ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 11, Issue 4, April 2024

A Invisible Watermark For Digital Images

Abdul Subhani Shaik, Lingala Akhila, Ganta Arun, Jadhav Sikindhar

Department of Electronics Communication & Engineering, CMR College Of Engineering & Technology,
Kandlakoya(V), Medchal(D), Hyderabad-501401, Telangana, India

ABSTRACT: Digital image watermarking is a critical tool for ensuring the security and authenticity of digital content in various applications. This study presents a comprehensive review of watermarking techniques specifically designed for digital images. Beginning with an overview of traditional methods encompassing spatial, frequency, and transform domain techniques, this review extends to recent advancements and emerging trends. Challenges, such as robustness against attacks, imperceptibility, and capacity for data embedding, were thoroughly analyzed. Real-world applications in multimedia forensics, copyright protection, and secure data transmission have been explored. Through this review, this paper aims to provide a thorough understanding of digital image watermarking techniques.

KEYWORDS: Discreet Wavelet Transform, Singular Value Decomposition, Embedding, Watermark

I. INTRODUCTION

In today's rapidly advancing technological landscape, the surge in demand for multimedia resources over the Internet has raised concerns regarding unauthorized access to such content. To counter this threat, the adoption of watermarking techniques is essential. Watermarking involves embedding one message into another, primarily to assert copyright ownership and conceal digital information. Typically, subtle and transparent watermarks often take the form of logos or text overlaid onto images or videos, serving as a protective measure against unauthorized access. They are prevalent in various media, including currency notes, photographs, bank checks, videos, and bond papers. Digital watermarking involves the embedding of data, known as watermarks, which can be subsequently extracted for ownership verification purposes. It ensures data integrity by inserting imperceptible and inseparable information into data. This process encompasses various methods and technologies designed to conceal information within digital media while maintaining imperceptibility to human observers. These embedded patterns, ranging in visibility, serve as markers of authenticity, quality, ownership, and source attribution. Operating within the realm of steganography, digital watermarking hides messages alongside content without being detected by public authorities or ordinary citizens. Hidden data can only be revealed using specific electronic devices that are capable of extracting the embedded message to ascertain its code. This study utilizes the transform domain method, The method used involves utilizing a combination of the discrete wavelet transform (DWT) and singular numerical and functional analyses, which was employed in this study. Wavelets in this transformation are sampled discretely, providing the benefit of capturing both frequency and location information. Unlike the Fourier Transform, DWT concentrates the signal energy into specific wavelet coefficients, which is beneficial for image compression purposes.

The original image is divided into four sub-bands that operate independently in the frequency and spatial domains as part of the Digital Wavelet Transform (DWT). The labels LL, LH, HL, and HH, respectively, designate these sub-bands. as seen in Figure 1.

