Advances in Applied Sciences
2022; 7(2): 27-32
http://www.sciencepublishinggroup.com/j/aas
doi: 10.11648/j.aas.20220702.12
ISSN: 2575-2065 (Print); ISSN: 2575-1514 (Online)

Signal Steganography Using Different Wavelets and Their Comparisons

Shemanta Kumar Biswas[1], Redwanul Islam[2], Md. Rafiqul Islam[1, *]

[1]Mathematics Discipline, Khulna University, Khulna, Bangladesh

[2]Department of Biomedical Engineering, Khulna University of Engineering & Technology, Khulna, Bangladesh

Email address:

mrislam_66@ku.ac.bd (Md. R. Islam), simantabiswasku@gmail.com (S. K. Biswas), redwanul10@gmail.com (R. Islam)

[*]Corresponding author

To cite this article:

Shemanta Kumar Biswas, Redwanul Islam, Md. Rafiqul Islam. Signal Steganography Using Different Wavelets and Their Comparisons. *Advances in Applied Sciences*. Vol. 7, No. 2, 2022, pp. 27-32. doi: 10.11648/j.aas.20220702.12

Received: May 9, 2022; **Accepted**: May 25, 2022; **Published**: June 30, 2022

Abstract: The process of inserting secret data in any media as pictures, audio, video, text and protocol, also it can be empathy this secret connection is called steganography. At present, the widespread use of internet applications has become a security risk. Steganography is used to overcome this undesirable situation. It shows a significant character in maintaining privacy. Some steganographic techniques modify the image using the spatial domain, transform domain, spread spectrum, statistical method and distortion techniques. This work aims to develop efficient data encryption and decryption technique that provide security of data. In this research exertion, it anticipated an image steganalysis method using various wavelet decomposition, especially using multiwavelet decomposition. First, we decomposed the image using different wavelets and multiwavelets. Then we extracted the more informative parts into wavelet sub-bands as a feature and inserted them into the LL sub-band wavelet decomposed image. The resulting image is sent to the recipient as a signal. The recipient retrieves confidential information through encryption. Finally, by analyzing the actions of different wavelets, we can retrieve the original message through the decryption technique. The multiwavelet technique achieves PSNR of 48.26 - 56.5926 and MSE of 0.1428 - 0.97. The result indicates that multiwavelet provided a good recovery of the secret image quality that led to an increase in the imperceptibility of the system.

Keywords: Decryption, Encryption, Wavelet and Multiwavelet Decomposition, Steganography

1. Introduction

The demand for digital communication has risen dramatically in recent years, and as a result, the Internet has essentially become a method of more effective and faster prime messages. According to Statista, Internet users increased day by day all over the world. Instantaneously, data over Internet has become vulnerable to copyright infringement, espionage, and piracy, necessitating private communication. As a result, data hiding, a new domain dedicated to information security, has emerged. Steganography is a relatively new addition to the field of data concealment, yet it has a lengthy history. Steganography is the use of a standard such as an image, audio, audiovisual, or script file to pelt information so that it does not attract attention and appears to be an innocuous medium. Many techniques have been developed to hide data in photos over the years, and inventing new algorithms is an active research issue. Spatial field methods, frequency field methods, and adaptive methods are the three basic types of steganographic methods. Because it is considered a special case, the last one can be used in both the previous two cases. In the work, Roy et al. [8] discussed host image, stego-image, stego-key and inserting domain as terminologies that are normally used in picture steganography systems. Pawar and Kakde [7] said that Secrecy (known only by the sender and receiver), Imperceptibility (indistinguishable from the original) and High Capability is the key compensations of steganography (Depends on the size of the signal). There are some drawbacks to this as well. Once the algorithm is understood, the information's confidentiality is destroyed. Hackers may take advantage of the technology. The original signal may not be recovered due to distortion. To overcome this drawback, here we used wavelet and multiwavelet transform.

