JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

Development of Amalgamation Approach to Strengthen Security using Watermarking.

Neha Saini[1], Nitin Kumar[2]
M. Tech Scholar[1] – GITAM, Department of ECE, Kablana, Jhajjar, Haryana, India
Assistant Professor[2]– GITAM, Department of ECE, Kablana, Jhajjar, Haryana, India
sainineha24081991@gmail.com[1], hod.cse@gangainstitute.com[2]

Abstract
In the era of Information and Communication Technology, the exchange of information has increased significantly, prompting a greater need for secure communication to ensure data security. The enlargement of the internet has introduced security challenges in watermarking. With the advancements in computer networks, digital data can be easily duplicated, modified, and illicitly distributed. As a result, copyright protection for digital data has become a crucial research focus in information security. Techniques such as encryption, steganography, and watermarking are employed to provide authenticity to multimedia data. Through an extensive review of high-quality research papers, it has been discovered that various methods exist for successful implementation of digital watermarking, tailored to specific application requirements. In our implemented work, the initial phase involves collecting a high-quality dataset from reliable sources. This is followed by rigorous testing against different attacks to ensure the proposed method's robustness. Through comparative analysis, it has been observed that the proposed method yields superior results compared to existing techniques.
Keywords: Watermarking, LWT, SVD, WHT, Cryptography, Security, Attacks

1. Introduction

The continuous advancement of technologies has led to significant research breakthroughs. However, with the widespread use of popular techniques over the internet, security concerns arise [1]. In order to protect the data available on the internet, various techniques have been developed to facilitate secure data transmission according to specific application requirements. Among these techniques, watermarking has emerged as an innovative technology for ensuring secure data transmission. Watermarking can be categorized into spatial domain and transform domain methods. In spatial domain watermarking, the method directly operates on the pixels of the digital image formed by integrating a large number of pixels [2]. On the other hand, transform domain watermarking involves altering coefficients using techniques such as DCT and DFT. DCT is robust against JPEG compression but vulnerable to geometric deformation [3], making it suitable for image compression. DFT, on the other hand, withstands geometric attacks and is commonly used for rotation invariant and translation resistant applications [4-5]. Sub-bands in transform domain watermarking provide information about the original image. The LL sub-band contains detailed information about the image at lower frequencies, while the remaining sub-bands offer diagonal, vertical, and horizontal information. L stands for LPF (Low-Pass Filter), and H stands for HPF (High-Pass Filter). The selection of a specific sub-band depends on the requirements, and the watermark is embedded accordingly [6-8]. Numerous secure watermarking methods exist to safeguard data from unauthorized access and protect against various types of attacks.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

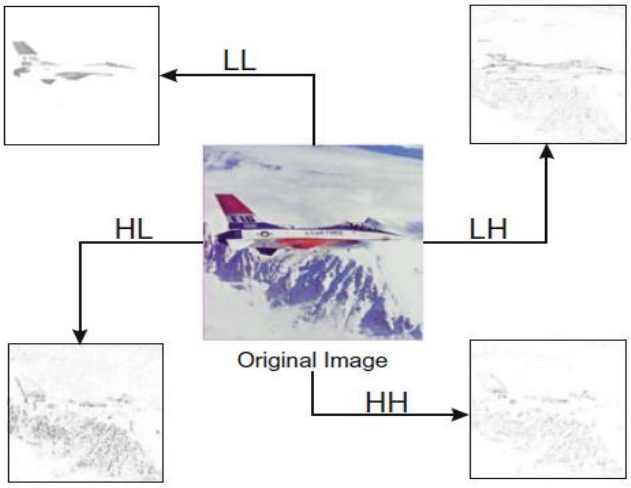


Fig.1: Image segmentation in different bands [7]

2. Watermarking and Attacks in Watermarking

Digital watermarking refers to the process of embedding digital data, such as images, audio, or videos, with additional information that is difficult to remove. As communication technologies advance, decrypting a ciphertext has become relatively easy [9-10]. Consequently, there is a growing need for more robust technologies that can provide enhanced data security beyond the limitations of cryptography. This is where techniques like steganography and watermarking come into play. Steganography involves hiding information within a cover image, ensuring that the hidden data cannot be accessed by unauthorized parties [11]. On the other hand, watermarking associates concealed information with a cover object, making it somewhat similar to steganography. Watermarking techniques are commonly used for copyright protection and authentication of the rightful owner of the content.

