Journal of
Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7642796

DESIGN AND IMPLEMENTATION 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

Steganography is the process of hiding a secret message inside another message so that only the sender and the person who is supposed to get it knows it's there. This secret message could be a string of words or even an image. Image steganography is the process of hiding a picture inside another picture. Steganography can be used for a number of good things in the modern world. The goal of this paper is to compare and contrast some existing methods, such as the Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), along four dimensions. These are quietness, durability, capacity, and signal-to-noise ratio at the peak (PSNR). Based on what we've found, DWT seems to be the best option. As a bonus, we also did noise analysis on the procedures we just talked about. To Exploring the Capabilities of DWT-DCT Transformation for Red Component Robust Steganography.

Keywords: Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT)

1. Introduction

In the past few years, the number of people who have access to the internet has grown dramatically. These people are spending more of their time in the thriving online marketplace for digital entertainment. Since digital content and multimedia are getting easier to access, the risks that come with their lack of security are growing at an alarming rate. Copyright protection in the digital world of today is a tough problem.

Many different scientific groups have come up with different ways to protect IP. With digital watermarking, files, photos, music, and videos can all be kept from being copied without permission. It is also one of the least expensive options. Digital picture watermarking can be broken down into two main groups: blind and non-blind. On the other hand, in order for non-blind watermarking to function, it is necessary to have access to the original cover image as well as additional information. Blind watermarking enables one to recover the watermark even if they do not have access to the facts mentioned above. Blind watermarking is a form of digital watermarking. Because it does not require any prior knowledge of the protected content or its cover art in order to retrieve the watermark, blind watermarking is the most difficult method. For watermarking purposes, it is possible to make use of both the spatial domain and the transform domain. The use of convenient and efficient spatial domain watermarking is undermined, however, by its susceptibility to a wide variety of threats. It is possible to hide watermark bits in a digital image by modifying the values of the pixels in the image's original state; however, this reduces the image quality. One of these methods is called Least Significant Bit Substitution (LSBS for short). When images are transferred to the transform domain, the watermark bits are initially hidden in a manner that is not reliant on the pixel frequency. The discrete cosine transform (DCT), the discrete wavelet transform (DWT), the fast fourier transform (FFT), and the lifting wavelet transform (LWT) are a few examples of different transform domains (LWT).

2. Related work

Er. Harjinder et al.(2017) In this study, we use a combination of the DCT and the DWT to get better results when compressing data. There are MATLAB programmes that can be used to help with the DCT, DWT, and DCT+DWT methods. The data collected shows that the DCT+DWT strategy is better than the solo JPEG-based DCT, DWT method in terms of the peak signal-to-noise ratio (PSNR) and how the image looks at higher compression ratios. This is true no matter how much the file is compressed. In the last step, the proposed method's results are compared to those of basic compression techniques like DCT and DWT. This is done with the help of three measures of quality. The results of the simulation show that using a hybrid strategy (DWT-DCT) that also uses steganography works better than just using JPEG-based DCT and DWT algorithms.

Laxmi Gulappagol et al.(2019) This study shows how Multiple Object Tracking can be used as a steganographic method in the transmission domain. This is done by using the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT) with the H.264 algorithm to encode and decode (DCT). At the start of the process, the incoming video is cut into a certain number of frames. This is the first step in being able to find and follow moving objects. In two dimensions, the RGB colour channels of each moving area go through a discrete wavelet transformation. Because of this, the spectrum is then split into the LL-LH and HH sub bands. DCT is also used in the same dynamic range. This is done so that DC and AC co-efficiency can be reached. A stego video is made by putting together parts of the original frame with changed parts of the frame's motion. The performance study looked at a number of different metrics, such as the Peak Signal-to-Noise Ratio (PSNR), Correlation, Mean Square Error, and SSIM.