2. Literature Review

In this sector, we will offer an indication of what has been used in previous research work to abstract the most commonly used techniques and methodologies, while the following literature surveys will be drawn from well-known published works that will describe previous research and development on the digital steganography method. The strategy taken by Serdean et al. [11] aims to compare the performance of wavelet coefficients and multiwavelet field watermarking against various assaults on a like-for-like basis. The focus of the research is on balanced multiwavelets. Hemalatha et al. [2] used Discrete Wavelet Transform (DWT) and Integer Wavelet Transform to build a novel picture steganography technique to disguise both the secret image and the key in a color host image. Abdulla et al. [1], approached the Spatial Domain Algorithm in their work and demonstrated that it is costly but not safe. Yuan et al. [13] employed Location Sensitive Inserting and explored Algorithms in Domain (Spatial) in their research. Sidhik et al. [9] suggested a simple technique for high-capability Steganography that only works with color images. The formula was primarily employed to enable independent rippling remodels, with rippling fusion being used for color picture Steganography. Instead of using DWT, DCT, and SVD separately or in a DWT-SVD / DCT-SVD combination, Singh [12] envisioned a remanufacture study combination of multiple retouching detection methods based on the fusion of separate riffle transforms (DWT), distinct trigonometric function transforms (DCT), and singular worth decomposition (SVD). Hussain et al. [3] discuss Algorithms that provide a secure and scalable method of transformation. Because no secret keys are utilized, messages are easily deciphered. Jeevitha et al. [10] developed an entirely new image steganography method based on the HMT (Hidden Mathematician Tree) and Contourlet rebuild. Contourlet transform was performed in two steps in HMT: low (LL band) and high variation (HL band). Murugan et al. [5] developed a method of steganography and show the performance of different wavelets. According to their paper, the Haar wavelet gives a more secure transmission ability Zhang et al., [15] have been working using DCT and transform (Contourlet). This approach is effective, adaptable, and has a good generalization capacity for detecting grayscale and color image splicing.

This paper proposes to find different ways for signal steganography using different wavelet transforms especially using multiwavelet. Initially collecting different signals, we will try to find a new way in the frequency domain for signal steganography. And we will finally compare the performance of different wavelet transformers. This work will be done by MATLAB software.

3. Multiwavelet Transforms

The wavelet transform and the multiwavelet transform are extremely similar. Because the wavelet transform uses only one fractal dimension and wavelet function, it is also known as the scalar wavelet transform. There are multiple scaling functions and wavelet functions in a multiwavelet transform discussed by Lin and Liu [4]. Vectors are used to organize the scaling and wavelet functions. The variety of the transform is determined by the number of certain functions that are combined. For notational convenience, Multiwavelet transforms with multiplicity can be written using a vector notation, the set of scaling functions and wavelet functions. If it forms a scalar wavelet transform then, it becomes Multiwavelet Transform. To date, Multiwavelet transforms of multiplicity have been studied. The Multiwavelet transform, like the linear wavelet transform, has such a sequence of dilation equations that produce the high- and low filter coefficients. Two low pass filters and two high pass filters are used in the Multiwavelet transform with multiplicity two.

The concept of the Multiwavelet comes from the generalization of scalar wavelets. Multiple scaling functions and wavelets are utilized instead of one scaling function and one wavelet. As a result, there is more flexibility in building wavelets.

4. Methodology

The main problem of secret signal hiding in another host signal is a large amount of data that requires a special data inserting technique to obtain enough capacity, transparency and robustness. Our proposed Steganography system, which embeds (RGB) secret image inside (RGB) host image chosen manually, applies a discrete wavelet transform (DWT) in the inserting process to achieve a robust and multilayer security system with high invisibility. Here, we used different wavelet transformations for the host and the secret image, where the host image and secret mage will be decomposed into different levels. Each level of disintegration yields four sub-bands of coefficients.

The proposed system consists of three main phases: the Preinserting phase, inserting phase and reconstruction phase.

4.1. Pre-inserting Stage

The inserting phase is proceeded by three main stages: secret image selection and processing stage, host image selection and processing stage and creating singular value decomposition matrix stage.

