3⌋

np2 = ⌊p2/3⌋

np3 = ⌊p3/3⌋

np4 = ⌊p4/3⌋

d1 = np1 + np3 + np4 - 2*np2

d2 = np2 + np4 + np1 - 2*np3

d3 = np3 + np1 + np2 - 2*np4

d4 = np4 + np2 + np3 - 2*np1

P1 = (D1 + D2 + D3)

P2 = (D2 + D3 + D4)

P3 = (D3 + D4 + D1)

P4 = (D4 + D1 + D2)

2. Extracting step

nP1 = P1/3

nP2 = P2/3

nP3 = P3/3

nP4 = p4/3

d1 = np1 + np3 + np4 - 2*np2

d2 = np2 + np4 + np1 - 2*np3

d3 = np3 + np1 + np2 - 2*np4

d4 = np4 + np2 + np3 - 2*np1

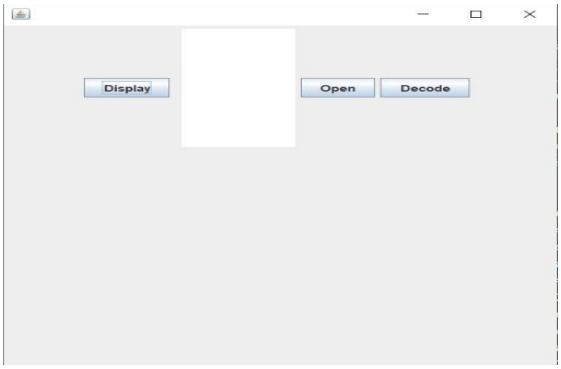
Since the floor division by 3 only takes away of utmost 2 pixels it is negligible and not visible to the naked eye.

Handling Edge Case

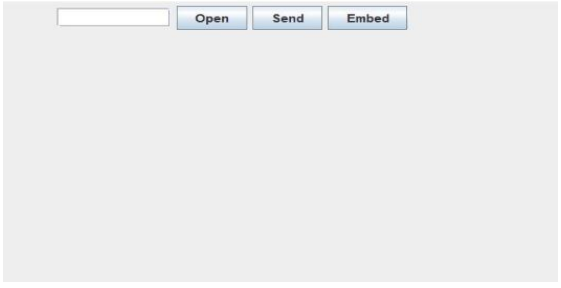
In the IDWT formulas,Since we are adding the values there might be a chance of overflow. This can be seen in the example when p1 = 255, p2 = 255, p3 = 255, and p4 = 0. Then the new pixels will be np1 = 85, np2 = 85, np3 = 85 and np4 = 85. Then the coefficients will be d1 = 0, d2 = 0, d3 = 255 and d4 = 0. When data is embedded using LSB, the coefficients might become d1 = 1, d2 = 1, d3 = 255, and d4 = 1. In such cases, the value exceeds the limit. To solve this issue we can do a border correction step which includes subtracting the new pixel values by 2 which only changes the value by at most 7 pixels which doesn't affect the quality of the embedded image.

Results & Conclusion

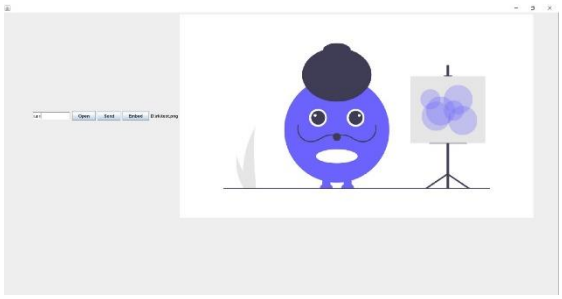
1.First we have to run the server application page



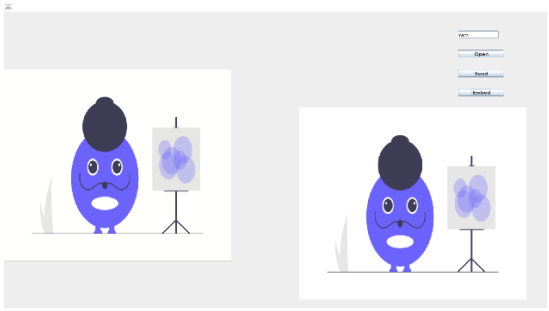
2.Next,we have to run client application in other instnace



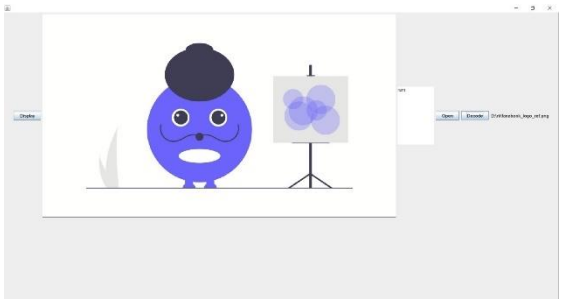
3.Now click on open button and we get a filechoser,there we have select an image to encode text



4.Moving further,we have to type text that has to be embeded in the text in the text box and now click on the emebed button to embed text in the image.



5.In the receiver end,we have to click on display button to get image from the server.after that we have click on open button to open stego-image which is received from the sender.now have click on the decode button to display text in box.



Limitations& Future Scope

DWT-based steganography techniques are vulnerable to a range of attacks, including statistical analysis and visual inspection. An attacker can use statistical analysis to detect the presence of hidden data, while visual inspection can reveal the presence of artifacts or distortions in the cover image.

Recent advances in deep learning have shown promising results in image steganography.Using deep learning-based techniques could increase the capacity and security of steganography systems.

References

[1] An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques Mukesh Garg Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper is Available online at: www.ijarcsse.com.

[2] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April, 2020.

[3] International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.68-71.

[4] International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012)

[5] T. Morkel , J.H.P. Eloff and M.S. Olivier “An Overview of Image Steganography”

[6] Hamad A. A, Ali A, Majid A. A, Waleed A, “High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data”, IEEE Jordan Conf. on Applied Electrical Eng. and Comp. Tech., March 2015.

[7] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 4, 3: 275-290. 2006.

[8] American Journal of Engineering Research (AJER) e-ISSN: 2320- 0847 p-ISSN: 2320-0936 Volume-02, Issue-11, pp-122-128 www.ajer.org .

[9] https://github.com/Rajesh-dot/steno