T. Yuvaraja et al.(2018) It means putting information away in a way that makes it look like nothing is being hidden. Data transmission from one place to another is hard to do safely because there is a chance of attack or accidental change during transmission. Encryption is now the standard way to keep sensitive information from falling into the wrong hands. Any communication system that uses encryption runs the risk of making would-be attackers want to break through the defences to get to the encrypted data. Steganography is a method that can be used to hide information to make it safer. It makes it easy to hide information at any time or place.

Eyssa et al.(2020) Since there isn't a lot of research on this topic, the goal of this analysis is to find out how channel degradation affects the search for hidden images. The Discrete Cosine and Discrete Wavelet transforms are used quite a bit in the way that was suggested. Once the brightness and colour values of the cover picture have been found, the hidden images can be swapped for them. The chaotic Baker map is used to protect sensitive images. It is part of a family of permutation-based algorithms that are more resistant to channel degradations. This map is used to hide what's in the pictures. You should be able to find a safe place to keep the pictures if you use this map as a guide. The main focus of the research was on orthogonal frequency division multiplexing (OFDM), a method of wireless communication that evens out the channels, as well as other similar methods. The results of the simulation show for sure that the steps that were taken to make sure that visual communication was reliable worked.

Hasan N.et al.(2021) Our research shows how cryptography can be used to mark an image with a watermark. At the second order, the system uses both the discrete cosine transform (also called the DCT) and the discrete wavelet transform (also called the DWT). A function for automatic extraction is also built in (2DWT). After comparing the 2DWT's visibility to that of other watermarking algorithms and its ability to stay hidden across a range of decomposition depths, it was decided that the 2DWT was the best watermarking method. Also, the 2DWT was able to hide itself no matter how deep the decomposition went. Using a method called discrete cosine transform (DCT), the image coefficients are combined into a single vector by doing a zig-zag operation on the selected area.

3. Methodology

In the study, both DCT and DWT are used and analysed, as well as a hybrid method that takes parts from both. Each module is looked at with both first-hand and second-hand data.

Secondary image data are stored in image data sets and can be in jpeg, bmp, or gif format. Primary image data are the actual pictures taken with the camera. The sipi pictures dataset is one example. Researchers have found that the above method is the safest because it has a high Peak Signal to Noise Ratio. Knowing that the goal of steganography is to stop eavesdropping, we can see that the methods used by steganographers are meant to make the message itself invisible to someone who isn't a part of the process. This is why it's important to compare the DCT and DWT algorithms, using the peak signal-to-noise ratio (PSNR) to measure how well each one works (Peak Signal to Noise Ratio). The goal of this comparison was to find the most secure and up-to-date way to do things.

3.1 Structure

The combined DCT/DWT method for hiding data will be compared to each of the methods on its own. Figure 3.1 shows how each method is generally set up.