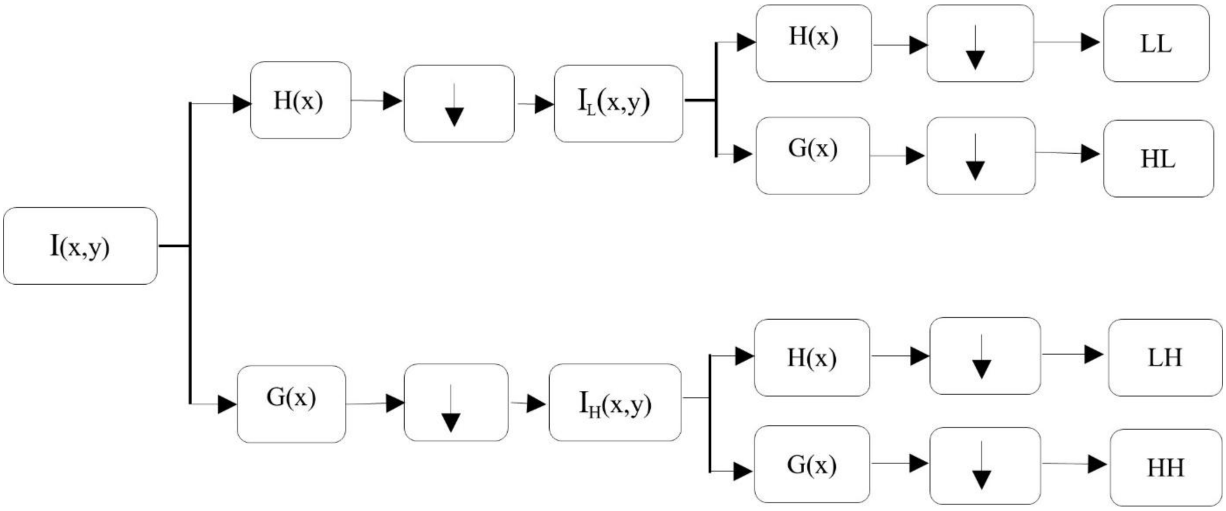


Figure 1: Subbands of discrete wavelet transform

Singular Value Decomposition (SVD) is a factorization technique in linear algebra that can be used on real or complex matrices. Image matrix A of size M×N is broken down into a product of three matrices using SVD, which represents an image as a matrix of scalar values: A = USVT Singular Value Decomposition (SVD) is used in the current scenario to decompose matrix A into three matrices: U (an M×M orthogonal matrix), S (an N×N diagonal matrix with singular values 1, 2,...,γ1,γ2,...,γn), and Vt (an N×N orthogonal matrix). Only the singular values γi, which are arranged so that η1>η2>η3>...>γr=ηn=0, where r is A's rank, are non-zero along the diagonal. When A stands for the pixel values of an image, this decomposition enables the image to be expressed as A=∑i=0$\alpha iui\ vi$ Information embedded in low-frequency components is extremely responsive to histogram modifications, such as gamma correction, contrast/brightness adjustments, and histogram equalisation, and decreases image distortions following embedding. Conversely, intermediate and high-frequency watermarking is generally more resistant to nonlinear deformations and noise addition. The Discrete Wavelet Transform's (DWT) overall robustness is improved by embedding several watermarks in its high- and low-frequency bands. The reason SVD is preferred is because it can preserve the singular values with little deviation, even when the image is subjected to small perturbations. 2. An image's singular values capture important algebraic characteristics.

II. SIGNIFICANCE OF THE SYSTEM

Copyright Protection: Watermarks help protect the intellectual property rights of creators by visibly or invisibly embedding ownership information into images. This discourages unauthorized use and distribution.
Content Authentication: Watermarks can be used to verify the authenticity and integrity of digital images. They serve as a digital signature, confirming that the image has not been altered or tampered with.
Brand Identity: Watermarks are often used by businesses and individuals to promote brand recognition and establish a visual identity. They can include logos, trademarks, or unique identifiers.
Deterrent to Unauthorized Use: Visible watermarks act as a deterrent against unauthorized use or reproduction of images. They make it clear that the image is protected and should not be used without permission.
Traceability: Watermarks can be used for traceability purposes, allowing creators to track the usage and distribution of their images across digital platforms.
Enhanced Trust: In professional and commercial contexts, watermarks can enhance trust and credibility. They signal to viewers that the image is authentic and associated with a legitimate source.

III. LITERATURE SURVEY

Watermarking is a commonly used technique that has been continuously improved through various approaches and applications [1]. This field has already been the subject of extensive research, which served as a basis for our contributions and technological breakthroughs in watermarking. Based on the widely used SSI metric, Zhang et al. [2] introduced the discrete wavelet transform-based Structural Similarity approach for picture quality assessment. However, this method functions largely in the pixel domain and incurs a significant processing expense when employed in the DWT domain. DWT is nonetheless used despite this because of its broad application, simplicity in use, and capacity to produce acceptable outcomes [3]. Vidyasagar et al. provided a thorough assessment of steganographic, and watermarking methods created especially for photos in a different study [4].

The survey provided a thorough analysis of both known and recently proposed approaches by classifying these techniques according to the domains in which watermark information is placed. For grayscale photos, Guan Jinyu et al. [5] presented a discrete wavelet transform-based digital watermarking technique. The technique they used showed excellent resilience to several types of attacks and watermark invisibility. In their discrete wavelet transform-based multiple watermarking systems, Raval Mehul S. et al. [6] placed special emphasis on embedding watermarks in low-frequency components for increased robustness. Discrete wavelet transforms and discrete Fourier transforms are combined in Xiangui Kang et al. [7] composite watermarking approach to fend off affine transform and JPEG compression attacks.