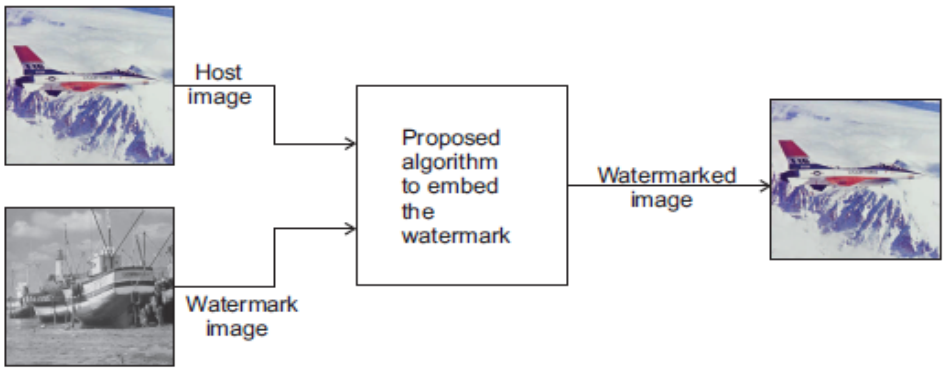


Fig.2: Fundamental Principle of Watermarking [3]

The process of watermarking involves inserting an authentic image and an appropriate watermark using various available techniques. At the receiving end, a reverse process is executed to extract the watermark image from the watermarked image. To ensure security and prevent unauthorized access to the data, a secret key is used during the insertion and extraction processes [13].

Watermarking Attacks: However, despite the advantages of watermarking techniques, they are not immune to attacks. Watermarked objects can be vulnerable to intentional or unintentional attacks. Various software tools are available that can be used to launch attacks on a watermarked system. The primary objective of these attacks is to disrupt the functionality of the watermarked system and prevent it from carrying out its intended purpose.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

Fig.3: List of various watermarking attacks

There are several types of attacks that can be launched on watermarked objects:

- **Removal Attack:** The objective of this attack is to remove the watermark data from the watermarked object. Attackers exploit the fact that the watermark often appears as noise in the host signal.
- **Interference Attack:** In this type of attack, additional noise is introduced into the watermarked object. Examples of interference attacks include quantization, averaging, denoising, lossy compression, and noise injection.
- **Geometric Attack:** These attacks manipulate the geometry of an image, such as flips, rotations, and crops. Crop attacks from the bottom or right-hand side of an image are examples of geometric attacks.
- **Protocol Attack:** Attackers may attempt to modify the watermark or estimate and modify the watermark algorithm when they gain knowledge about the watermarking algorithm. A secure watermark algorithm should be resistant to distortion, detection, and forgery of the embedded data [14]. However, there are some limitations, including:
- Watermarking techniques cannot prevent image imitation, but they can help identify the genuine owner of the imitated image.
- If an image is manually manipulated, the watermark may disappear from the image.

It is important to develop robust watermarking techniques that can withstand these attacks and provide effective protection for the embedded data.

3. Proposed Work

Lifting Wavelet Transform: The wavelet transform is a time domain analysis technique that decomposes data, such as an image, into different spatial domains and independent frequencies. In the case of the Discrete Wavelet Transform (DWT), the image is segmented into four regions: HH, HL, LH, and LL. Among these, LL represents the low-frequency segment, while the others correspond to high-frequency segments. Figure 1 illustrates the one-level DWT decomposition process. However, one of the drawbacks of the DWT technique is the blurring effect caused by the wavelet filter, along with the production of ringing noise at the image edges. The Lifting Wavelet Transform (LWT) addresses these drawbacks and also minimizes the processing time, which is a significant milestone [9-11].

Walsh-Hadamard Transform: While the Fourier transform can be applied to both real and complex numbers, the Hadamard transform is a specific type of Fourier transform. The Hadamard transform performs various operations, such as linear, orthogonal, and symmetric, on 2m real numbers. It can be regarded as a composition of Discrete Fourier Transforms (DFTs).

