International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

A Novel Technique for Enhancing Data Security Using Hybrid Coding in Medical Images

Anant Shankar Ellapalli
Research Scholar, Dept. of ECE, S V University College of Engineering,
S V University,
Tirupati-517502, India
anant.shankar16@gmail.com

Dr.S.Varadarajan
Professor, Dept. of ECE, S V University College of Engineering,
S V University,
Tirupati-517502, India
varadasouri@gmail.com

Abstract— The Internet's rapid development in data transmission has made it simpler to convey data quickly and accurately to the intended recipient. Data is one of the most essential assets to be protected during Internet transmission, thus it is necessary to handle the rising danger of security. Through hacking, unauthorized person can alter or misuse the crucial data. Therefore, security is a primary problem that requiring attention. Compression and encryption are frequently used to share and save images respectively. The effectiveness of digital image services depends on how the two activities are performed. Medical images play a significant role in the modern healthcare system because they are utilized to preserve patient data including illness diagnoses and other pertinent details. Thus, data must be maintained in a secure manner. To deliver data safely and unchanged to the target place, a variety of techniques, including cryptography and steganography are utilized to solve security difficulty, several research and exercises were done to produce a range of tactics and algorithms. In this paper, a technique for concealing the secret image is proposed.

Keywords- Steganography, cryptography, Encryption, decryption, Compression, Secured data transmission.

I. INTRODUCTION

A fast and correct diagnosis is essential for saving lives in the medical field. Examples of imaging methods used in diagnosis include MR imaging (MRI), x - rays, sonography, nucleology, mechanical imaging, infrared thermography (IRT), optoacoustic imaging and (EEG).The health care system is significantly reliant on the medical business, especially when it comes to distant collaboration, biomedical research, and diagnostic procedures. It monitors people's health and provides clinicians with the resources they require to treat patients effectively. Medical equipment and patient record management systems are being rapidly improved as computing technology advances. It might be difficult to transmit images via the internet. Encryption is a technique that may be used for secure transmission. The picture is safeguarded and the communication path is more efficiently exploited when cryptography is used.

Digital watermarking, steganography, and cryptography are just a few techniques that have been used to protect telemedicine applications. After being transformed via cryptography, the medical information can only be viewed by those who have the required authority to preserve confidentiality and provide authenticity. These Images are huge, thus transmitting them in their original form requires a lot of bandwidth and storage space. With this technique, a message is subtly added to the data. Image compression may be done in a few different ways. Image size reduction often involves using the image compression method, which has no effect on image quality. Figure 1 depicts the basic steganography procedure.

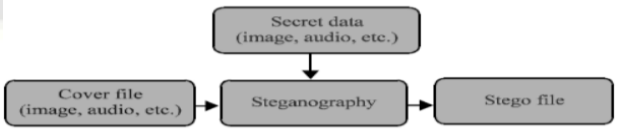


Figure 1. Process of Steganography

Steganography can be essentially processed in text, audio and image Text: Using this technique, ordinary text can be concealed and used to reveal secret information. One of the more traditional and significant strategies of information

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

concealment is this one. This approach is thought to be effective for regular text files with minimal redundant content [1].

Audio: To conceal the information in this technique, audio files are employed as cover files.

Image: The secret information is concealed using visuals in this technique. Moreover, one of the most widely used methods for a variety of reasons is to conceal information in digital images. Digital images can have many extra bits replaced with secret data without affecting the appearance of the image. Digital images are increasingly being used in various digital media. In this domain, there are also two different kinds of image steganography techniques:

The spatial domain, where sensitive information will be inserted right into the pixel intensity.

Transform domain/frequency domain, where secret information is initially inserted into the image after which it has been changed [2], [3].

This article focuses mostly on image-based steganography because, while there are many different ways to hide information, image-based steganography is particularly useful. Types of steganography techniques can be classified based on hiding methodology as shown in the Figure.2.

