**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 14, No. 1, 2023, p.117-123
https://publishoa.com
ISSN: 1309-3452

# Development of Amalgamation Approach to Strengthen Security using Watermarking: A Review

**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**
The following paper presents a comprehensive conceptual framework addressing security issues in watermarking. The widespread availability and usage of digital data, such as videos, audios, and images, due to the expansion of the internet, have introduced security challenges. To establish authenticity in multimedia data, techniques like encryption, steganography, and watermarking are employed. Extensive analysis of several high-quality research papers reveals the existence of numerous methods that can successfully implement digital watermarking, tailored to specific application requirements. These methods include DWT-DFT-SVD, LWT-WHT-SVD, DWT-QR, and DWT-FFT-SVD. In our research work, we will proceed in three distinct phases. First, we will prepare a dataset upon which the chosen watermarking technique will be applied. Second, we will evaluate different watermarking techniques to identify the one that yields optimal results in terms of PSNR (Peak Signal-to-Noise Ratio) and processing time. In this phase, we will subject the images to various attacks to ensure the implemented method can withstand such adversarial attempts. Finally, in the third and final phase, we will execute the reverse process to extract the host image and watermark. By following this structured approach, we aim to contribute to the field of security in watermarking and provide insights into efficient and robust techniques for protecting digital content integrity.
**Keywords:** Security, Watermarking, frequency, DWT, SVD, LWT

## 1. Introduction

In recent times, there has been a significant rise in the unauthorized alteration of digital multimedia, including videos, audios, and images. This surge can be attributed to the exponential growth of the internet and other multimedia sources. As a consequence, there is an urgent need for highly efficient digital watermarking algorithms to safeguard digital multimedia from unauthorized modifications [1]. Digital watermarking involves the concealment of digital information within the host data, allowing for subsequent extraction to verify ownership. The applications of watermarking techniques encompass crucial areas such as copyright protection, ownership verification, fingerprinting, and broadcast monitoring [2]. Key attributes of watermarking techniques include robustness, which denotes the ability of the watermark to withstand various forms of attacks. These attacks may include cropping, rotating, scaling, low-pass filtering, sharpness adjustments, resizing, addition of noise, JPEG compression, histogram equalization, and contrast adjustments [4-5]. It is imperative to develop watermarking methods that exhibit resilience against these types of attacks, ensuring the integrity and protection of digital multimedia content. By employing robust watermarking techniques, we can mitigate the risks associated with unauthorized modifications and maintain the authenticity and ownership verification of digital multimedia assets. Both intentional and unintentional attacks can compromise the security of digital watermarks. Robustness is a crucial property in watermarking algorithms, particularly for ownership verification. Achieving a high level of robustness entails embedding the watermark in the robust components of the host data [6]. However, it is important to strike a balance between robustness and perceptibility, as increasing the visibility of the watermark can degrade the quality of the watermarked image. In the realm of wavelet-based watermarking, the lifting wavelet transform has emerged as a preferred alternative to the discrete wavelet transform. The lifting wavelet transform generates second-generation wavelets that are not solely translations and dilations of a single function [7]. The process of assembling wavelets using the lifting scheme involves three steps: split, predict, and update. In the split phase, the data is divided into odd and even sets. The predict step utilizes the even set to predict the odd set. This prediction

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 14, No. 1, 2023, p.117-123
https://publishoa.com
ISSN: 1309-3452
phase ensures polynomial cancellation in the high-pass component. The update phase employs wavelet coefficients to update the even set, which is then used to calculate the scaling function. By incorporating the lifting wavelet transform and following these three steps, watermarking algorithms can enhance the robustness of the watermark, ensuring effective ownership verification while minimizing perceptibility and maintaining the quality of the watermarked image [9-10].