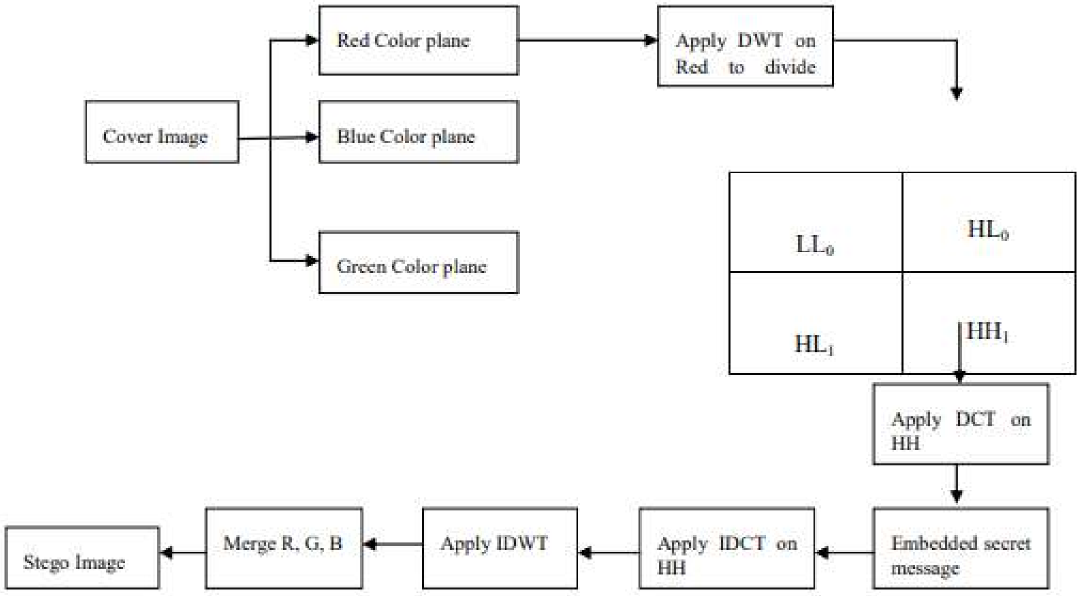

Figure 1: Message Encoding can be done with DCT and DWT.

The sender and the receiver will use the DCT with DWT method to safely send the secret message without the eavesdropper being able to hack, decipher, or change the stego image or the message itself. This is shown in Figure 3.1. Using DCT and DWT, the sender and receiver can send and receive a secret message without being caught. The goal of the Sender is to get a private message to the right person. The goal of the Attacker is to intercept, decode, and change the message for the Attacker's own purposes. So that the Attacker's plans don't work out, and so that the Attacker can't even tell the stego image from the others. After a discrete wavelet transform (DWT) splits the cover image into four bands, DCT is used on the HH band (LL0, HL0, HL1, and HH1). The sender then sends the stego image to the recipient. To decode the image, the recipient uses a DWT and DCT extraction method. The sender then sends the stego image to the other person.

3.2 Cosine Transform in Continuous and Uniform Domains (DCT)

For each colour channel in a JPEG file, the discrete cosine transform is used. With this method, the image is changed into 64 DCT coefficients for each 88 block of pixels in order. It can be shown that the DCT coefficients F(u,v) of an 8x8-pixel image block take the form f. (x, y).

$$f(u,v) = \frac{1}{4} C(i)C(j) \sum_{x=0}^{7} \sum_{y=0}^{7} p(x,y) \cos[\frac{(2x+1)u\Pi}{16}] \cos[\frac{(2x+1)v\Pi}{16}].$$

Where,

P stands for the pixel in the image at the coordinates (x, y) that the matrix p represents (x,y).

N shows how big the block is that is used to figure out the DCT.

The DCT uses the cosine function to make a matrix that is sensitive to changes in the frequency of the horizontal, diagonal, and vertical directions. The values of pixels are used to figure out one new entry (i,jth) in the image that has been changed.

Using the DCT method, the following is the algorithm for adding the text message:

a. Taking apart the relevant picture:

Based on how the cover image is read, the picture is broken up into 8x8 pixel squares

b. Make each Block work with DCT by doing the following:

Here, we take the image block out of each of the 128 records. This is because the DCT method only works with pixel values between -128 and 127, so this is the only range it can handle. The DCT, which is found by multiplying the two matrices together, is then applied to the new matrix.

D=TMT’

We can get the DCT matrix T by working out the following equation:

$$T_{i,j=}\left\{\begin{array}{l} 1/\sqrt{N}\ \text{if}\ i{=}0 \\ \sqrt{(\frac{1}{N})}\cos\left[\frac{(2j+1)i\Pi}{2N}\right]\ \text{If}\ i{>}0 \end{array}\right\}$$

3.3 DWT stands for "discrete wavelet transform" (DWT)

Wavelets are a specific type of function that are used to represent signals (much like the sin and cosine functions are in Fourier analysis). We used the Haar-DWT, which is the simplest member of the DWT family of transforms, for this. In Haar-DWT, the low frequency wavelet coefficient is made by taking the difference in value between two pixels and taking the mean. The high frequency wavelet coefficient is made by dividing by two the difference between two pixels that are the same.

