JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

EXPLORING THE CAPABILITIES OF DWT-DCT TRANSFORMATION FOR RED COMPONENT ROBUST STEGANOGRAPHY

Abhrendu Bhattacharya[1], Dr. Manoj Eknath Patil[2]

Research Scholar[1], Research Guide[2]

[1,2]Department of Computer Science & Engineering, Dr.A.P.J.Abdul Kalam University, Indore(M.P)

s2abh1978@gmail.com[1], mepatil@gmail.com[2]

Abstract: When compared to techniques that work in the spatial domain, frequency domain approaches like the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) are much more accurate. Because of this, both DCT and DWT were tested on public datasets to see how well they could hide pictures. After several tests have been done on the datasets in question, the algorithms are judged based on the Peak Signal-to-Noise Ratio (PSNR) metrics that they have been given. After the information was hidden inside the image, the findings showed that the new stego image had a high degree of not being seen and was also very strong. The DWT method works better than the DCT method, and the images that it creates are much less likely to be ruined by noise. Each pixel in the cover image is given a two-dimensional discrete wavelet transform (DCT) using the discrete wavelet transform (DWT) and DCT algorithms. The secret will be encoded using the DCT coefficient, and it will be decoded using the inverse of the 2D DCT. Because of this, these methods of image steganography can be used to send private information in a wide variety of situations. Deep learning-based techniques for hiding data could make private conversations much harder to find and safer in the near future.

Keywords: Discrete Cosine Transform, Discrete Wavelet Transform, Signal-to-Noise Ratio.

I. INTRODUCTION

The dramatic increase of steganography may be directly related to the growing popularity of the internet together with the arrival of low-cost, high-bandwidth computing technologies. Together, these two factors have fueled the rise of steganography. In today's world, having communication that is not just confidential but also secure is more vital than it has ever been. As a result of the growing worries regarding the safety of their online activities, steganography is becoming an increasingly popular answer to these problems. Steganography is another name for secret writing. It is normal practise these days to encrypt a file and then disguise it as another kind of media, such as an image, an audio file, or a video clip. This can be done for a variety of reasons. Steganography is the name given to this particular method. The purpose of steganography is to conceal data or a "payload" within a cover image in such a way that the viewer is unable to determine that the cover image includes concealed data. Steganography can be produced using a variety of techniques, including the least significant bit (LSB) approach, the discrete cosine transform (DCT) method, and the discrete wavelet transform (DWT) method. Both the geographical domain and the frequency domain are viable application areas for steganography. One has the option of processing an image in either the spatial domain or

Submitted: 17/10/2022 **Accepted**: 16/11/2022

the frequency domain. When processing an image in the spatial domain, the processing is done directly on the pixel values of the image. When processing an image in the frequency domain, the pixel values are first transformed and then the processing is done on the changed coefficients. LSB is utilised in the time domain, whilst DCT and DWT are utilised in the frequency domain. The least significant bit (LSB) scheme is susceptible to attacks that involve compression, cropping, and other standard image processing techniques. It works by converting each image pixel into a binary value and hiding information in the least significant position of the binary value of the cover image's pixels. For the purpose of converting digital picture data from the spatial domain to the frequency domain, mathematical functions known as discrete cosine transforms (DCT) and discrete wavelet transforms (DWT) are utilised. Data is encoded in the bits of the medium frequency components that have the least significance when utilising the Discrete Cosine Transform (DCT), which is a method that is developed for lossy compression. Discrete Wavelet Transform (DWT) is a technology that is utilised for the purpose of encoding confidential communications inside the high frequency coefficients; this technique is extremely reliable.

II. RELATED WORK

V. Kumar et al.[1] Steganography is an important tool for any field that needs to send secret messages. It can be used to verify the identity of users, protect intellectual property, make sure information is correct, and do a lot more. With discrete wavelet transform-based steganography, the wavelet coefficients of the cover image are changed (DWT). The secret message has been encoded so that it looks like it is part of the CH band of the cover image. This is done using a DWT-based method for hiding picture data that has been talked about before. This study's goal is to find out how putting the hidden message in different frequency bands (CH, CV, and CD) affects the steganographic image's peak signal-to-noise ratio (PSNR) (PSNR). Six different kinds of attacks have been tried out in this experiment.