4.2. Inserting Phase

Once the results coming out of the pre-inserting stages are ready, the inserting phase can take place.

Step-1: Get a color layer of the host image and the same color layer of the secret image.

Step-2: Perform n-level DWT on the host image.

Step-3: Select sub-band to make reference singular value.

Step-4: Perform n-level discrete wavelet decomposition on the secret image.

Step-5: Perform Singular Value Decomposition (SVD) on both the reference and secret singular value.

Step-6: Modify the singular values of reference or host image with the singular values of the secret image by adding both the singular values using watermark strength.

Step-7: Obtain modified reference singular value by merging left singular values, diagonal elements and right singular values.

Step-8: Perform n-level inverse discrete wavelet decomposition to get the stego-image.

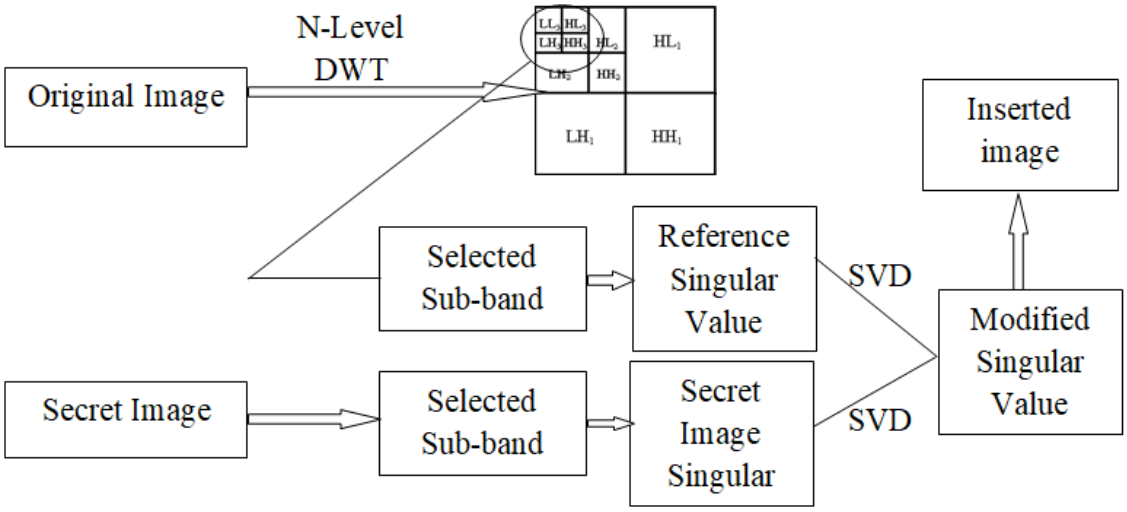

Figure 1. *Inserting algorithm flow diagram.*

4.3. Reconstruction Phase

Once the stego-image is received by the receiver side, it is processed to extract the secret image. The reconstruction process is given below:

Step-1: Split the stego-image into R, G and B color layers.

Step-2: Get a color layer of stego-image.

Step-3: Perform n-level discrete wavelet decomposition on the stego-image using different Mother Wavelets.

Step-4: Using sub-band select the stego-image reference singular value.

Step-5: Perform Singular Value Decomposition (SVD) transform on both original reference and stego-image reference singular value.

Step-6: Extract the singular values of the stego-image by subtracting the diagonal value of the host image from the diagonal value of watermarked image and dividing by the watermark strength.

Step-7: Obtain the estimate of the stego-image by using the extracted singular value with the left and right singular values of the secret image.

Step-8: Apply the Inverse Discrete Wavelet Transform (IDWT) to get the color layers of the recovered secret image.

Step-9: Repeat steps (2) to (8) to get the rest color layers of the recovered secret image.

Step-10: Combine the color layers coming from step (9) to get the full color (RGB) recovered in the secret image.