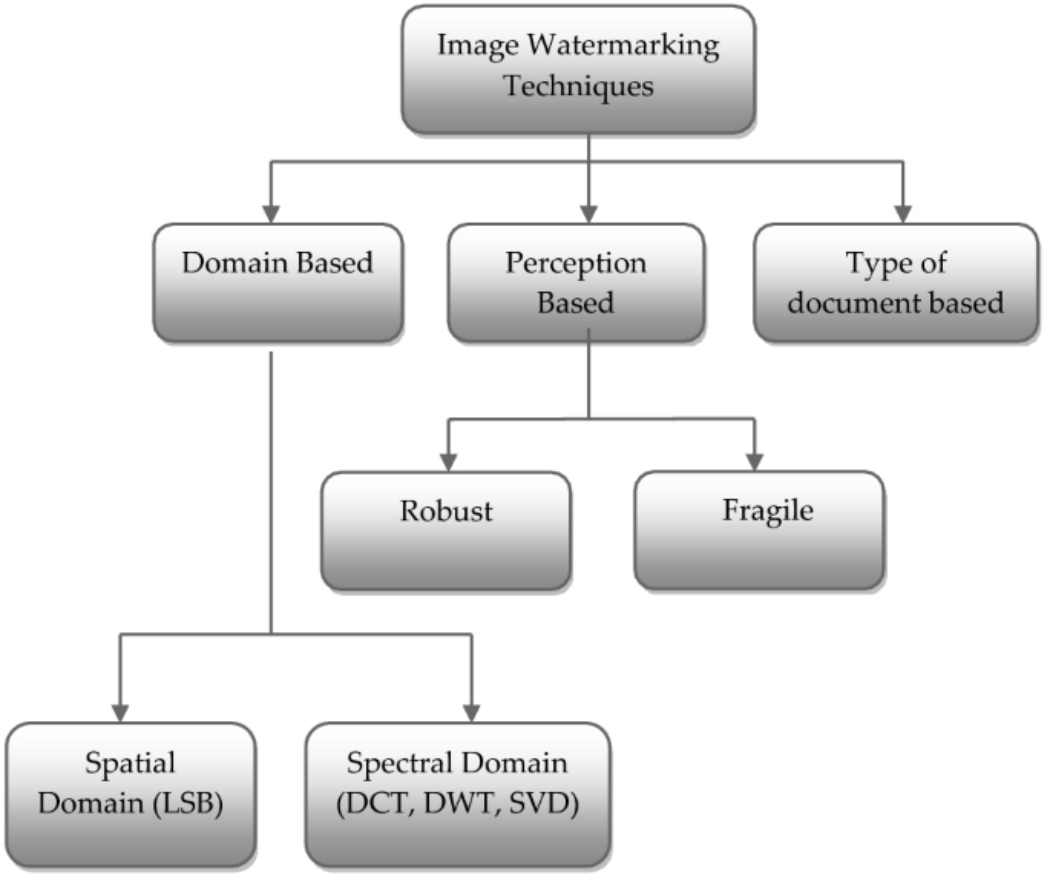


**Fig.1:** Image Watermarking Techniques

## 2. Watermarking and Its Principle

Digital watermarking refers to the process of embedding digital data, such as images, audio, or videos, with imperceptible information that is difficult to remove. It serves as a means of identifying and protecting digital content. As communication technology has advanced, traditional encryption methods have become easier to decrypt, highlighting the need for more robust security measures to safeguard our data. Steganography and watermarking have emerged as solutions to overcome the limitations of cryptography. Steganography involves the hiding of information within a cover image, audio, or video in such a way that it remains inaccessible to unauthorized parties. This technique ensures that the concealed information is integrated seamlessly with the cover object. In contrast, watermarking is closely related to steganography, as it also involves concealing information within a cover object. However, watermarking primarily focuses on copyright preservation and authentication of the holder. By employing watermarking techniques, we can establish ownership and protect digital content from unauthorized use [11]. The integration of hidden information within digital data provides a robust solution for ensuring copyright protection and verifying the authenticity of the content's owner.

**Principle of Watermarking:** There are mainly three different steps involved for a watermarking system:

- Embedding
- Attack
- Detection

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 14, No. 1, 2023, p.117-123
https://publishoa.com
ISSN: 1309-3452

During the initial stage, referred to as embedding, an algorithm receives a host image and a cover image to produce a watermarked image. Following this, the watermarked image or data is transmitted to another party. When this recipient manipulates the communicated data, it constitutes an attack, and various types of attacks can be aimed at the data. Lastly, in the detection phase, an algorithm is utilized to extract the watermark from the tampered signal. If the signal remains unaltered during the communication process, the watermark persists and can be retrieved. Likewise, when the image is replicated, the associated information is also carried within the duplicate.