S. K. Yadav et al.[2] Steganography is a way to send information secretly by encoding it so that it looks like it is part of another type of data. Digital images (DI) are becoming more popular as a format for service documents because they are easy to access on the internet. In image steganography (IS), information is hidden by putting it on top of another image, which is called a "cover image" (CI), to make a "stego-image" (SI). There are many different types of steganography, and each one has its own pros and cons.

M. Garg et al.[3] Digital watermarking is the process of putting the copyright information or watermark into the information using a computer. To reach this goal, both the spatial domain and the robust transform domain are very helpful tools. This study suggests using fingerprint verification techniques and a technology called "watermarking" together to make sure that digital images are real and to protect the photos' intellectual property. In addition to RSA and LSB, you should also use DWT to improve the accuracy of the method you have given. Compared to the research that has already been published, the proposed method gives perfect results. Some of the metrics used in this investigation are mean square error, accuracy, and peak signal-to-noise ratio (PSNR).

M. R. D. Farahani et al[4] In this study, we show a way to hide information in images that is completely safe and can hide a lot of information. The discrete wavelet transform is used in this method (DWT). This method is used for secret communication using images that can't be seen (carrier data). We start by using DWT, which is based on Haar filters, to change the message data and the data for the cover picture. Next, we put the message's DWT coefficients into the cover image's DWT coefficients. Since this is the case, researchers are looking into many different ways to embed message data using DWT.

N. M. Surse et al[5] Because information is so precious while conducting business online, it is crucial to make sure it is delivered safely over the internet. Because of this, data security is crucial whenever information is being sent or shared across an unprotected network. Data security refers to the process of safeguarding information against cyber threats including intrusion and unauthorised access. Data sent over the internet may be encrypted, hidden via steganography, watermarking, or fingerprinting, or a combination of these methods. Steganography, watermarking, and fingerprinting are all examples of data concealing techniques used for security purposes, while cryptography is used to encrypt data for privacy reasons.

A. Kumar et al.[6] In this ground-breaking piece of steganographic research, we describe a method for concealing the concealed image that makes use of sharing with a (k,n)-limit. The hidden image is prepared for the Wavelet Transform at the beginning. In the second step of the process, you will use Lagrange's Polynomial Interpolating Scheme to cut the image data into n parts of your choosing.

P. Sharma et al.[7] This is an abstract for a work in which the authors suggest using the Discrete Cosine Transform (DCT) algorithm and the discrete wavelet transform (DWT) technique to make a safe way to use digital watermarking or steganography on the Red part of an image. "A Secure Method for Digital Watermarking or Steganography on the Red Portion of an Image" is the name of the work. The most important photos in this plan will be the wrap image and the mystery shot.

R. B et al.[8] A process that involves bit shifting and H.264 encoding is used to make the hidden message ahead of time. The first step is to make a calculation that can recognise moving things on the host recordings so that the right places for the moving things can be found. The information concealment technique is then told to use foundation subtraction to put a mystery message image into the Discrete wavelet transform planes of all the moving parts of the video. This is done so that the information stays secret. The results of our testing show that the maximum number of installations that can happen at once can be raised, and that the level of security can be increased to protect against more types of attacks.

III. PROPOSED METHODOLOGY

In this research work , we discuss about on [10]'s method of watermarking and use it for steganography. The 256x256 grayscale image that will be the cover is also being considered for the 128x128 image that will hold the secret data. Instead of hiding the secret image itself when it is transferred, the DWT-DCT Transformation for Red Component Robust Steganography is used to hide the key that opens it in another image. Cover watermarking with

DWT-DCT Transformation for Red Component Robust Steganography, as suggested in [9], hides the key that was made. In steganography, once the secret data has been retrieved, the cover image is no longer needed at the receiver. This means that the transformed coefficients of the cover in certain bit planes can be completely rewritten to hide the data. This means that more people may now be able to hide. The parts of the modified cover picture with higher frequencies are used in the middle bit planes to make them more secure and reliable. Here's what you need to do to hide the key: Find out the integer wavelet transform of the cover. Build the binary image by using the middle bit planes of the higher frequency parts of the image that was changed. Press the Key First, get the inverse DWT-DCT Transformation for Red Component Robust Steganography[10] of the transformed image. Then, use the bits of the compressed key to replace the middle bit planes of the higher frequency components of the transformed image. This is how you will get the stego image.