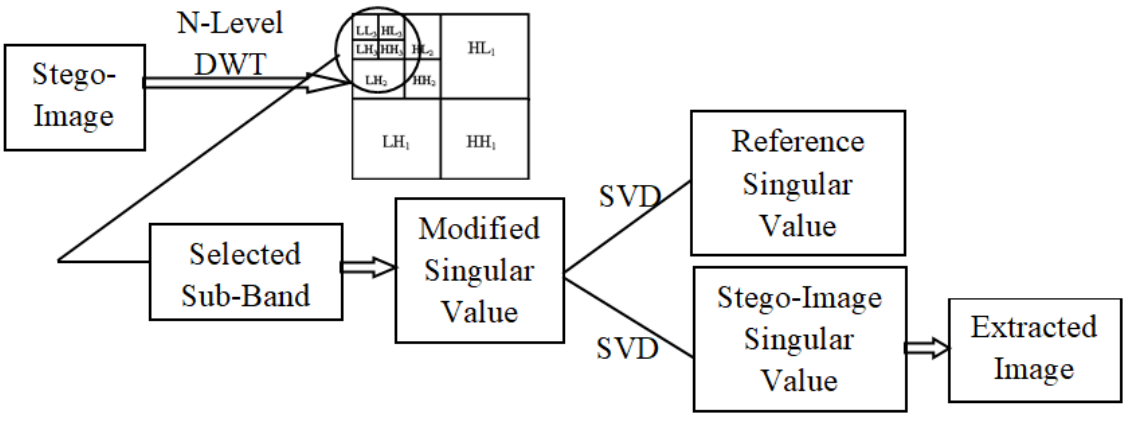

Figure 2. *Reconstruction algorithm flow diagram.*

5. Results and Discussion

We performed our experiment for six different wavelets on the host image and secret image. Using MATLAB wavelet toolbox for each case we tabulate the PSNR and MSE values.

Table 1. *PSNR and MSE values for the Stego-image.*

	Map+Doraemon		Bird+Garden		F-16+Baboon	
	PSNR	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
Haar	53.4665	0.2927	52.3539	0.3777	54.1081	0.2525
Daubechies	53.4414	0.2944	52.3398	0.3794	54.0790	0.2542
Coiflets	53.4003	0.2972	52.2615	0.3863	53.9627	0.2611
Symlets	53.4414	0.2944	52.1835	0.3933	53.8478	0.2681
Discrete Meyer	53.4149	0.2962	52.1637	0.3951	53.8171	0.2700
Multiwavelet	53.6375	0.2814	52.5329	0.3629	54.3705	0.2377

To highlight the important characteristics of our proposed system, a histograms comparison between the resulted stego-image and the host-image is presented in the following figures. The histogram test shows that the modified image (stego-image) is not affected by the hidden image. The histogram of the host image is approximately the same as the histogram of the resulted stego-image as shown in the cases below. Here different discrete wavelet transform has been used with 512*512 secret images, host images and stego-images. Figure 3 shows the secret images and the corresponding host images which are used to test our proposed system.