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

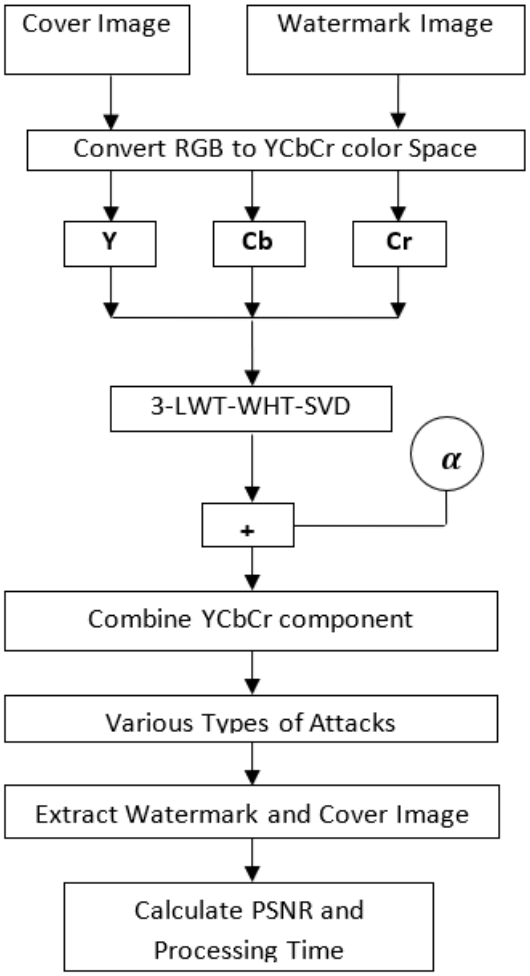


Fig.3: Block Diagram of Proposed Architecture

Figure 3 represents the watermarking process from host and watermark image in YCbCr color space using three level LWT-WHT-SVD technique. After that, Watermarked image exposed to various attacks like blur attack, sharpen attack etc. to check the robustness of the process. Finally, both cover and watermark images are extracted with PSNR, RMSE.

The Walsh-Hadamard Transform disassembles a random input vector into a combination of Walsh functions. The Hadamard transform matrix comprises elements that are either 1 or -1, making it an orthogonal square matrix. The smallest Hadamard matrix, denoted as H1, is represented as [9-11].

$$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \quad \text{…….. Eq. (1)}$$

Higher size matrix computed with help of smallest Hadamard matrix as shown below:

$$H_2 = H_1 \times H_1 = \frac{1}{(\sqrt{2})^2}\begin{bmatrix}H_1 & H_1\\ H_1 & -H_1\end{bmatrix} \quad \text{…….. Eq. (2)}$$

In general formula for computing higher order matrix is depicted below:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

$$H_n = H_{n-1} \times H_1 = \frac{1}{\left[\sqrt{2}\right]^n}\begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} \quad \text{…….. Eq. (3)}$$

Singular Value Decomposition

The Hadamard Singular Value Decomposition (SVD) technique is widely used in various applications, including matrix operations and data reduction in machine learning. Consider a matrix M of size m×n, which can be either real or complex. The SVD technique decomposes this matrix into three distinct matrices as shown in Equation (4):

$$M = USV^T \quad \text{……. Eq. (4)}$$

In this equation, V is a unitary matrix of size n×n (real or complex), U is also a unitary matrix of size m×m (real or complex), and S is a rectangular diagonal matrix of size m×n. The diagonal of S contains non-negative real numbers. One significant advantage of the SVD technique is that when using a singular matrix to insert a watermark, the minimum values of the host images are altered. This results in minimal changes occurring in the image, allowing for the discard of insignificant modifications [9-11].

4. Result and Discussion

In this section existed technique and proposed hybrid technique result are analysed for various parameters for example peak signal to noise ratio (PSNR), Computational time for embedding and extracting an image.

