Digital Image Watermarking

Prof. Akshay Loke
Assistant Professor
Department of Information Technology
Vidyalankar Institute of Technology
akshay.loke@vit.edu.in

Hardik Parate
BE in Information Technology
Vidyalankar Institute of Technology
hardik.parate@vit.edu.in

Rohit Kute
BE in Information Technology
Vidyalankar Institute of Technology
rohit.kute@vit.edu.in

Raj Chaudhari
BE in Information Technology
Vidyalankar Institute of Technology
raj.chaudhari20@vit.edu.in

***Abstract*— Digital watermarking has become an essential method for encrypting multimedia files by adding undetectable data. In this work, we present a novel approach to digital watermarking that makes use of the Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) methods. By combining these methods, robustness against different types of attacks can be achieved while preserving excellent perceptual quality. Our approach ensures resilience and invisibility by embedding the watermark in the singular values that are obtained from the decomposition of DWT subbands. The outcomes of the experiments show that the suggested strategy is more efficient and effective than the current techniques when it comes to maintaining image quality and being resistant to common image processing threats.**

I INTRODUCTION

Nowadays, the majority of people utilize the Internet to post pictures and videos of their daily activities on sharing websites and social media. Since they are dispersed throughout the Internet, data are open to unwanted access. The ease of access to the Internet exacerbates intellectual property violations, which are made possible by such unlawful access. With recent technical improvements, there has been an increase in the unlawful use, misappropriation, and misrepresentation [1] of digital data. Copyright violations and misappropriations are seen as the main dangers. Owing to the massive volume of material that is exchanged, copyright infringement of this kind are frequently difficult to trace on the Internet. Moreover, thousands of lawsuits seeking ownership verification are being brought in courts as a result of these infringements. The key to pursuing a copyright violation lawsuit is having the capacity to demonstrate who owns an image or other digital media. However, if digital data is not registered in an intellectual property registry—which is expensive for those who create digital content—there is no recognized standard to demonstrate ownership of such data. Currently, digital watermarking is a widely accepted technique for demonstrating ownership. A collection of factors control the quality of watermark embedding into digital data. These factors include the following. These include the embedded watermark's adequate capacity, robustness against potential attacks, and inability to corrupt the original data. With an informed (non-blind) detector based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD) for color images, the technique described in the study constitutes an undetectable watermarking scheme for color images. It is demonstrated empirically that the watermarks implanted by the algorithm meet the aforementioned quality requirements.

The remainder of the paper is structured as follows. Section II provides the related work and followed by the proposed method in Section III. Section IV consists of the Performance Metrices, In Section V we have Experimental Evaluation and this paper concludes in Section VI.

II REVIEW OF RELATED WORKS

Review of literature survey has been conducted on discrete wavelet transformation (DWT), discrete cosine transform (DCT) combined with singular value decomposition (SVD) techniques for hiding information in digital color images.

In [1] Paper proposes a novel watermarking technique for color images to protect digital multimedia data from unauthorized

access. It uses a unique combination of HL sub-band of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The technique adds singular matrices obtained from SVD to the DWT applied watermark image, enhancing its quality. Experimental results show promising performance on benchmark test images.In [2] The digital information revolution has brought both advantages and challenges in protecting ownership and preventing unauthorized manipulation of digital media. Watermarking is a key method for copyright protection, hiding proprietary information in digital media. This paper presents a robust image watermarking algorithm using DWT and SVD to embed two watermarks in the HL and LH bands of the host image. Simulation evaluation demonstrates the technique's ability to withstand various attacks.

In [3] Paper proposes a watermarking algorithm for color images using Discrete Wavelet Transform, Discrete Cosine Transform, and Singular Value Decomposition (DWT-DCT-SVD). The algorithm converts the host color image from RGB to YUV, applies a layer of DWT to the luminance component, divides the low frequency into blocks, and conducts SVD with each block. The algorithm effectively resists common watermark attacks.

The image is converted to K level in [4] using the DWT approach.

The watermark is hidden and the middle frequency band LH and HL are SVD converted. A similar distributed discrete wavelet transform approach is used to incorporate the watermark in the high and low frequency bands (DDWT). Both algorithms have undergone attack testing and have demonstrated their resilience to cropping attempts. The suggested strategy is strong against attacks like rotation, Sharpness, Histogram Equalization, Contrast Adjustment, and Gaussian Noise since it takes advantage of the SVD watermarking technique.