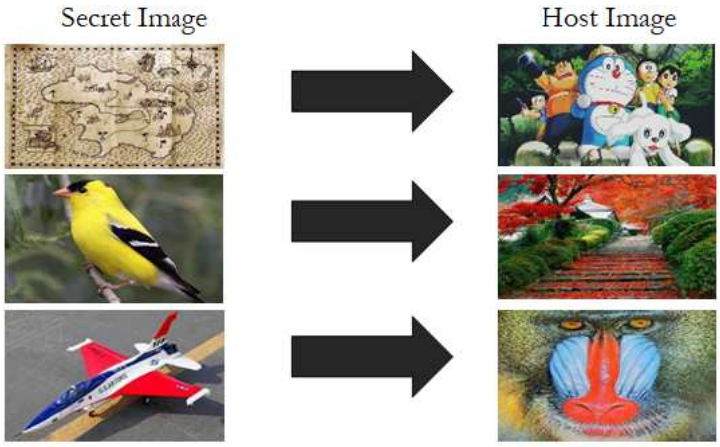

Figure 3. *The selected secret and host images.*

Table 2. *PSNR and MSE values for the Reconstructed-image.*

	Map+Doraemon		Bird+Garden		F-16+Baboon	
	PSNR	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
Haar	51.6824	0.4414	48.3207	0.9572	56.5081	0.1453
Daubechies	51.7830	0.4313	48.2751	0.9673	56.2162	0.1554
Coiflets	51.7830	0.4313	48.2711	0.9682	56.1912	0.1563
Symlets	51.7830	0.4313	48.2639	0.9698	56.1469	0.1579
Discrete Meyer	51.8295	0.4267	48.2434	0.9744	56.0222	0.1625
Multiwavelet	52.0316	0.4073	48.3334	0.9544	56.5926	0.1428

In our experiment, we used Haar, Daubechies, Coiflet, Symlet, Discrete Meyer and Multiwavelet transformation. The results on different wavelets for each stego-images and reconstructed images are shown in Table 1 and Table 2 respectively.

Figure 4 shows hiding secret images inside host images with their histogram by using Multiwavelet transformation.

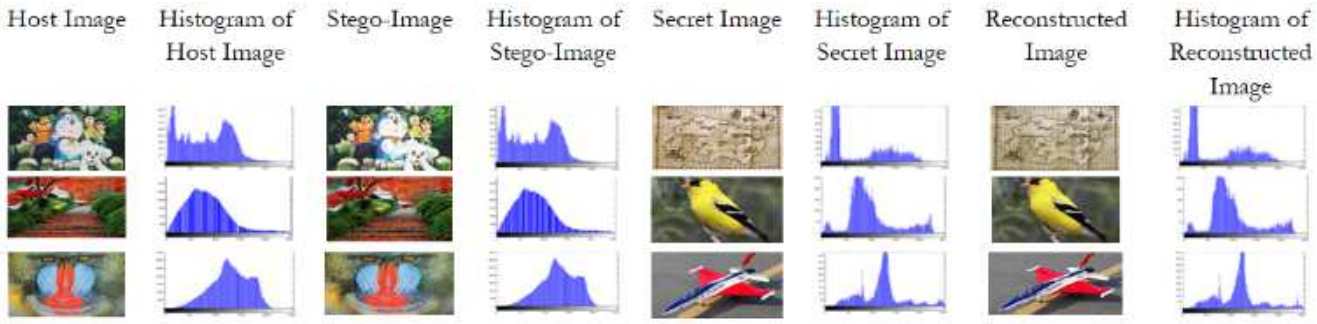

Figure 4. *Stego-Images and Reconstructed Images with their Histogram.*

As shown in Figure 4, the histogram of both host and stego-images are almost similar as well as for secret images and reconstructed images.

We know from the theoretical aspect that the higher PSNR value and least MSE value show the perfectness of the reconstruction image. From Figure 5 and Figure 6 it is clear that multiwavelet transformation has the least MSE values and more PSNR values in all our tested cases. Therefore, we can conclude that multiwavelet transform produces more secure signals than any other wavelet in the steganography concept.