Separating two-dimensional images into their horizontal (HL), vertical (LH), and diagonal (HH) components is a valuable use of the Discrete Wavelet Transform (DWT) method. The latter three band photos all have a lower resolution than the first three (LL).

LL_0	HL_0
HL_1	HH_1

Figure 2: The Discrete Wavelet Transform in Two Dimensions, with One Level

Significant parts (smooth areas) of the spatial domain image are in the DWT's approximation band of low frequency wavelet coefficients. Edge and texture features are often in higher frequency sub bands like HH, HL, and LH. This is because the DWT shows the image as a set of wavelet coefficients.

Here's what you need to do to use DWT to add the secret message:

1. If the image is in colour, the first step is to get the cover art and divide it into red, green, and blue planes.
2. Then the Haar DWT on the red plane and divide the resulting spectrum into four sub bands.
3. Then, you have to figure out the LSB of the HH sub band.
4. After that, the secret message is turned into binary, and the least significant bits (LSBs) of the sub band that was chosen before are changed to include parts of the secret message that was turned into binary.
5. Use IDWT on the embedded data, and then put the planes together to make the stego image.

3.3.1 Dual-Color and Dual-Waveform Transforms

This method combines the DCT and DWT techniques into a single, simpler process. Using discrete wavelet transform (DWT), this method divides the red part of the cover image into four sub bands. We separate the signal into its low frequency and high frequency parts using discrete wavelet transform (DWT). DCT can only be used in the HH band because that's where the information about the edge component is. Since the human visual system is less sensitive to edge changes than it is to changes in lower frequency components, high frequency components are used more often. As a summary of the algorithm, the following is given:

1. First, we take a picture of the cover and split it into three layers, each with a different colour.
2. Second, use discrete wavelet transform (DWT) in the red plane and divide the bands into four subsets.
3. The last step is to use the DCT on the HH band in the red window.
4. Fourth, the secret message is turned into binary, and the least important bits are used to replace the unused bits in the DCT coefficients of the sub band that was chosen earlier (LSB).
5. Do something different from what everyone else is doing. A discrete cosine transform for the HH subband
6. Seven, after the bits of the secret message have been encoded in the red plane, the plane must be recovered using an inverse wavelet transformation.
7. The colour steganographic image is made by putting all the planes together.

Here, on the other hand, the DC coefficient of the HH sub band is used to hide an LSB-encoded hidden message bit. The 2D series of random numbers is broken up into a few high-frequency subsets in a random way.

4. Results analysis

The maximum signal-to-noise ratio is measured and looked at to see how well the proposed method works. the signal-to-noise ratio that is the best it can be (PSNR) The MSE and PSNR values show how good the stego image is compared to the original. If the MSE value is low and the PSNR value is high, the quality is good. The PSNR metric is used to figure out how good an image is. Most of the time, a high PSNR score means that a good image has been reconstructed. If the number of pixels or samples in both images is 8, then their PSNR is the same. A positive peak-to-sideband signal-to-noise ratio (PSNR) is a logarithmic (ten) ratio of the maximum signal-to-noise ratio (Max2) to the maximum signal error. MAX2 is the highest value of a pixel in the original image. To figure out the mean square error, you can just use the notation MSE. Steganography is not meant to be used instead of cryptography. Instead, it is meant to work with cryptography in some way. If the secret message is encrypted and hidden using steganography, it is less likely that it will be found by someone who isn't supposed to. People who work in fields like intelligence and covert operations may know what steganography is, but the rest of the world is just now learning about it.

Most of the time, the current generation of computer systems isn't strong enough to keep embedded data from being found and removed. As more and more people use benchmarking strategies, there is a pressing need for a better standard definition. During their research, the researchers found that a lot of work had already been done on audio steganography. Text, video, photos, and audio can all be hidden in an audio file, and audio can also be used as a cover file and a hidden message. However, there has been no progress in encrypting photos.