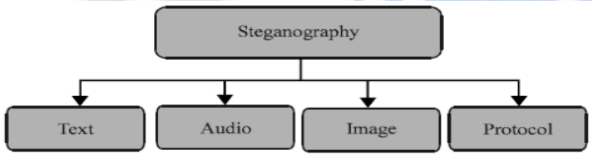


Figure 2. Types of Steganography

Secured medical image transmission is built on the guiding principles of authenticity, secrecy, and integrity. Confidentiality includes preventing unauthorized parties from accessing data. Only authorized users can be given access to information. Data must be same in both the sending and receiving directions. There should be no changes, omissions, or revisions. Integrity refers to the procedure in question here. The process of determining whether or not a communicating entity actually is who it purports to be is known as authentication. This substantiates the hypothesis that the data pertain to the same subject. Any message, whether it is text or a picture, can be concealed if cryptography is utilized as the method of protection. In order to transform a generic algorithm into a particular encryption method, cryptographic procedures call for the utilization of encryption keys. Encryption converts data into a format that cannot be read, hence providing security for the data. As a consequence of this, the invaders are unable to comprehend the information contained inside the data unless particular and complicated modifications are made. This work highlights the importance of security and introduces a safe data transmission approach for medical photographs that Figure against privacy intrusions [4]. The primary purpose of steganography is to conceal essential information within a medium in such a way that only authorized individuals are able to access it. It is crucial to have secure texting, particularly when dealing with sensitive and confidential information. Messages can now be sent in a variety of media, including text, image, audio, and video. A strong security system that combines steganography and cryptography is required to secure its confidentiality and integrity [5]. Figure 3 Shows the types of Steganography based on hiding methods.

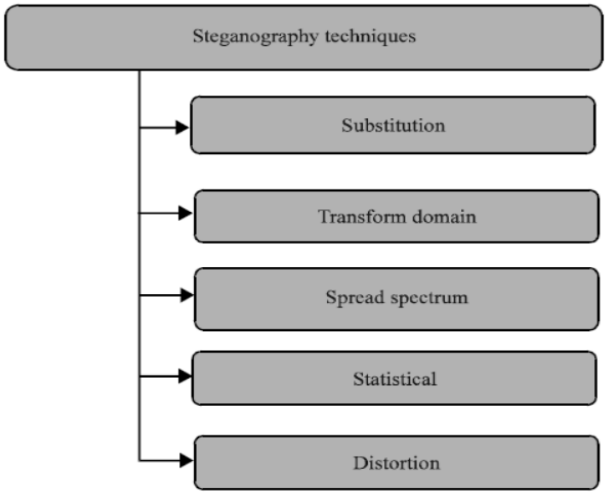
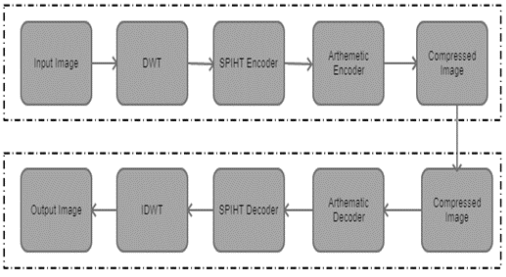


Figure 3. Types of Steganography based on hiding methods

2. RELATED WORK

Compression is essential for increasing transmission speed and is sufficient for utilizing the available bandwidth while transferring data over a channel. The best optimization technique and compression algorithm combine to reduce the image's size while preserving its quality. Set Partitioning in Hierarchical Trees (SPIHT), a strong wavelet-based compression algorithm is responsible for the creation of compressed images of an exceptionally high quality. One of the many advantages provided by SPIHT is gradual visual transmission. This is just one of several. A straightforward quantization approach that facilitates quick encoding and decoding. It produces lossless data compression and is entirely flexible.[6]. The SPIHT-HC (SPIHT-Huffman coding) strategy for reducing redundancies has decreased flow rates and given the encoding and unwinding processes plenty of time. Given that each image in the layout is encrypted by the Huffman encoder. Figure 4 presents the block diagram of an image compression algorithm that makes use of SPIHT in conjunction with arithmetic coding.



Block diagram for SPIHT and arithmetic coding-based picture compression

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A. Set Partitioning in Hierarchical Trees- Description One of the more sophisticated systems is SPIHT (Set Partition in Hierarchical Trees). The fundamental idea is to process an image using progressive coding while simultaneously decreasing the threshold. The idea of zero trees is where the distinction lies (spatial orientation trees in SPIHT) [7]. It is likely that the offspring of a coefficient at the highest level of the transform in a specific sub-band that was found to be unimportant against a particular threshold will also be unimportant. As a result, we can encode several coefficients using a single symbol. A pyramid formed by iteratively dividing four sub-bands defines a spatial orientation tree. As a result, the SPIHT method maintains several bits that specify unimportant coefficients [8].