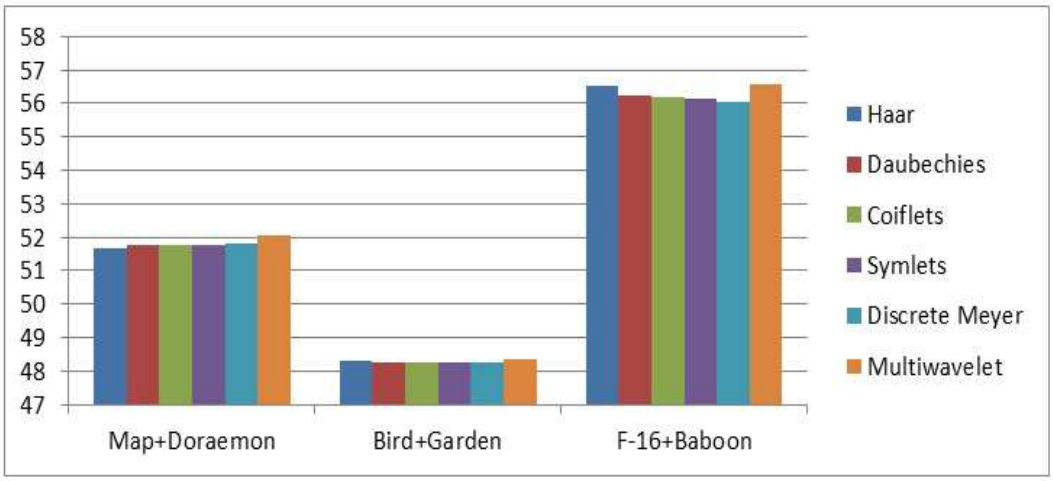

Figure 5. *In the bar diagram PSNR values for reconstructed images using different wavelets.*

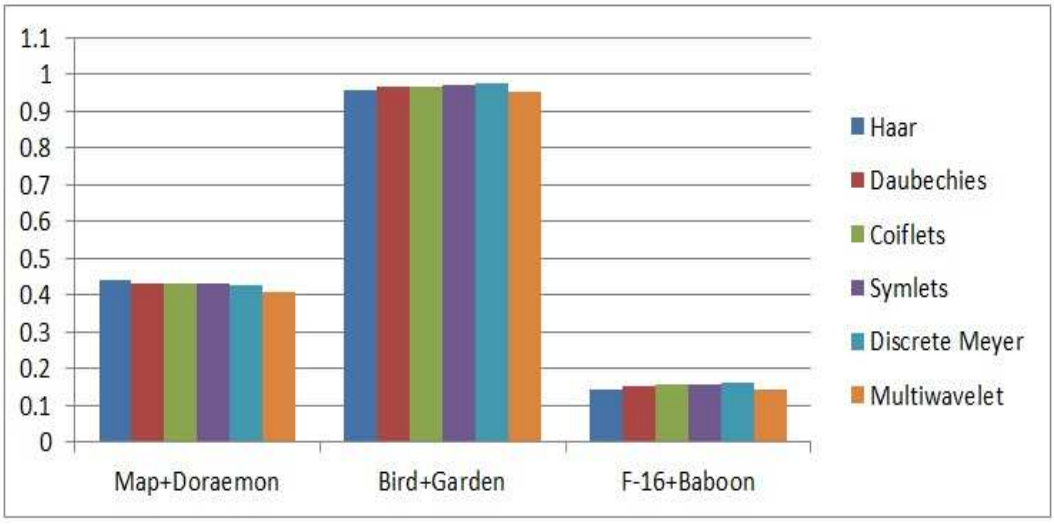

Figure 6. *In the bar diagram MSE values for reconstructed images using different wavelets.*

In Table 3, we compared our work with existing similar work performed by Parul et al. [6], Murugan et al. [5], etc. In this work, we have taken different images but considered the same pixel size as the literature mentioned.

Table 3. *Comparison of proposed work with existing work for reconstructed image for F-16+Baboon.*

Work	Image	PSNR (dB)	MSE
DWT Parul et al. [6]	RGB Image (512*512)	47.9144	-
DWT+Fusion Factor Murugan et al. [5]	RGB Image (512*512)	53.3530	0.300
DWT & IDWT Nipanikar et al. [14]	RGB Image (512*512)	47.65	0.75
DWT Proposed Work	RGB Image (512*512)	56.5081	0.1453
Multiwavelet Proposed Work	RGB Image (512*512)	56.5926	0.1428

Wavelet transformation performs better in signal steganography because it divided data into frequency components, which partitions the high frequency and low-frequency information. In signal steganography, different DWT was studied previously. In this work, multiwavelet is used in signal steganography which performs better than

different wavelet transformations.