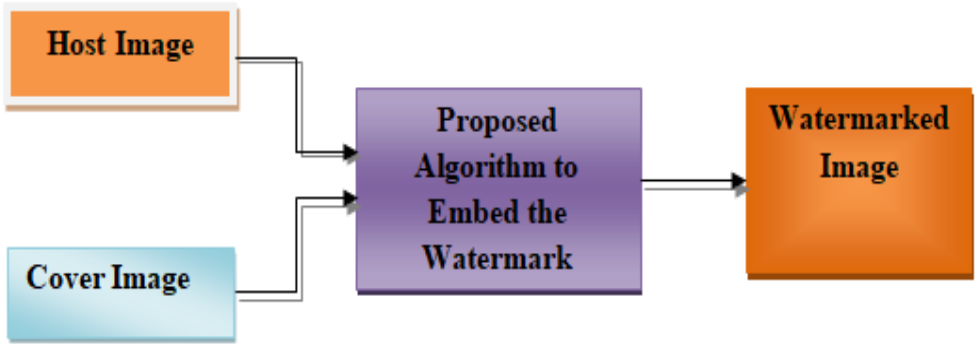


**Fig.2:** Basic Principle of Watermarking

To insert the genuine image and appropriate watermark, one of the available techniques is utilized. The receiver then employs a reverse process to extract the watermark image from the watermarked image. To ensure data security, a secret key is used during both insertion and extraction, preventing unauthorized access [12]. Digital watermarking techniques can be classified into two main categories: Spatial domain technique and frequency-domain technique.

**Spatial domain** techniques involve directly embedding secret messages into the cover image. This is achieved by modifying the pixels in randomly selected regions of the image, based on the chosen watermark. The algorithm parameters in this technique are determined by three factors: the signature's associated information, a secret random key, and the image's masking property. Spatial domain methods offer advantages such as ease of implementation, high payload capacity, and straightforward control. An example of such a technique is LSB watermarking. However, spatial domain methods are vulnerable to various steganalysis methods, even those with minimal impact.

**Frequency domain** techniques, on the other hand, encompass transformations of the cover image into frequency domain coefficients, such as DWT, LWT, DCT, and FFT, prior to embedding the secret message. One advantage of frequency domain techniques over spatial domain techniques is their ability to resist steganalysis methods and signal processing manipulations. However, the transformation into the frequency domain is computationally complex.

## 3. Literature Survey

**Yueh-Peng Chen et. al:** In these days machine learning, deep learning playing very crucial role to execute diverse application in different domain. This paper based on deep learning technology which developed a model to find out watermark copyright and this process is called as WMNet. As we know for developing deep learning model fundamental requirement is data amount and it must be very high so that model can be predict accurate result otherwise accuracy will be degraded. In developing WMNet a specific procedure carried out to produce huge amount of distorted watermark and after that it collected so that training data can be formed [2].

**Ferda Ernawan et al:** This article depicted the concept of block-based Tchebichef watermarking method which helps to defend exclusive rights. In this process first, host image is segmented into blocks with non-overlapping and then Tchebichef instants designed for every slab. The watermarks are entrenched into blocks with help of lesser optical randomness [4].

**Piyush Pandey et al:** This paper depicted the concept to improve presentation of watermarking system using WHT method especially in YCbCr colour space by implementing integrated techniques that is LWT & SVD. The implementation procedure is very complex and every stage is tested very well so that accuracy will be better.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 14, No. 1, 2023, p.117-123
https://publishoa.com
ISSN: 1309-3452
YCbCr colour space is especially considered due to its de-correlation possessions to augment relationship between watermarked, cover images [6].

**Rajeev Dhanda et al:** Walsh Hadamard Transform domain approach in YCbCr color space using the unique combination of 2–Level Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD). All stages of the system are tested. YCbCr color space is used to make use of its decorrelation property to increase the correlation between host and watermarked final image. LWT stage selectively uses the detail coefficients of the 2–dimensional LWT of an image. After applying LWT we apply WHT (Walsh Hadamard Transform) to find the WHT coefficient and at the final we apply SVD on each coefficient to get the final watermarked image. Through this method we find the increased PSNR value [8].