B. Set Partitioning of Hierarchical Trees with Arithmetic Coding (SPIHT-AC) A significant number of consecutive "0"s are used in SPIHT encoding to create the bit stream. The best likelihood value for the number "000" is typically 1/4. In this manner, divide the double yield SPIHT stream into 3 bits-long gatherings. Each cluster was represented by a picture, a composite of eight distinct types of images, and their occurrence probability was encoded using entropy coding to reflect how closely they were packed within the suggested framework. It is used as an entropy coding (number juggling coding). One of the well-known method for lossless information number-crunching coding [9], [10]. The idea can be traced back to Shannon [11], but it was unambiguously portrayed by Shannon first. The process of computing numbers generates pressure that can approach or perhaps reach entropy. If our message consists of pictures spread out over a limited alphabet, we can create the appropriate number of bits for each picture (say, 1.6 bits/image) using this method. Huffman encoding sets this limitation on itself by requiring that the number of bits encoded per image be a whole number (for instance, 2 bits/image). Number juggling coding produces entropy (or extremely close to it) by clustering images together until a whole number estimate of bits may be a yield for a series of images (e.g. ABC may compare to 1011)[12].

Compressed Secret Image Encryption:

A lot of data is exchanged on the networks every day as a result of the prevalence of social networks and other digital applications, which are utilized more regularly. Making sure that this Data is secure is the main priority. Secure data transit over the internet must be ensured. As society evolves to the digital information era, the significance of network security challenges has grown. Internet use is increasing, which encourages an increase in cybercrime. [13].

By using cryptography, data security can be established. In this process, data is converted into a secret code with the aid of a key. The only way to return this data to its original state using a key is for authorized users. Cryptography is the term for this technique. Encryption transforms the original data into coded form, and decryption restores the original data to its original form. Cryptographic keys are classed based on how many are utilized for encryption and decoding. [14]. this is feasible to see the two crypto categories of different information protection techniques, as shown in the Figure 5.

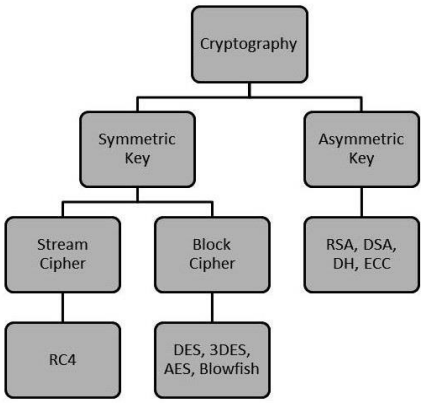


Figure 4. Different Cryptographic Techniques

Encryption:

Step 1: Read raw plain text and determine each character's matching ASCII value, and save in the input array.

Step 2: Reading the secret code in array S converts each element of array S into seven-bit binary.

Step 3: Compute the binary sequence's 2's complement that was received in step 2.

Step 4: Increase the value from step 2 by 8 bits on the left side. Now change it to matrix 8x8 called "X."

Step 5: Increase the value from step 3 by 8 bits on the left side. Change it to an 8x8 matrix called "Y."

Step 6: Z=XY

Step 7: The result is saved in "A" once Z elements are added. If the sum is 0, then a secret value needs to be assigned. If the sum is more than 127, A=A mod 127. Then, repeat those seven bits until the length matches the input by converting A to seven-bit binary. Include it in array I. Split I into two arrays, I1 and I2, with the elements of I1 spanning the range from sum to end and the elements of I2 spanning the range from 0 to sum-1. To make S1, a single array, combine I1 and I2.

Step 8: Execute an XOR operation between this S1 and the input array's binary representation. Consider that the ASCII characters that correspond to the result are a cypher by converting the result into decimal numbers.

Decryption:

Step 1: Input the encrypted text, look up the ASCII value of each character, then save the results in the Output Array.

Step 2: Read the hidden code in array S and every component should be converted to seven-bit binary.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Step 3: Compute the binary sequence that was obtained in step 2's 2'compliment.

Step 4: Increase the value from step 2 by 8 bits on the left side. Now change it to matrix 8x8 called "X."

Step 5: Increase the value from step 3 by 8 bits on the left side. Change it to an 8x8 matrix called "Y."