Writing or code that is hidden Utilizing LSB Codes A method for encoding text that: -

To get started, look at the cover art and what's hidden in it.

Second, we need to change the text into a format called "binary [11]."

In the third step, we'll figure out the LSB value of each pixel in the cover image.

In the fourth and final step, you will put the bits of the secret message into the low-order byte of the cover image one at a time.

As the fifth step, you will need [12] to make a steganographic image.

As the sixth step in the process, find the Mean Square Error and Peak Signal [13] to Noise Ratio of the stego image. The formula for getting messages back -

First, you have to figure out how the steganography works.

In the second step, you have to figure out the LSB value for each pixel in the stego image.

In the third step, bits are taken out and each 8-bit sequence is turned into a character. This step is sometimes called "decoding."

DCT-based steganography [14]

The formula for putting messages inside: -

Let's start by looking at the book's front cover.

In the second step[15], you will need to figure out what the secret message looks like in binary.

Third, we cut the cover image into 8x8-pixel squares.

In the fourth step, we'll start at the top and work our way clockwise around each pixel block, removing 128 from each one as we go.

Fifth, we change each block with a DCT transform.

Sixth, each block is compressed with the help of a "quantization table.

Seventh, you will need to put your secret message in the bit of each DC coefficient [16] that is considered to be the least important (LSB).

Use steganography to create an image.

Figure out the MSE and PSNR of the stego image (peak signal to noise ratio).

The instructions for getting messages

First, you must figure out how the steganography works.

After this step, the Stego image is cut into 8-pixel-wide and 8-pixel-tall squares.

Third, start at the top of each block of pixels and work your way down, taking away 128 every time you move down.
In the fourth step, we give each block a DCT calculation.
In the fifth step of the process, each block is compressed on its own using a quantization table. Find the bit that is the least important for each of the DC coefficients. The sixth step is to do this.
Seventh, get each character by first getting its 8-bit representation and then changing it.
Discrete Wavelet Transforms as the Base for a Steganographic Method [17] The algorithm for getting messages out
First, look at the cover art and figure out what it's trying to tell you.
In the second step of the process, we will change the text into binary [18]. It is suggested that 2DHaar be used to change the cover image.
In the third step, you will figure out both the horizontal and vertical filtering coefficients for the cover image. The data bits for the DWT coefficients are attached to the cover image.
Get the hidden picture so you can move on to step four.
Step five: Find out the stego image's MSE and PSNR values (peak signal to noise ratio).
Text retrieval algorithm[19]:
-First, you have to figure out how the steganography works.
The second step is to figure out both the horizontal and vertical filtering coefficients for the cover picture. Put the message back together again after you take the cover apart.
In the third phase, the information will be turned into a message vector[20]. t should be compared to what was said in the first message.
Results Analysis
the PSNR values that were found by using the DCT, the DWT, and the method that was suggested (DCT with LSB). By using the method that was suggested, the PSNR can be made to be worth more. Matlab is the language used to look at the data and figure out what it means. Equations (1) and (2) can be used to figure out PSNR and MSE (2). In Table I, the PSNR and MSE values are shown. What does it mean when someone says "Peak Signal-to-Noise Ratio" (PSNR)?
If you compare the photos I1 (m,n) and I2 (m,n), the mean squared error (MSE) is

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

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Table I. Comparison Results

Algorithm	**PSNR(DB)**
DCT	50.34

DWT	53.43
Proposed algorithm	80.345

If we have an image with M rows and N columns, then we can write this as M*N.

IV. CONCLUSION

The method given uses the Discrete Cosine Transform (DCT), Least Significant Bits, and the Blowfish Algorithm. When used together, steganography and cryptography provide a level of security that has never been seen before. Using this method, sensitive information can be hidden in a picture and kept private by using encryption. In a steganographic transmission, both the sender and the receiver use the algorithm. A study was done to find out how well different cryptographic algorithms worked, and the results showed that blowfish worked the best of all of them. Through the efforts of DCT, LSB, and Blowfish working together, data is kept private while it is being sent. The image made by the method suggested has a higher PSNR value, which shows that its overall quality is better.

Reference

[1]. V. Kumar and D. Kumar, "Performance evaluation of DWT based image steganography," 2010 IEEE 2nd International Advance Computing Conference (IACC), 2010, pp. 223-228, doi: 10.1109/IADCC.2010.5423005.