The techniques used for watermarking were founded on a training sequence and the spread spectrum approach is incorporated in the LL band of the discrete wavelet transform. In addition, Saied Amirgholipour and Ali Al-Haj et al. [8] Discrete wavelet transform and discrete cosine transform are combined in watermarking systems described by Kasmani et al. [9] to improve robustness and imperceptibility against signal-processing attacks. The DWT-SVD technique was introduced by Preeti Sharma et al. and Poonam et al. to address copyright difficulties. Sharma et al. used a hybrid transformation that concentrated on singular value alterations, while Poonam et al. [10] used a genetic algorithm in conjunction with a third-level DWT watermarking technique. An effective and self-synchronized audio watermarking technique was presented by Shaoquan Wu et al.[11], who included synchronisation codes and concealed data into the low-frequency coefficients of DWT. Xiang-Gen Xia and associates. Different approaches for incorporating discrete wavelet transform into watermark embedding on cover images were presented by Zhang et al.[12] and Wang et al.[13]. They presented a multiresolution watermarking technique in which the high- and middle-frequency bands of the DWT's coefficients were modified to include pseudo-random codes. This technique proved robust against common image distortions, and the amount of noise in the image determined how much watermark information could be recovered. They created a contour-based, semi-fragile image watermarking system in. Using this approach, a filtered contour picture is produced by first using a 2-level DWT and then a Canny edge detector to split the original image's Y-component into 4 × 4 blocks. In order to remove spatial relativity from the watermark image, an Arnold transform was also performed. Finally, watermark embedding was achieved by altering the chosen middle DWT coefficients in accordance with the relevant watermark bits. On the other hand, a unique method that included chaos was used with wavelet transformation to embed the watermark into the host image's singular values of the DWT subbands. In the DWT sector, Roland Kwitt et al. [14] presented a lightweight technique for computationally efficient additive watermark detection. Using DWT and singular value decomposition, Guohui Li et al. [15] introduced a sorted neighbourhood technique to identify duplicated regions in picture forgeries. These many research initiatives have had a big impact on how the digital watermarking approach is adopted and used.

IV. PROPOSED METHODOLOGY

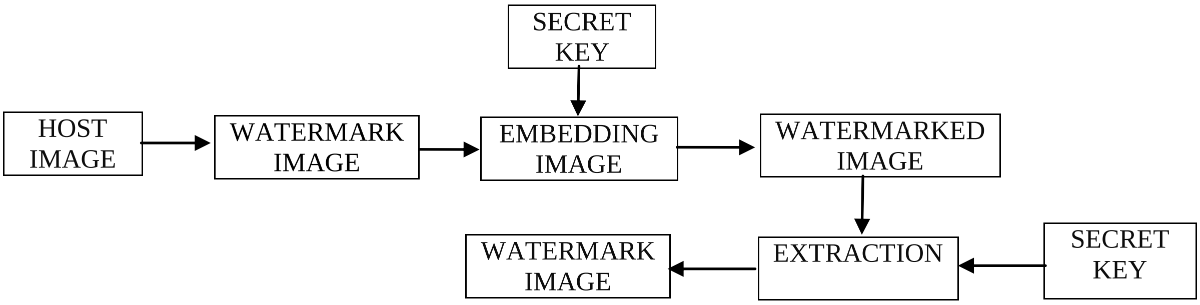


Figure 2: Proposed block diagram

Watermark Embedding Procedure: Here is a breakdown of the steps involved in adding the watermark for this project: Select the host and add a watermark on the pictures. b. Transform the original and watermarked photos using the Discrete Wavelet Transform (DWT). The original and watermarked images' LL (low-low) sub-bands should be subjected to Singular Value Decomposition (SVD). d. Use the watermarking algorithm on the two photos to create the watermarked image that results.