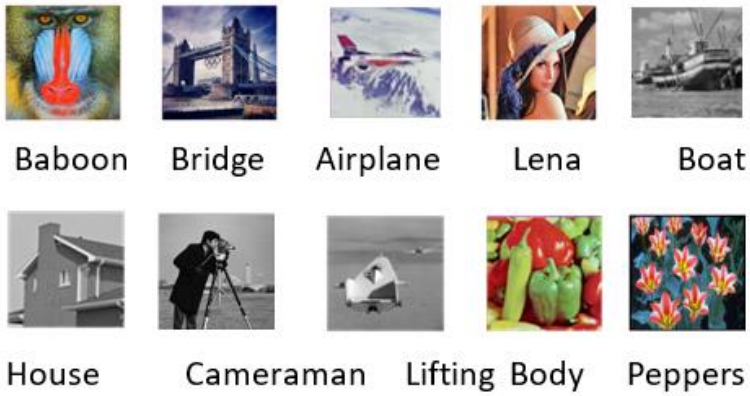


Fig.4: Expermental dataset used for Watermarked process

First of all, there is a requirement of data set on which watermarking process will be executed. There are various sources available from where data set can be fetched.

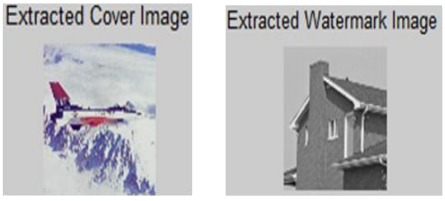


Fig.5: Extracted cover and watermark image

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

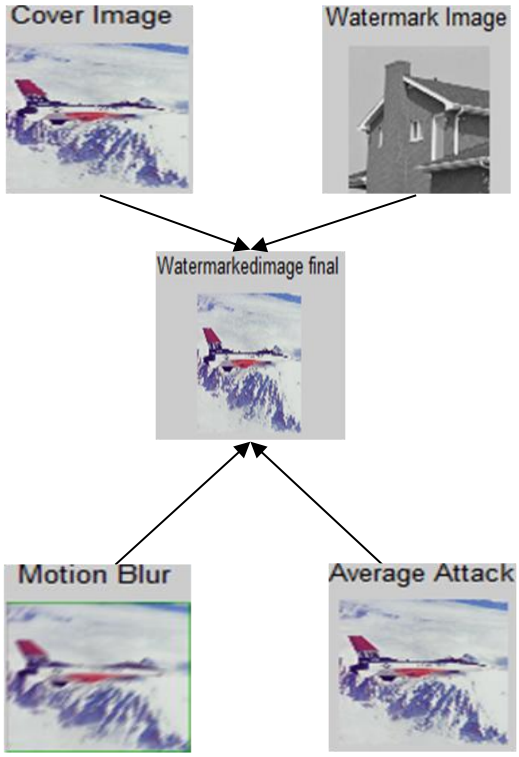


Fig.6: Complete output overview of Algorithm

Following equation are used to determine RMSE and PSNR of cover image and watermarked image.

$$\text{RMSE}(x) = \sqrt{\frac{1}{N}||x - x\hat{}||^2} = \frac{1}{N}\sum_{i=1}^{N}(x - x\hat{})^2 \text{..... Eq. (5)}$$

Where N represent cover image size, x represents cover image and x^ depicts watermarked image.

$$\text{PSNR}(x) = \frac{20 * \log((255))}{\text{RMSE}(x)} \text{..... Eq. (6)}$$