We used ciphertext images for this attempt at audio steganography, which we did (encrypted using DCT). Most of the shots have a PSNR of 40 or higher, which means that very little information has been lost.

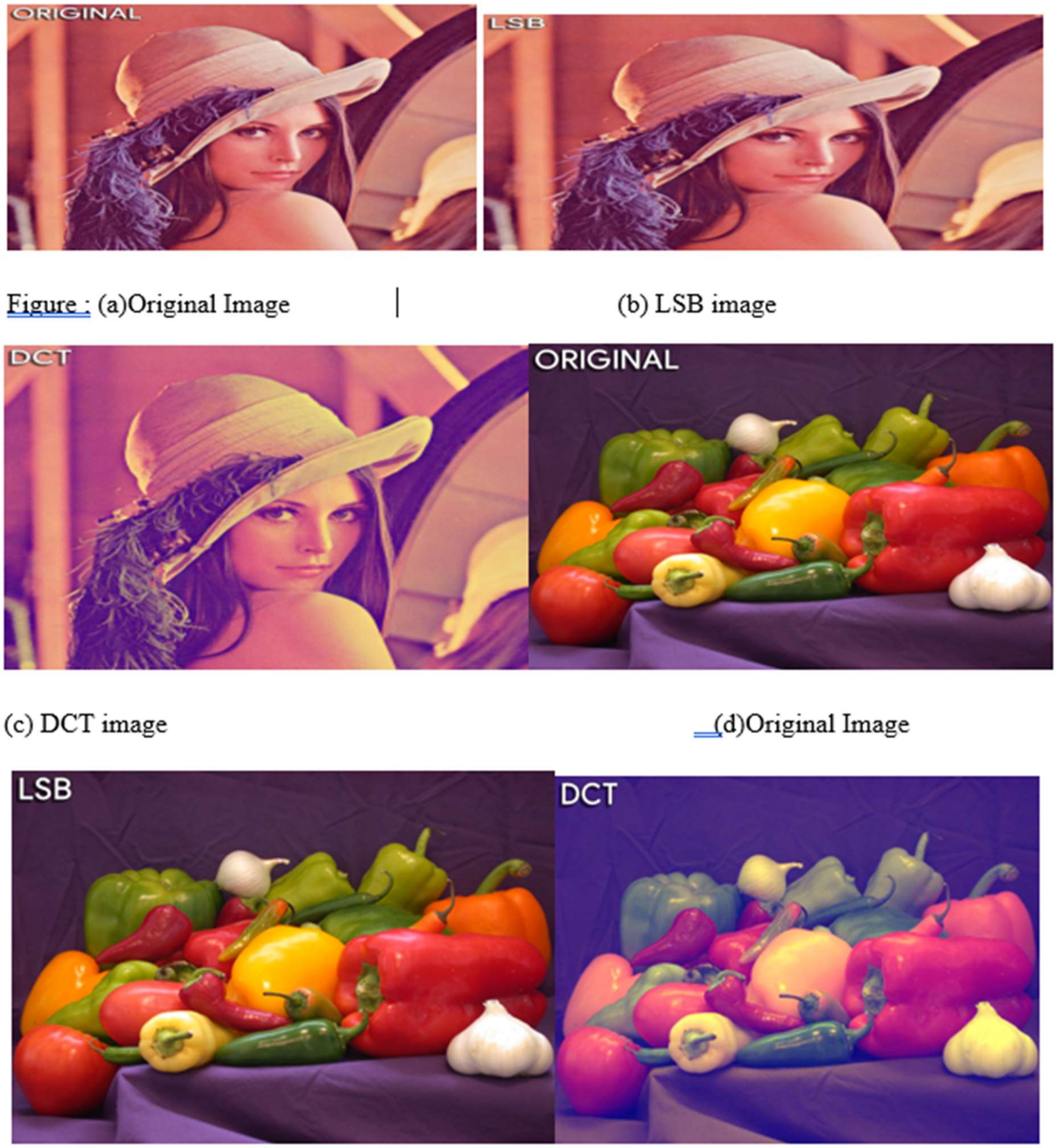

Figure : (a)Original Image | (b) LSB image

(c) DCT image (d)Original Image

(e)LSB Image (b)DCT image

4. Conclusion

In this study, we use a high-capacity data hiding method to hide credit card numbers in images. However, the nature of the data hiding method makes it hard for us to do this. Data embedding already gives some level of security, but a reliable way to scramble and un-scramble the data has been made to make it even safer. The main part of this method is an MK randomise key generator. There are three different kinds of security at work here. First, the original data is scrambled. Then, it is scrambled again with keys made by an M-K randomise key generator. Finally, the DCT coefficients are embedded. DWT-based steganography lets the coefficients in the low frequency sub-band stay the same so that the image quality is better. Because the DWT coefficients in different subbands have different properties, this is what happens. PSNR is recommended because the hidden messages won't affect the most important part of the image, which is the low frequency content, if they are put in the high frequency sub bands that correspond to the edges of the original image. The PSNR, MSR, Correlation, Processing time, Capacity, and Embedding estimations are used to measure how well different DCT and DWT methods work and to compare them to each other. The proposed Method is very useful for LOGO image files and most mobile bank transactions that happen over the internet.

Reference