6. Conclusion

The main purpose of steganography is to create messages in such a manner that the messages when retrieved by the receiver without loss and robustness. The finest steganography system should have supreme inserting ability, great reliability, high invisibility and decent safety level. Discrete wavelet transform has solved those problems. In this work, splitting the surreptitious and host images into (R, G, B) color layers and different wavelet decomposition led to high perceptual quality in both inserting and recovered phases. Our system provided a good recovery of the secret image quality which led to an increase in the imperceptibility of the system. The PSNR and MSE values found in our work are between 48.26-56.59 dB and 0.14-0.97 respectively which are better than previously reported work. The histogram similarity of stego and host images proves the high robustness and security of the system against attackers. So, our system is the potential to give security to any other data transfer technique.

References

[1] Abdulla, A. A., Sellahewa, H. and Jassim, S. A., (2014) "Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping," in *Security Standardisation Research*. Cham: Springer International Publishing, pp. 151–166. DOI: 10.1007/978-3-319-14054-4_10.

[2] Hemalatha, S., Acharya, U. D. and Renuka, A., (2013) "A Secure Color Image Steganography in Transform Domain," International Journal on Cryptography and Information Security, 3 (1), pp. 17–24. arXiv preprint arXiv: 1307.3026.

[3] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. and Jung, K. H., (2018) "Image steganography in spatial domain: A survey," Signal processing. Image communication, 65, pp. 46–66. DOI: 10.1016/j.image.2018.03.012.

[4] Lin, G. and Liu, Z. M., (2000) "The application of multiwavelet transform to image coding," IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, 9 (2), pp. 270–273. DOI: 10.1109/83.821740.

[5] Murugan, G. V. K. and Uthandipalayam Subramaniyam, R., (2020) "Performance analysis of image steganography using wavelet transform for safe and secured transaction," Multimedia tools and applications, 79 (13–14), pp. 9101–9115. DOI: 10.1007/s11042-019-7507-6.

[6] Parul, M. and Rohil, H. (2014) "Optimized Image Steganography using Discrete Wavelet Transform (DWT)," International Journal of Recent Development in Engineering and Technology (IJRDET), 2 (2), pp. 75–81.

[7] Pawar, S. S. and Kakde, V. (2014) "Review on Steganography for Hiding Data," International Journal of Computer Science and Mobile Computing, 3 (4), pp. 225–229.

[8] Roy, R. et al. (2013) "Evaluating Image Steganography Techniques: Future Research Challenges, International Conference on Computing Management and Telecommunications," pp. 309–314. doi: 10.1109/ComManTel.2013.6482411.

[9] Sidhik, S., Sudheer, S. K. and Mahadhevan Pillai, V. P. (2015) "Performance and analysis of high capacity Steganography of color images involving Wavelet Transform," Optik, 126 (23), pp. 3755–3760. DOI: 10.1016/j.ijleo.2015.08.208.

[10] Jeevitha, S. and Amutha Prabha, N. (2020) "Effective payload and improved security using HMT Contourlet transform in medical image steganography," Health and technology, 10 (1), pp. 217–229. DOI: 10.1007/s12553-018-00285-1.

[11] Serdean, C. V., Ibrahim, M. K., Moemeni, A. and Al-Akaidi, M. M., (2007) "Wavelet and multiwavelet watermarking," IET image processing, 1 (2), p. 223. DOI: 10.1049/iet-ipr:20060214.

[12] Singh, A. K. (2017) "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," Multimedia tools and applications, 76 (6), pp. 8881–8900. DOI: 10.1007/s11042-016-3514-z.

[13] Yuan, H. D., (2014) "Secret sharing with multi-host adaptive steganography," Information Sciences, 254, pp. 197–212. DOI: 10.1016/j.ins.2013.08.012.

[14] Nipanikar, S. I., Hima Deepthi, V. and Kulkarni, N. (2018) "A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform," *Alexandria Engineering Journal*, 57 (4), pp. 2343–2356. doi: 10.1016/j.aej.2017.09.005.

[15] Zhang, Q. and Lu, W. (2016) "Joint Image Splicing Detection in DCT and Contourlet Transform Domain," *Journal of Visual Communication and Image Representation,* 40, pp. 449–458.