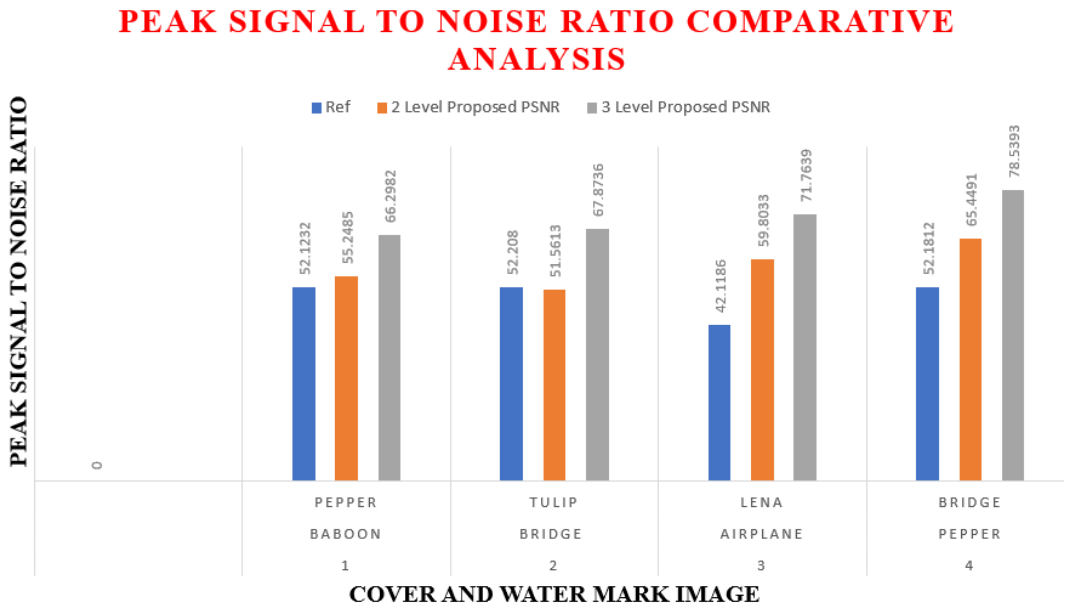
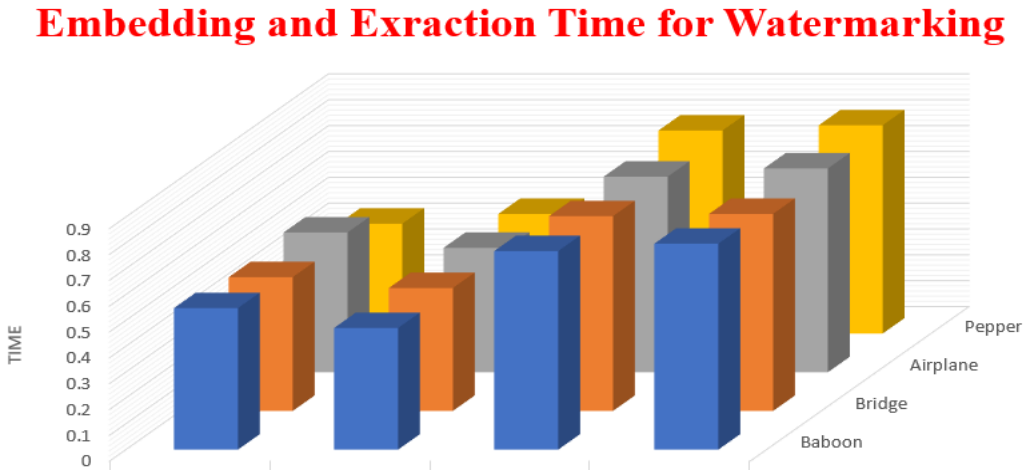


Fig.7: Comparative investigation of reference PSNR, 2 level PSNR and 3 Level PSNR (Proposed Method) for watermarking.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452



	Ref Embedding Time	1 Level Proposed Embedding Time	2 Level Proposed Extraction Time	3 Level Proposed Extraction Time
Baboon	0.5474	0.4704	0.7681	0.7966
Bridge	0.5175	0.4755	0.7535	0.7623
Airplane	0.5407	0.4815	0.7569	0.7884
Pepper	0.4251	0.463	0.7857	0.8057