1. Er. Harjinder Kaur Sidhu , GURU KASHI UNIVERSITY,TALWANDI SABO,BATHINDA; C.Er. Harisharan Aggarwal, GURU KASHI UNIVERSITY,TALWANDI SABO,BATHINDA "Review of Increasing Image Compression Rate Using (DWT+DCT) and Steganography." International Journal of Recent Trends in Engineering and Research, vol. 3, no. 6, 13 June 2017, pp. 67–72, https://doi.org/10.23883/ijrter.2017.3276.lw9sc. Accessed 14 Oct. 2019.
2. Laxmi Gulappagol, K.B.ShivaKumar. Secured Video Steganography in DWT-DCT Domains Based on Multiple Object Tracking using H.264 Algorithm. International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, Volume-7 Issue-6S2, April 2019.
3. T. Yuvaraja M.E., C. Soundarya Devi, S. Sushmitha, P. Uvarani, S. Kaviya, 2018, DCT & DWT Based Secured Image Transmission Using Steganography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ETCAN – 2018 (Volume 6 – Issue 05).
4. Eyssa, A.A., Abdelsamie, F.E. & Abdelnaiem, A.E. An Efficient Image Steganography Approach over Wireless Communication System. Wireless Pers Commun 110, 321–337 (2020). https://doi.org/10.1007/s11277-019-06730-2.
5. Hasan N, Islam MS, Chen W, Kabir MA, Al-Ahmadi S. Encryption Based Image Watermarking Algorithm in 2DWT-DCT Domains. Sensors (Basel). 2021 Aug 17;21(16):5540. doi: 10.3390/s21165540. PMID: 34450982; PMCID: PMC8402257.
6. Goswami, Anuradha, and Sarika Khandelwal. "Coloured and Gray Scale Image Steganography Using Block Level DWT DCT Transformation." International Journal of Computer Applications, vol. 148, no. 7, 16 Aug. 2016, pp. 1–3, https://doi.org/10.5120/ijca2016911205. Accessed 18 Jan. 2022.
7. Mstafa, Ramadhan J., et al. "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC." IEEE Access, 2017, pp. 1–1, https://doi.org/10.1109/access.2017.2691581. Accessed 12 Apr. 2021.
8. "Image Steganography Using Dct and Dwt." International Journal of Latest Trends in Engineering & Technology, vol. 7, no. 1, 2016, https://doi.org/10.21172/1.71.106. Accessed 29 Aug. 2019.