In [5], an image is subjected to a three-level DWT decomposition in order to obtain ten bands of frequencies. To embed the watermark, the ten bands of frequency coefficients are SVD converted. It is discussed a new watermarking strategy for images that uses the wavelet domain's Singular Value Decomposition (SVD) and Human Visual System (HVS). Its improved performance for scaling attacks, cropping, and compression is demonstrated by experimental findings. In [6], a picture is transformed into bands of varying frequencies using the two-level decomposition of DWT. A certain band is then chosen and divided into blocks of a certain size.4x4 for data embedding. Every block has undergone SVD transformation, and a watermark is concealed within each block's diagonal matrix. The correlation factor NC is used to calculate how similar the extracted watermark from the attacked image is to the original watermark. The algorithm demonstrates that the watermarking approach works better than the traditional DWT algorithm in terms of robustness against Gaussian noise, compression, and cropping assaults when DWT is paired with SVD technique.

In [7] Paper proposes a hybrid image watermarking technique that combines various transforms like RDWT, DCT, SVD, and trigonometric functions to create a non-blind, robust, and reversible scheme. The algorithm is tested on various formats and intensity watermarks, showing robustness against various attacks and maintaining indistinguishable visual quality even when distorted. This technique can be used for copyright protection, ownership problems, content verification, and authentication. In [8] The proposed watermarking technique combines DWT and DCT, offering low frequency watermarking with weighted correction. DWT has excellent spatial localization, frequency spread, and multi-resolution characteristics, similar to the human visual system. DCT provides compression and DWT offers scalability. Watermark bits are embedded in the low frequency band of each DCT block of selected DWT sub-band. Weighted correction improves imperceptibility. The algorithm preserves superior image quality and robustness under various attacks, unlike other approaches.

In [9] Digital image watermarking is widely used due to its accessibility and protection against illegal use. This paper compares two digital image watermarking techniques based on DCT, DWT, and SVD. Scheme-A uses a conventional DCT-DWT-SVD hybrid watermarking technique, while scheme-B uses an image scrambling method. The quality of the extracted watermark is measured using normalized correlation (NC) between the original and distorted watermarked image. The preferred technique achieves higher NC values than the conventional scheme. In [10] Internet technology has revolutionized our lives, but duplication and unauthorized use of information pose significant threats. Techniques like digital watermarking, steganography, and cryptography have been introduced to combat these issues. Digital watermarking embeds secret data into digital signals, using techniques like Least Significant Bit and Patch Work Algorithm. A new method combining DCT and DWT techniques for digital watermarking is proposed, enhancing image quality and reducing the Mean Square Error.

III PROPOSED METHOD

In this research, we offer a new approach to watermark digital images utilizing Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). The goal of this technique is to add undetectable watermarks to photos while maintaining security against frequent assaults. Our solution balances security and invisibility by using SVD for feature extraction and DWT for frequency analysis. We show that our approach effectively prevents illegal use or modification of digital photos through experimental validation.

1. DWT

The Discrete Wavelet Transform (DWT) is a signal processing technique that decomposes a signal into approximation and detail coefficients across multiple scales. This procedure involves downsampling an image, first for the rows and then for the columns, after it has been through both high pass and low pass filtering. The original image is first broken down by the filter into four multi-resolution, non-overlapping subband images using DWT. These four images consist of one low-frequency component (LL) termed an approximate sub-image that converges of strength

 DOI: 10.55041/IJSREM32204

original image and three high-frequency parts (HL, LH, and HH) called detail sub-images. The stability of the approximation sub-image is superior to the detail sub-images, and it receives the majority of the image's energy. In a 2D application, do DWT in both the vertical and horizontal directions in order to break down an image into its component levels. The level numbers in the multi-level decomposition procedure into the DWT domain are provided as the secret key.

2. SVD

Because of its stability, Singular Value Decomposition (SVD) provides a stable domain for watermark embedding in digital image watermarking. Consider the image's subband as a matrix. SVD of an image is given by $A = USV^T$ in which U (which represents row information), S (which contains diagonal singular values), and V^T (which represents column information). The essential energy distribution of the image is captured by the solitary values in S. During watermark embedding, the watermark information is invisibly absorbed by gently altering these values. This is useful because, in contrast to directly changing pixel values, SVD manipulations are less obvious and, at the same time, they remain resistant to attacks that could change the structure of the image.