Step 6: Z=XY

Step7: The sum of the Z elements is stored in "A." If the sum is 0, a hidden value should be assigned. If the sum is greater than 127, replace it with A=A modulo 127. Iterate the binary representation of A (7 bits) until it exactly matches the length of the input. Arrange it in a matrix. Separate I into a smaller array, I1, holding the values 0 through sum, and a larger array, I2, including the values 0 through the end of I. Join arrays I1 and I2 to form S1.

Step 8: Execute an XOR operation between this S1 and the output array's binary form. Consider seven bits at a time when converting the result into decimal values. The resulting string of ASCII characters will be converted to plain text.

3. LIFTING WAVELET TRANSFORM (LWT) EMBEDDING IN TRANSFORM DOMAIN:

Lifting wavelet transform is equivalent to DWT [15]. With the exception of the fact that the amount of samples at each stage is the same as the initial set of data. In order to create an approximation as well as details, the input samples are first split up into even and odd sets of samples, and then they are processed by the filters of the lifting phases. Memory can be saved as a result of the fact that the number of samples that need to be stored at each stage is equal to the number of samples that are input. The number of necessary computations is reduced as a result of the fact that the approximation coefficients at one level can be derived from the detail coefficients that have previously been computed in addition to some of the samples that are input. [16][17]. with perfect reconstruction, the integer wavelet coefficients are also feasible [18]. The lifting wavelet transform makes hardware implementation simple. With zero padding extension mode and no extra coefficients, LWT is equivalent to the poly-phase version of the DWT method [19].

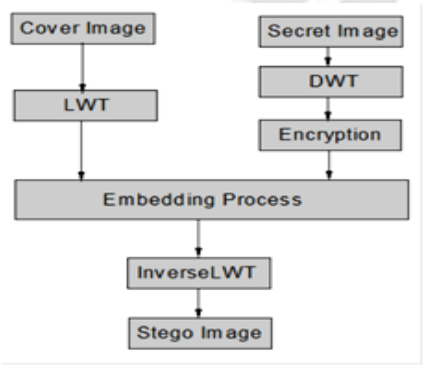


Figure 5. Block Diagram for Embedding Stage in Proposed Steganography

4. RESULT AND DISCUSSION

In this section, 150 color images with a resolution of 256 X 256 pixels each are used to test the experimental outcomes of the technique. Due to space restrictions, some simple visual examples are provided below. After conducting the number of experiments the efficiency of the proposed model is evaluated and tabulated in the following tables. Figure.7. is the cover images of testing the algorithm. Figure.8 [20,21] .shows the testing images of secret images for the algorithm. Figure 9 and Figure 10 are the simulated results of the algorithm. The table 1 shows the secret image's Mean square error (MSE), peak signal to noise ratio (PSNR) and compression ratio (CR). The table 2 shows the cover images, secret images and stego image and PSNR, MSE