9. R, Rajalakshmi. “A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC.” International Journal for Research in Applied Science and Engineering Technology, vol. 6, no. 4, 30 Apr. 2018, pp. 531–537, https://doi.org/10.22214/ijraset.2018.4093. Accessed 15 Sept. 2022.
10. Singla, Tamanna, and Ashwani Sethi. “Steganography: A Juxtaposition between LSB DCT, DWT.” International Journal of Computer Applications, vol. 126, no. 11, 17 Sept. 2015, pp. 6–10, https://doi.org/10.5120/ijca2015906215. Accessed 21 Mar. 2020.
11. Mohammed, Nadia. “Chaotic Image Steganography Using DCT and DWT.” AL-Rafidain Journal of Computer Sciences and Mathematics, vol. 10, no. 3, 1 Sept. 2013, pp. 61–73, https://doi.org/10.33899/csmj.2013.163536. Accessed 9 Feb. 2023.
12. SureshSingh, N., and G. Suganthi. “High Secured and Authenticated Secret Message Sending Using TIRI-DCT-DWT Based Iris Recognition and Steganography.” International Journal of Computer Applications, vol. 70, no. 8, 17 May 2013, pp. 26–30, https://doi.org/10.5120/11983-7858.
13. “Robust and Reversible Image Watermarking Scheme Using Combined DCT-DWT-SVD Transforms.” Journal of Information Processing Systems, June 2015, https://doi.org/10.3745/jips.02.0021.
14. Vasudha. “ROBUST IMAGE STEGNOGRAPHY USING DWT and DCT.” International Journal of Research in Engineering and Technology, vol. 05, no. 16, 25 May 2016, pp. 363–367, https://doi.org/10.15623/ijret.2016.0516080.
15. Mstafa, Ramadhan J., and Khaled M. Elleithy. “An ECC/DCT-Based Robust Video Steganography Algorithm for Secure Data Communication.” Journal of Cyber Security and Mobility, 9 May 2017, https://doi.org/10.13052/2245-1439.531.
16. Sari, Wellia Shinta, et al. “A Good Performance OTP Encryption Image Based on DCT-DWT Steganography.” TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 15, no. 4, 1 Dec. 2017, p. 1987, https://doi.org/10.12928/telkomnika.v15i4.5883.
17. Abadi, Roxana Yahya, and Payman Moallem. “Robust and Optimum Color Image Watermarking Method Based on a Combination of DWT and DCT.” Optik, vol. 261, July 2022, p. 169146, https://doi.org/10.1016/j.ijleo.2022.169146.
18. Du, Guest Editor Jianping. “A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DCT Encrypted Domain.” International Journal of Simulation: Systems, Science & Technology, 1 Jan. 2016, https://doi.org/10.5013/ijssst.a.17.43.34.
19. M., A., et al. “Improved BEMD-DWT-DCT-SVD Robust Watermarking Technique for Still Images.” International Journal of Computer Applications, vol. 150, no. 9, 15 Sept. 2016, pp. 13–20, https://doi.org/10.5120/ijca2016911620.
20. Faza, Aditya Mahmud, et al. “Analisis Kinerja Kompresi Citra Digital Dengan Komparasi DWT, DCT Dan Hybrid (DWT-DCT).” Jurnal Online Informatika, vol. 1, no. 1, 1 June 2016, p. 1, https://doi.org/10.15575/join.v1i1.3.
21. Bajracharya, Subin, and Roshan Koju. "An improved DWT-SVD based robust digital image watermarking for color image." International Journal Engineering and Manufacturing1 (2017): 49-59.

22. Fan, P., Zhang, H. & Zhao, X. Robust video steganography for social media sharing based on principal component analysis. EURASIP J. on Info. Security 2022, 4 (2022). https://doi.org/10.1186/s13635-022-00130-z