A) Embedding Process

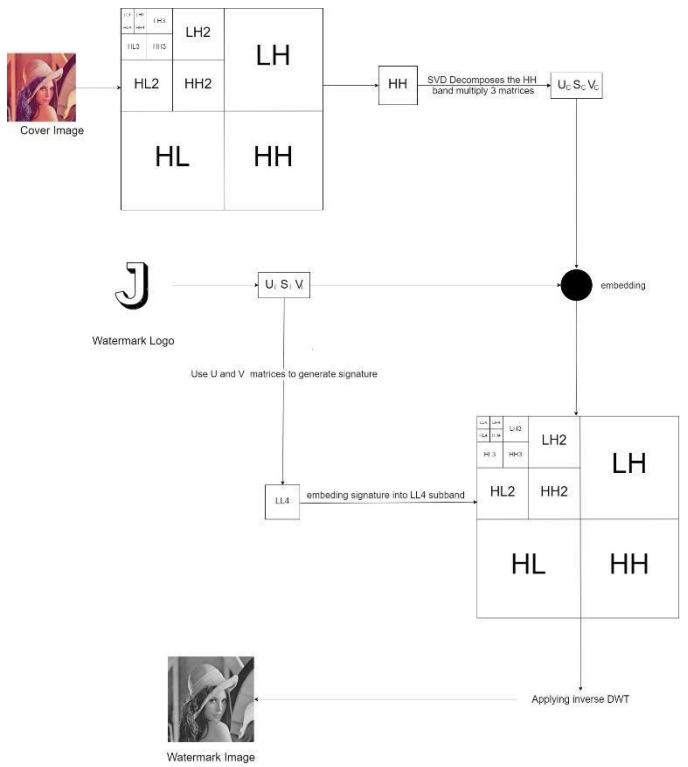

Fig 1

1. Input
   - The original image that the watermark will be inserted in is the input, or Cover Image (CI).
   - The picture or pattern to be used as a watermark is called the Watermark Logo (WL).
   - Key (K): A secret key that's embedded during the process.
2. Wavelet Transformation
   - To divide the Cover Image (CI) into the LL (Low-Low), HL (High-Low), LH (Low-High), and HH (High-High) bands, apply the Haar Wavelet Transform.
3. Additional LL Band Decomposition:
   - Apply the Haar Wavelet Transform to further break down the LL band that was acquired in the preceding step up to the fourth level. The LL4, HL4, LH4, and HH4 bands are the outcome of this.
4. Singular Value Decomposition (SVD):
   - The HH4 band should be subjected to SVD.
   - Likewise, use SVD to break down the Watermark Logo (WL) and get the matrices Uw, Sw, and Vw.
5. Swapping Singular Values:
   - Swap the Watermark Logo's singular values for the HH4 band's singular values (diagonal components of Sw). By doing this, it is ensured that the image's high-frequency components contain the watermark information.
6. Signature Generation:
   - Utilizing the matrices Uw and Vw from the Watermark Logo's SVD, generate a signature. The secret key (K) is used to generate the signature.
7. Embedding the signature:
   - Insert the created signature into the LL4 band. This can be accomplished in a number of ways, including by performing transformations or changing particular coefficients.
8. Inverse Wavelet Transformation:
   - To create the watermarked image, apply the Inverse Haar Wavelet Transform to the modified LL4, the original HL4, LH4, and modified HH4 bands.
9. Output:
   - The produced signature and the watermarked image are the results of the embedding operation.