Fig.8: Embedding and Exraction Time for Watermarking

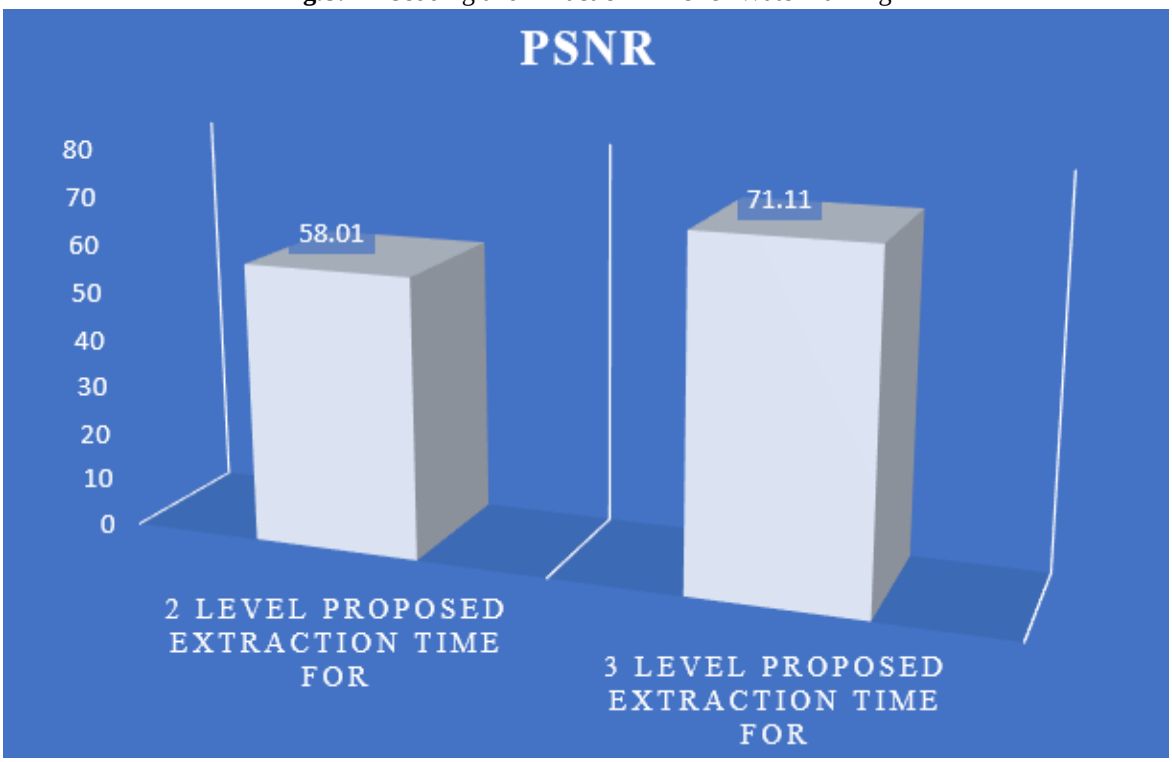


Fig.9: PSNR Comparative analysis for existed and proposed technique

JOURNAL OF ALGEBRAIC STATISTICS
Volume 14, No. 1, 2023, p.107-116
https://publishoa.com
ISSN: 1309-3452