Figure 6. Testing cover Images for the algorithm

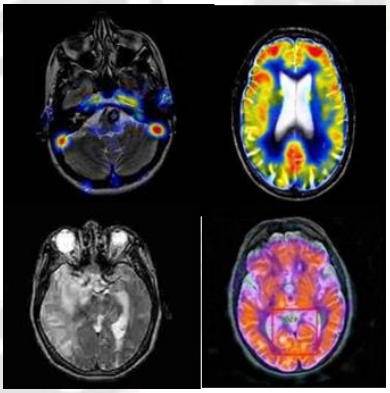


Figure 7. Testing Secret Images for the algorithm

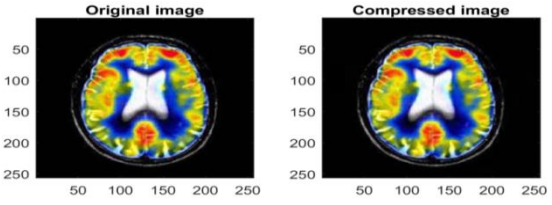


Figure 8. Compression algorithm Results

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

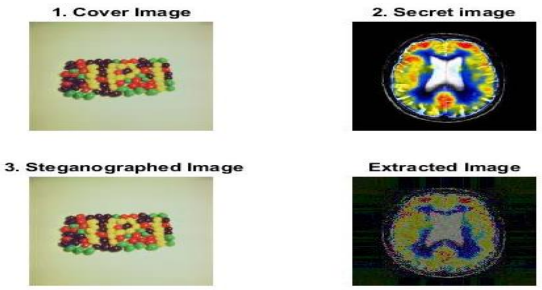


Figure 9. Steganography Results

TABLE I. PERFORMANCE EVALUATION OF COMPRESSION ALGORITHM FOR DCT & DWT

S.No.	*Method*	*Compression Ratio*	*Mean Square Error*	*Peak Signal to Noise Ratio*
1	DWT	34.8404	2.5715	44.0290
2		51.1042	2.3852	44.3556
3		37.3001	1.1196	47.6403
4		49.8099	3.1185	43.1914
1	DCT	9.2871	30.6228	33.2704
2		14.2902	33.4726	32.8839
3		10.0302	22.5553	34.5983
4		11.4880	30.4286	33.2980

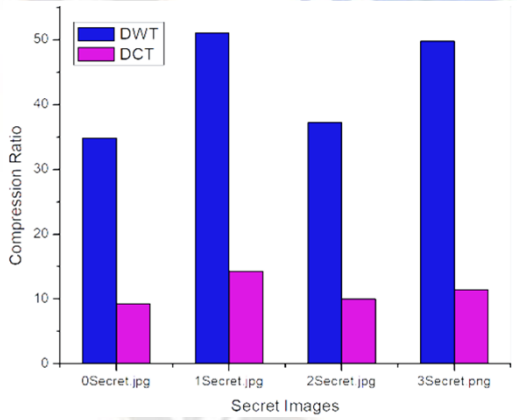


Figure 10. Comparison of compression Ratio

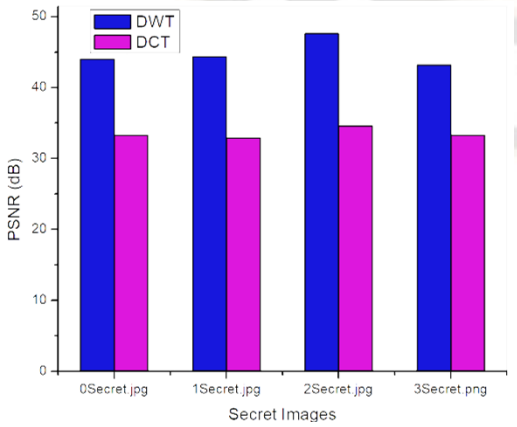


Figure 11. Comparison of PSNR during Compression

From Figure 11 & Figure 12 it is evident that DWT based compaction of data prior to embedding is dominant when compared with DCT and this dominance is owing to the usage of proper thresholding of unwanted high frequencies in the image.

TABLE II. PERFORMANCE EVALUATION OF STEGANOGRAPHY ALGORITHM FOR DWT & LWT

S.No.	*Method*	*Mean Square Error*	*Peak Signal to Noise Ratio*
1	DWT	59.8372	30.3951
2		63.8171	30.1154
3		193.0374	25.3084
4		34.1306	38.8540
1	LWT	59.1626	30.4443
2		64.2786	30.0841
3		192.6645	25.3168
4		33.9782	38.8734

From Table II it is evident that the usage of lifting schemes in design of filter bank the LWT based embedding scheme is more efficient.

5. CONCLUSION

The proposed technique of encrypting data, which uses hybrid steganography rather than just steganography alone, surpasses the traditional steganography approach. This model is separated into two stages as was previously stated. The initial phase is the embedding phase. The subsequent phase is the extraction process. The key elements of the steganography model's success were taken into account in this study (security, compression, robustness). A few measures, including PSNR, MSE, and CR, were calculated to assess the suggested methodology. The hidden image that was extracted resembles the original private image. And we may state that the following was delivered by this model. The proposed model provides increased security. More space is provided for hiding secret image by using the DWT algorithm. The embedding model is made robust owing to the advantages of lifting wavelet transforms (LWT).