**Rishi Sinhal et al:** Digital medical images play a crucial role in providing valuable information about a patient's health and are highly valuable for accurate diagnosis. Any alteration, even minor, in medical images, particularly in the region of interest (ROI), can potentially misguide doctors and healthcare practitioners when determining the appropriate course of treatment. Extensive experimentation has demonstrated that this specific technique exhibits exceptional imperceptibility, robustness, and tamper detection capabilities, while also enabling precise localization of tampered areas and achieving flawless recovery of the ROI with 100% reversibility [1].

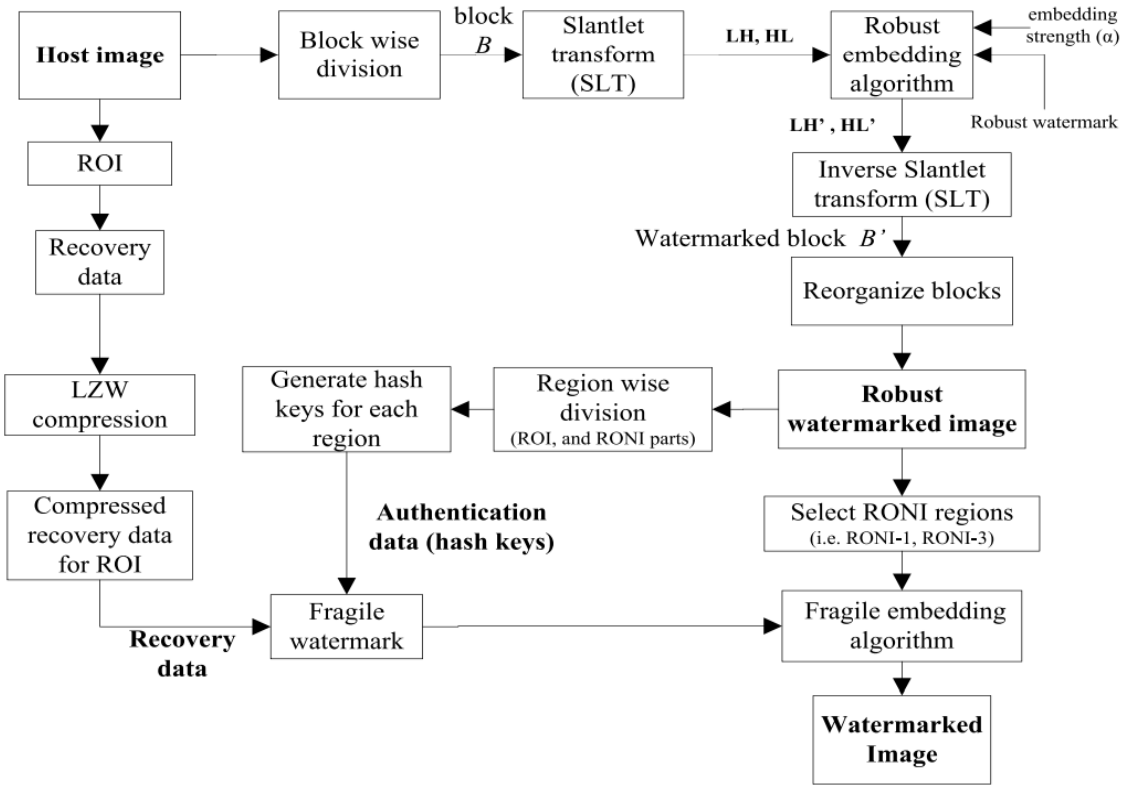


**Fig.3:** The Hybrid approach for watermark embedding process [1].

**D.Vaishnavia et al:** This paper presented two different techniques for toughness and indistinguishable image watermarking using RGB colour space. While implementing first technique, gray sca1e of watermark is entrenched on b1ue colour channe1. After that in second procedure, b1ue colour channe1 elements of watermark are entrenched on blue color channel elements of swarm image. After executing both processes SVD is engaged on the b1ue channel of host image to recover SV and watermark is entrenched in these SV. Overall examination of implemented method analysed by two parameters that is NC and PSNR [13].