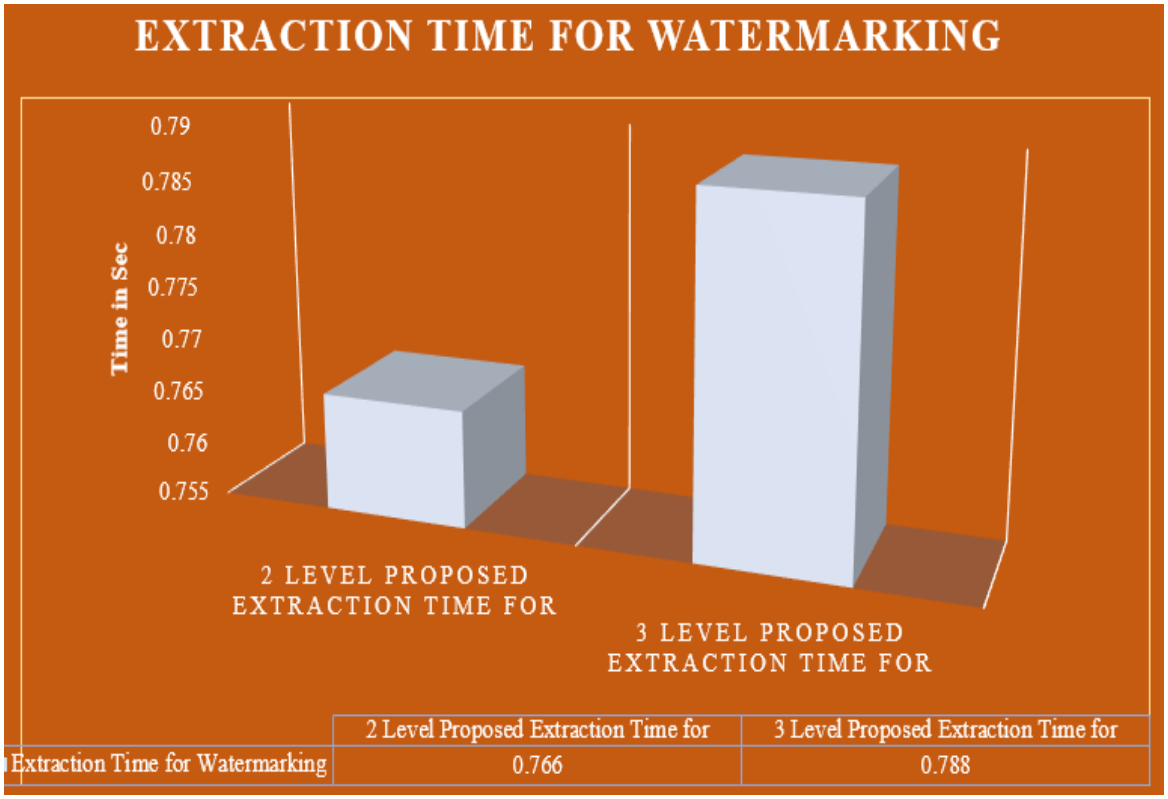


Fig.10: Extraction time Comparative analysis for existed and proposed technique

5. Conclusion

In this paper, a hybrid method for watermarking in the YCbCr color space was implemented. The initial phase involved translating both the cover and host images from RGB to YCbCr color space. From the projected color space, three channels were generated, with the Y channel selected for further processing. Alternatively, any channel could be chosen. The next step involved performing a three-level lifting wavelet transform (3-LWT) to divide the images into four frequency-based segments or bands (HH, HL, LH, LL). Following the 3 level-LWT, WHT method was applied, followed by SVD to obtain the projected output. The key objective of implemented work was to achieve a desirable PSNR value and robustness against numerous attacks, ensuring superior performance compared to other methods. The implemented method demonstrated better results across various parameters. Relative investigation among existed and proposed method analyzed for PSNR values and processing times for embedding. According to the findings, the existing technique yielded a PSNR value of 58.01, while the proposed technique achieved a significantly higher value of 71.11. In this proposed work computational time was recorded 0.788 second whereas for existing method it was 0.766 seconds. From implemented work it is clear that proposed 3 level LWT-WHT-SVD perform better than existed methods. Overall, this research work successfully implemented a hybrid technique in the YCbCr color space for watermarking, showcasing boosted performance in terms of PSNR and processing time when compared to existing methods.

References

[1] R. Sinhal and I. A. Ansari, "Machine learning based multipurpose medical image watermarking," Springer, Neural Computing and Applications, vol. 24, Mar. 2023.
[2] V. K. Pallaw, K. U. Singh, A. Kumar, T. Singh, C. Swarup, and A. Goswami, "A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications," MDPI, Electronics, vol. 12, no. 334, 2023.
[3] C.-C. Lin, T.-L. Lee, Y.-F. Chang, P.-F. Shiu, and B. Zhang, "Fragile Watermarking for Tamper Localization and Self-Recovery Based on AMBTC and VQ," MDPI, Electronics, vol. 12, no. 415, pp. 1-15, 2023, doi: 10.3390/electronics12020415.