Refrences

[1] A Review on Medical Image Compression Using Wavelet Transform in Medical Images.pdf'.
[2] J. Adabala and K. N. Prakash, 'D Ual T Ree C Omplex W Avelet T Ransform for', vol. 4, no. 2, pp. 482–492, 2020.
[3] J. G. Clearly, R. M. Neal, and I. H. Witten, '[CNW87] Arithmetic coding for data compression', Commun. ACM, vol. 30, no. 6, pp. 520–540, 1987, [Online]. Available: https://dl.acm.org/citation.cfm?id=214771
[4] H. I. Shahadi, R. Jidin, and W. H. Way, 'Lossless audio steganography based on lifting wavelet transform and dynamic stego key', Indian J. Sci. Technol., vol. 7, no. 3, pp. 323–334, 2014, doi: 10.17485/ijst/2014/v7i3.14.
[5] A. Priyadharshini, R. Umamaheswari, N. Jayapandian, and S. Priyananci, 'Securing medical images using encryption and LSB steganography', Proc. 2021 1st Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. ICAECT 2021, pp. 2–6, 2021, doi: 10.1109/ICAECT49130.2021.9392396.
[6] O. P. Singh and A. K. Singh, 'Data hiding in encryption–compression domain', Complex Intell. Syst., no. 0123456789, 2021, doi: 10.1007/s40747-021-00309-w.

[7] R. Farheen and S. B. Lakshmi, 'WAVELET LIFTING SCHEME FOR IMAGE COMPRESSION BASED ON', vol. 6, no. 6, pp. 2876–2882, 2019.
[8] L. Wei, P. P. Zhen, and J. L. Zhi, 'SPIHT algorithm combined with Huffman encoding', 3rd Int. Symp. Intell. Inf. Technol. Secur. Informatics, IITSI 2010, pp. 341–343, 2010, doi: 10.1109/IITSI.2010.63.
[9] X. Huang and K. L. Ou, 'Faculty of Education, Science, Technology and Mathematics University of Canberra, Australia 3 College of Oral Medicine, Taipei Medical University, Taiwan', vol. 7, no. 1, pp. 1–16, 2015.
[10] A. U. Islam et al., 'An improved image steganography technique based on MSB using bit differencing', 2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016, pp. 265–269, 2017, doi: 10.1109/INTECH.2016.7845020.
[11] A. Krishna A and L. C. Manikandan, 'A Study on Cryptographic Techniques', Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3307, pp. 321–327, 2020, doi: 10.32628/cseit206453.
[12] S. K. Kumar, P. D. K. Reddy, G. Ramesh, and V. R. Maddumala, 'Image transformation technique using steganography methods using LWT technique', Trait. du Signal, vol. 36, no. 3, pp. 233–237, 2019, doi: 10.18280/ts.360305.
[13] G. G. Langdon, 'An Introduction to Arithmetic Coding', IBM J. Res. Dev., vol. 28, no. 2, pp. 135–149, 1984, doi: 10.1147/rd.282.0135.
[14] T. A. majead Kadum and S. N. Al-Saad, 'Image Hiding Using Lifting Wavelet Transform', Int. J. Sci. \& Eng. Res., vol. 7, no. April, 2016.
[15] C. Valens, 'The Fast Lifting Wavelet Transform'. 1999.
[16] T. W. Sweldens, '3 . Lifting Scheme of Wavelet Transform', pp. 82–108.
[17] T. Morkel, M. S. Olivier, and J. H. . Eloff, 'an Overview of Image Steganography', Africa (Lond)., vol. 83, no. July, pp. 51–107, 2005, [Online]. Available: http://martinolivier.com/open/stegoverview.pdf
[18] M. S. Murthy, 'Efficient Digital Image Compression by Using SPIHT Algorithm Combined with Huffman Encoding', vol. 2, no. 12, pp. 301–308, 2013.
[19] D. Nashat and L. Mamdouh, 'An efficient steganographic technique for hiding data', J. Egypt. Math. Soc., vol. 27, no. 1, 2019, doi: 10.1186/s42787-019-0061-6.
[20] Xiaoxiao Li; Xiaopeng Guo; Pengfei Han; Xiang Wang; Huaguang Li; Tao Luo 'Laplacian Redecomposition for Multimodal Medical Image Fusion' IEEE Transactions on Instrumentation and Measurement (Volume: 69, Issue: 9, September 2020) DOI: 10.1109/TIM.2020.2975405
[21] Kai Guo. Xiongfei Li, Hongrui Zang and Tiehu FanMulti-Modal Medical Image Fusion Based on FusionNet in YIQ Color Space' Entropy 2020, 22, 1423; doi:10.3390/e22121423 www.mdpi.com/journal/entropy