B) Extraction Process

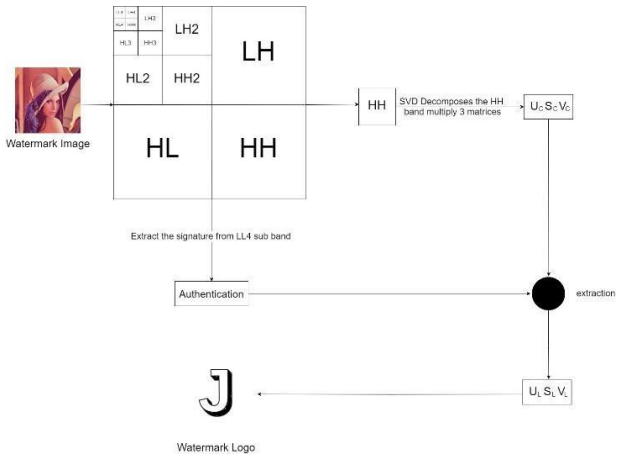

Fig 2

1. Input
   - Watermarked Image (WI): The watermarked image that is integrated in the image.
   - Watermark Logo (WL): The watermark design from the beginning.
   - Key (K): The embedding process's secret key
   - Signature Authentication (SA): A flag that designates whether the signature has to be verified at the time of extraction.
2. Wavelet Transformation:
   - Wavelet Transformation: To divide the Watermarked Image (WI) into the four sub-bands of LLw, HLw, LHw, and HHw, apply the Haar Wavelet Transform.
3. Additional LLw Band Decomposition:
   - Apply the Haar Wavelet Transform to further break down the LLw band that was acquired in the preceding phase up to the fourth level. LLw_4, HLw_4, LHw_4, and HHw_4 bands are the outcome of this.
4. Singular Value Decomposition (SVD):
   - The Watermark Logo (WL) may be broken down using Singular Value Decomposition (SVD) to produce the matrices Uw_x, Sw_x, and Vw_x.
5. Signature Generation:
   - Using the secret key (K) and the matrices Uw_x and Vw_x from the Watermark Logo's SVD, generate a signature.
6. Signature Authentication:
   - To confirm authenticity, compare the extracted signature with the generated signature if Signature Authentication (SA) is enabled.
6. Singular Value Extraction:
   - Take the singular values out of the Watermarked Image's HHw_4 band.
7. Watermark Reconstruction:
   - Utilizing the recovered singular values and the matrices Uw_x and Vw_x from the Watermark Logo's SVD, reconstruct the watermark.

8.Output:The extracted watermark logo and, if desired, the created and rebuilt signatures are the results of the extraction procedure.

IV PERFORMANCE MATRICES

1. MSE

For calculating the Mean Squared Error (MSE), we have to concentrate on original value and values received after the experiment. With the help of the following formula, it can be calculated

$$MSE = \frac{1}{MN}\sum_{I=1}^{M}\sum_{J=1}^{N}((f(i,j) - f(i,j))^2$$

Here M and N are the height and width of the image respectively. And f(i,j) is the pixel value of original image and f(i,j) is the pixel value of embeded image.

2. PSNR

This proportion is generally utilized as value capacity between the original image and the image retrieved after the watermark. Here the value capacity is the amount of information which are inserted to cover image. More capacity means more information can be hidden. PSNR is used to calculate the loss in quality of the image received after watermark I*concerning the original image I. It is given as

$$10log_{10}\left(\frac{MAX^2}{\frac{P1}{MSE}}\right)$$

Here I_{max} is the higher pixel value of the image I. For an 8-bit image, it is 255.

3. Correlation Coefficient

$$r = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2 \sum_{i=1}^{n}(Y_i - \bar{Y})^2}}$$

In digital watermarking, the correlation coefficient (ρ) represents the strength of linear connection between two variables. In the context of watermarking, it gauges how similar the recovered watermark signal (W') is to the original watermark signal (W). This correlation coefficient, which provides a numerical indication of how successfully the watermarking process retained and recovered the embedded data, can be used to assess the similarity between the original and returned watermarks. association coefficients close to 1 show a strong positive association and imply accurate watermark extraction, whilst values closer to 0 indicate a weaker connection and potential decline in watermark detection accuracy.

V EXPERIMENTAL EVALUATION

The proposed method's experimental results will be shown in this section. In MATLAB, the algorithm is implemented. The typical RGB color is utilized as the cover picture in the algorithm.Image size of Lena is 512*512. The watermark image is binary watermark image of size 64*64.

Fig3(a) Cover Image

Fig3(b) Watermark logo

After water marking:


Fig4(a) Watermarked Image

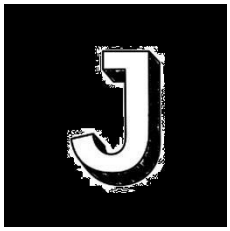
Fig4(b) Extracted logo

ATTACKS

1. MEAN

The watermarked image in Fig. 4(a) is transformed into Fig. 5(a) after adding Mean attack, Fig. 5(b) is the watermark image extracted from Fig. 5(a). Where correlation is 0.59708


Fig 5 (a)


Fig 5 (b)

2. MEDIAN

The watermarked image in Fig. 4(a) is transformed into Fig. 6(a) after adding Median attack, Fig. 6(b) is the watermark image extracted from Fig. 6(a). Where correlation is 0.58071


Fig 6 (a)


Fig 6 (b)

3. NOISE

The watermarked image in Fig. 4(a) is transformed into Fig. 7(a) after adding Noise attack, Fig. 7(b) is the watermark image extracted from Fig. 7(a). Where correlation is 0.44993


Fig 7 (a)