[4] R. Sinhal, S. Sharma, I. A. Ansari, and V. Bajaj, "Multipurpose medical image watermarking for effective security solutions," Multimedia Tools and Applications, vol. 81, pp. 14045–14063, Springer, 2022.
[5] Y.-P. Chen, T.-Y. Fan, and H.-C. Chao, "WMNet: A lossless watermarking technique using deep learning for medical image authentication," Electronics, vol. 10, no. 8, article no. 932, 2021.
[6] Z. Zhang, M. Zhang, and L. Wang, "Reversible image watermarking algorithm based on quadratic difference expansion," Mathematical Problems in Engineering, vol. 2020, article ID 1806024, Hindawi, 2020.
[7] F. Ernawan and M. N. Kabir, "An improved watermarking technique for copyright protection based on Tchebichef moments," IEEE Access, vol. 7, pp. 84843–84853, 2019.
[8] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," IEEE Access, vol. 6, pp. 36460–36474, 2018.
[9] P. Pandey and R. K. Singh, "Novel digital image watermarking using LWT-WHT-SVD in YCbCr color space," International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 6, June 2017.
[10] V. Purohit and B. Verma, "A new approach for image watermarking using 3 LWT-Walsh transform-SVD in YCbCr color space," IJSRD - International Journal for Scientific Research & Development, vol. 5, no. 2, 2017.
[11] R. Dhanda and K. K. Paliwal, "Hybrid method for image watermarking using 2 level LWT-Walsh transform-SVD in YCbCr color space," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, no. 11.
[12] S. Hussainnaik, F. Indikar, and R. H. Husennaik, "Review on digital watermarking images," IJEDR - International Journal of Engineering Development and Research, vol. 5, no. 2, pp. 336–339, 2017.
[13] N. V. Kumar, A. V. Ramana, C. S. Kumar, and V. Raghavendra, "An enhanced invisible digital watermarking method for image authentication," International Journal of Applied Engineering Research, vol. 12, no. 22, pp. 12016–12024, 2017.
[14] M. Khalili and M. Nazari, "Non Correlation DWT Based Watermarking Behavior in Different Color Spaces," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 7, no. 1, pp. 160-164, 2016.
[15] N. Chandrakar and J. Bagga, "Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space," International Journal of Scientific Research Engineering & Technology (IJSRET), vol. 4, no. 1, pp. 131-135, Jan. 2015.
[16] D. Vaishnavia and T. S. Subashini, "Robust and Invisible Image Watermarking in RGB Color space using SVD," 2014 International Conference on Information and Communication Technologies (ICICT), pp. 1-6, Dec. 2014.
[17] A. K. Singh, M. Dave, and A. Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain," The National Academy of Sciences, India (NASI), vol. 84, no. 2, pp. 351–358, Jul. 2014.
[18] P. M. Pithiya and H. L. Desai, "DCT Based Digital Image Watermarking, Dewatermarking & Authentication," International Journal of Latest Trends in Engineering and Technology (IJLTET), vol. 2, no. 3, pp. 223-227, May 2013.
[19] H. B. Kekre, T. Sarode, and S. Natu, "Performance Comparison of DCT and Walsh Transforms for Watermarking using DWT-SVD," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 4, no. 2, pp. 8-12, Feb. 2013.
[20] Anuradha and R. P. Singh, "DWT Based Watermarking Algorithm using Haar Wavelet," International Journal of Electronics and Computer Science Engineering, vol. 1, no. 1, pp. 1-6, 2012.
[21] R. Ansari, M. M. Devanalamath, K. Manikantan, and S. Ramachandran, "Robust Digital Image Watermarking Algorithm in DWT-DFT-SVD Domain for Color Images," 2012 International Conference on Communication, Information & Computing Technology (ICCICT), pp. 1-6, Oct. 2012.
[22] H.-C. Chen, Y.-W. Chang, and R.-C. Hwang, "A Watermarking Technique based on the Frequency Domain," Journal of Multimedia, vol. 7, no. 1, pp. 23-30, 2012.
[23] A. S. Akash and T. Anjul, "Choice of Wavelet from Wavelet Families for DWT-DCT-SVD Image Watermarking," International Journal of Computer Applications (IJCA), vol. 48, no. 17, pp. 1-5, June 2012.

[24] A. Poljicak, L. Mandic, and D. Agic, "Discrete Fourier transform–based watermarking method with an optimal implementation radius," Journal of Electronic Imaging, vol. 20, no. 4, p. 043013, 2011.
[25] M. Khalili and D. Asatryan, "Effective Digital Image Watermarking in YCbCr Color Space Accompanied by Presenting a Novel Technique Using DWT," Mathematical Problems of Computer Science, vol. 33, pp. 150–161, 2010.