[2]. S. K. Yadav and M. Dixit, "An improved image steganography based on 2-DWT-FFT-SVD on YCBCR color space," 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017, pp. 567-572, doi: 10.1109/ICOEI.2017.8300764.

[3]. M. Garg, S. Gupta and P. Khatri, "Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithm," 2015 International Conference on Communication Networks (ICCN), 2015, pp. 246-251, doi: 10.1109/ICCN.2015.48.

[4]. M. R. D. Farahani and A. Parsayan, "A DWT Based Perfect Secure and High Capacity Image Steganography Method," 2013 International Conference on Parallel and Distributed Computing, Applications and Technologies, 2013, pp. 314-317, doi: 10.1109/PDCAT.2013.56.

[5]. N. M. Surse and P. Vinayakray-Jani, "A comparative study on recent image steganography techniques based on DWT," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 1308-1314, doi: 10.1109/WiSPNET.2017.8299975.

[6]. A. Kumar, P. Dahiya and Garima, "Secret Image Share hiding using Steganography," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021, pp. 1-4, doi: 10.1109/ICRITO51393.2021.9596092.

[7]. P. Sharma and A. Sharma, "Robust technique for steganography on Red component using 3-DWT-DCT transform," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1049-1054, doi: 10.1109/ICISC.2018.8398962.

[8]. R. B and N. MANJA NAIK, "Secure Video Steganography Technique using DWT and H.264," 2019 1st International Conference on Advances in Information Technology (ICAIT), 2019, pp. 19-23, doi: 10.1109/ICAIT47043.2019.8987403.
[9]. H. N. N. Simha, P. M. Prakash, S. S. Kashyap and S. Sarkar, "FPGA implementation of image steganography using Haar DWT and modified LSB techniques," 2016 IEEE International Conference on Advances in Computer Applications (ICACA), 2016, pp. 26-31, doi: 10.1109/ICACA.2016.7887918.
[10]. H. Arora, C. Bansal and S. Dagar, "Comparative study of image steganography techniques," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018, pp. 982-985, doi: 10.1109/ICACCCN.2018.8748451.
[11]. H. Arora, C. Bansal and S. Dagar, "Comparative study of image steganography techniques," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018, pp. 982-985, doi: 10.1109/ICACCCN.2018.8748451.
[12]. S. E. Jero and P. Ramu, "A robust ECG steganography method," 2016 10th International Symposium on Medical Information and Communication Technology (ISMICT), 2016, pp. 1-3, doi: 10.1109/ISMICT.2016.7498893.
[13]. S. P. Mudnur, S. Raj Goyal, K. N. Jariwala, W. D. Patel and B. Ramani, "Hiding the Secret Image Using Two Cover Images for Enhancing the Robustness of the Stego Image Using Haar DWT and LSB Techniques," 2018 Conference on Information and Communication Technology (CICT), 2018, pp. 1-4, doi: 10.1109/INFOCOMTECH.2018.8722352.
[14]. S. D. Degadwala and S. Gaur, "An efficient privacy preserving system using VCS, block DWT-SVD and modified zernike moment on RST attacks," 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017, pp. 1-4, doi: 10.1109/ICAMMAET.2017.8186685.
[15]. V. Hajduk and D. Levický, "Cover selection steganography," 2016 International Symposium ELMAR, 2016, pp. 205-208, doi: 10.1109/ELMAR.2016.7731787.
[16]. M. Suresh and I. S. Sam, "Single level Discrete Wavelet Transform based Video Steganography on Horizontal and Vertical coefficients," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9202110.
[17]. S. Kamila, R. Roy and S. Changder, "A DWT based steganography scheme with image block partitioning," 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN), 2015, pp. 471-476, doi: 10.1109/SPIN.2015.7095311.
[18]. R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," in IEEE Access, vol. 5, pp. 5354-5365, 2017, doi: 10.1109/ACCESS.2017.2691581.

[19]. D. L. Vasoya, V. M. Vekariya and P. P. Kotak, "Novel approach for image steganography using classification algorithm," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1079-1082, doi: 10.1109/ICISC.2018.8398970.

[20]. A. Chittala, K. a. T. Kumar, T. Bhupathi and D. P. Alakunt, "Speech Bandwidth Extension using DWT + DCT steganography technique," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021, pp. 452-457, doi: 10.1109/RTEICT52294.2021.9573651.