**R Ansari et al:** A transform domain approach in YCbCr color space for enhancing the performance of a watermarking system, employing the unique combination of 2–Level Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and Singular Value Decomposition (SVD). Individual stages of the system are

examined and an attempt is made to improve each stage. YCbCr color space is utilized to make use of its decorrelation property in order to improve correlation between original and watermarked image. DWT stage selectively utilizes the horizontal and vertical detail coefficients of the 2–dimensional DWT of an image [18].

**Table I: Comparative Analysis of Different Frequency Domain and Spatial Domains Watermarking Techniques**

| Algorithm | Advantages | Disadvantages |
|---|---|---|
| **DFT** | DFT is rotation, scaling and translation (RST). Therefore, it is used to recover from geometric distortions. | Complex implementations.<br>Computing cost may be higher. |
| **DWT** | Higher compression ratios<br>Avoid blocking artifacts<br>Non-essentially to divide the input coding into non-overlapping 2-D blocks<br>Allow good localization both in spatial and time frequency domains | DWT uses larger DWT basis function<br>Cost of computing may be higher.<br>Compression time may be longer.<br>Noise may appear near the |
| **LWT** | DWT limitations are overcome by LWT algorithm<br>It reduces the computation time and speed up the computation process. | It consists three segments: Splitting, prediction and updating therefore to implement is little complex |
| **DCT** | More robust against digital processing operations.<br>Watermark cannot be removed by any attacks because of embedding. Water-mark into middle frequency coefficient. | Certain higher frequency components tend to be suppressed during the quantization process.<br>Block wise DCT destroys the invariance properties of the system.<br>Vulnerable to crop-ping, scaling. |
| **LSB** | Low degradation of image quality.<br>Easy to implement and understand.<br>High perceptual transparency. | Very sensitive to noise.<br>Vulnerable to cropping, scaling attacks.<br>Very less robust against attacks. |
| **Correlation** | Increases the robustness of watermark by increasing the gain factor. | Due to very high increment in gain factor, image quality may decrease. |
| **Patchwork** | High level of robustness against many types of attacks. | Very small amount of in-formation can be hidden. |

## 4. Watermarking Applications

Watermarking techniques are widely employed in various domains to ensure data security. Some of the domains where this technique is utilized include copyright protection, entertainment and data authentication, medical science, and defense. Digital image watermarking finds extensive application in areas where digital images are used. Specifically, it is applied in entertainment, copyright protection, content authentication, defense, and medical science [19-20]. The following are a few application areas where digital image watermarking is prominently depicted:

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 14, No. 1, 2023, p.117-123
https://publishoa.com
ISSN: 1309-3452


**Fig.4:** List of watermarking applications

- **Copyright Protection:** Digital watermarking techniques are employed to identify and protect copyright ownership. Watermarks containing metadata can be embedded in digital data to identify the copyright owners.
- **Medical Applications:** Watermarking techniques find extensive use in the medical domain. For instance, in medical imaging, digital watermarks can be used to print crucial patient information, such as name and age, on MRI scans and X-ray reports. This helps in avoiding mix-ups and potential casualties in case the reports are unintentionally combined.
- **Digital Fingerprinting:** Watermarking is utilized for digital fingerprinting, which aids in identifying the genuine identity that breaches license agreements and illegally distributes copyrighted data in copyright protection applications.
- **Content Archiving:** Digital data is typically identified by file names, which can be easily changed, making it a delicate process. To address this, object identifiers are inserted into the data, reducing the possibility of tampering.
- **Broadcast Monitoring:** Watermarking techniques are crucial in profit-oriented advertisement broadcasting for broadcast monitoring purposes. Advertisers need to know if their advertisements have been aired, if they were aired at the right time, and for how long.
- **Tamper Detection:** Delicate watermarking can be inserted into digital data to identify tampering attempts. If there is degradation in the watermark, it indicates that the data has been modified and cannot be trusted.

## 5. Conclusion

In today's digital landscape, preserving the confidentiality of individuals and securing their critical information has become of utmost importance. Consequently, several robust techniques, including cryptography, watermarking, steganography, and more, can be utilized to safeguard valuable data on the internet. This review paper explores a range of frequency domain and spatial domain techniques. Among them, the LWT technique is highlighted for its numerous benefits, such as a higher compression ratio, the ability to avoid blocking artifacts, and fast computational speed. Additionally, the paper covers various types of watermarking classifications, providing insights into their applications and characteristics.

## 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.