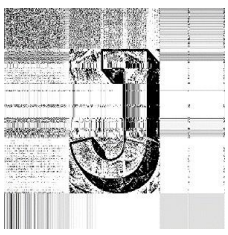
Fig 7 (b)

4. ROTATION

The watermarked image in Fig. 4(a) is transformed into Fig. 8(a) after adding Rotation attack, Fig.8(b) is the watermark image extracted from Fig. 8(a). Where correlation is 0.45290


Fig 8 (a)

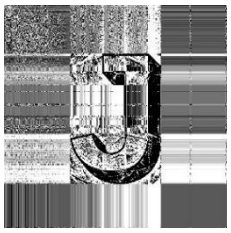
Fig 8 (b)

5. SHEAR

The watermarked image in Fig. 4(a) is transformed into Fig. 9(a) after adding Shear attack, Fig. 9(b) is the watermark image extracted from Fig. 9(a). Where correlation is 0.54721


Fig 9 (a)


Fig 9 (b)

6. CROP

The watermarked image in Fig. 4(a) is transformed into Fig.10(a) after adding Crop attack, Fig. 10(b) is the watermark image extracted from Fig. 10(a). Where correlation is 0.53778


Fig 10 (a)


Fig 10 (b)

VI CONCLUSION

This research proposed a robust approach for image watermarking utilizing DWT and SVD. In this case, the watermarking image is created by combining the singular values discovered through the application of SVD to the sub-band that is left behind after applying DWT to the original image with the unique values discovered from the application of SVD to the HH sub-band of DWT applied to the watermark image.The correlation coefficient,

PSNR, and MSE were used to assess the performance. The results of the simulation demonstrate how resilient this strategy is to different kinds of attacks.

ACKNOWLEDGMENT

I extend my sincere thanks to Professor Akshay Loke for his invaluable guidance and expertise, which have been instrumental in shaping the development of Digital Image Watermarking. Professor Akshay Loke's insights and mentorship have greatly contributed to the success of this project.

Furthermore, I would like to express my gratitude to Vidyalankar Institute of Technology for providing the necessary infrastructure and resources that made the development of Digital Image Watermarking possible. The support and facilities provided by Vidyalankar Institute of Technology have been essential in facilitating the implementation and execution of this project.

REFRENCES

[1] H. Joseph and B. K. Rajan, "Image Security Enhancement using DCT & DWT Watermarking Technique," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0940-0945,doi: 10.1109/ICCSP48568.2020.9182052.

[2] A. S. Yadav and S. Kumar, "Comparative Analysis of Digital Image Watermarking Based on DCT, DWT and SVD with Image Scrambling Technique for Information Security," *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, Lucknow, India, 2018, pp. 89-93, doi: 10.1109/CCTES.2018.8674135.

[3] K. Deb, M. S. Al-Seraj, M. M. Hoque and M. I. H. Sarkar, "Combined DWT-DCT based digital image watermarking technique for copyright protection," *2012 7th International Conference on Electrical and Computer Engineering*, Dhaka, Bangladesh, 2012, pp. 458-461, doi: 10.1109/ICECE.2012.6471586.

[4] Joseph, Anumol, and K. Anusudha. "Robust watermarking based on DWT SVD." *International Journal on Signal & Image Security* 1.1 (2013): 1-5.

[5] N. S. Naik, N. Naveena and K. Manikantan, "Robust digital image watermarking using DWT+SVD approach," *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 2015, pp. 1-6, doi: 10.1109/ICCIC.2015.7435653.

[6] He, Y., & Hu, Y. (2018). *A Proposed Digital Image Watermarking Based on DWT-DCT-SVD. 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC)*. doi:10.1109/imcec.2018.8469626

[7] Ying Yang, Xingming Sun, Hengfu Yang, Chang-Tsun Li, & Rong Xiao. (2009). A Contrast-Sensitive Reversible Visible Image Watermarking Technique. IEEE Transactions on Circuits and Systems for Video Technology, 19(5), 656–667. doi:10.1109/tcsvt.2009.2017401

[8] Jung-Chun Liu, Chu-Hsing Lin, and Li-Ching Kuo" A Robust full band image watermarking scheme" Proceedings on IEEE .2006

[9] 10Qiang Li, et al, "Adaptive DWT-SVD Domain Image Watermarking Using Human Visual Model" proceedings of 9th international conference on advanced communication Technology, Volume 3, pp:1947 - 1951, Feb.2007

[10] Ruth Buse Dili, Elijah Mwangi, "An Image Watermarking method based on the s ingular value transformation and the wavelet transformation "Proceedings on IEEE. 2007