The planned procedure for extracting the watermark is outlined below:
a) Select host and watermarked images.
b) Apply the Discrete Wavelet Transform (DWT) to both the original and watermarked images.
c) Perform Singular Value Decomposition (SVD) on the LL (low-low) sub-band of both the original and watermarked images.
d) Execute the extraction algorithm on the two images to generate the resulting watermarked image.

V. EXPERIMENTAL RESULTS

Implementing the watermarking algorithm allowed us to evaluate and compare the quality of both the embedding and processes.

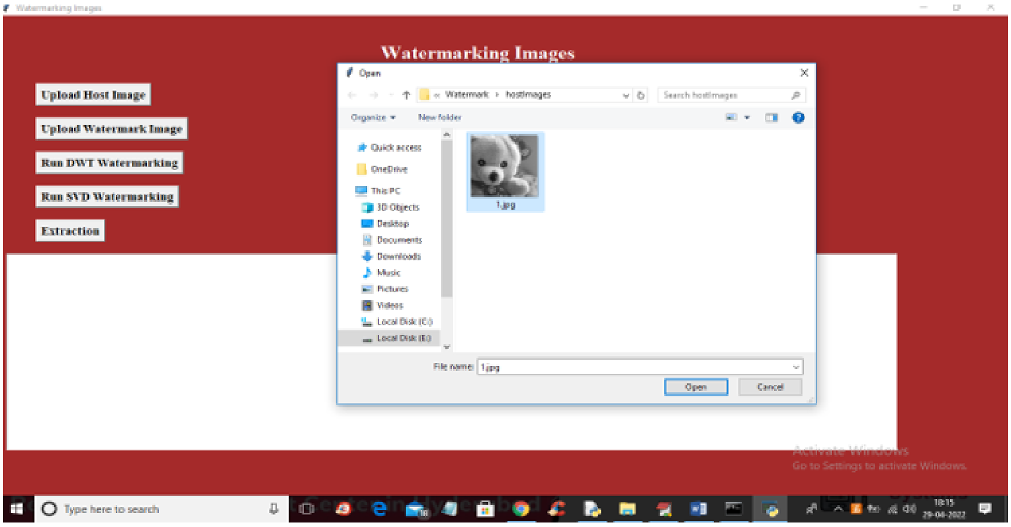


Figure 3: Uploading the Host image

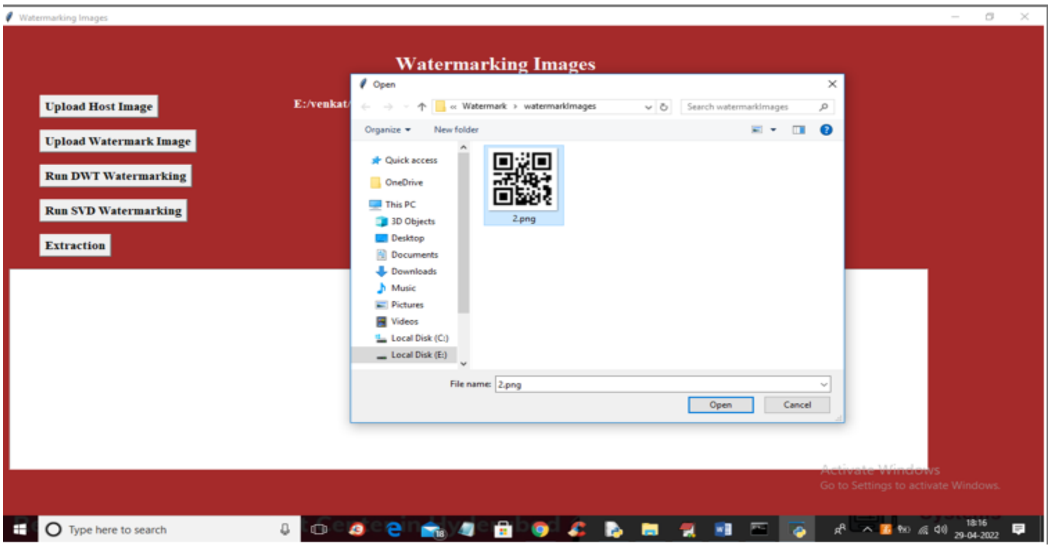
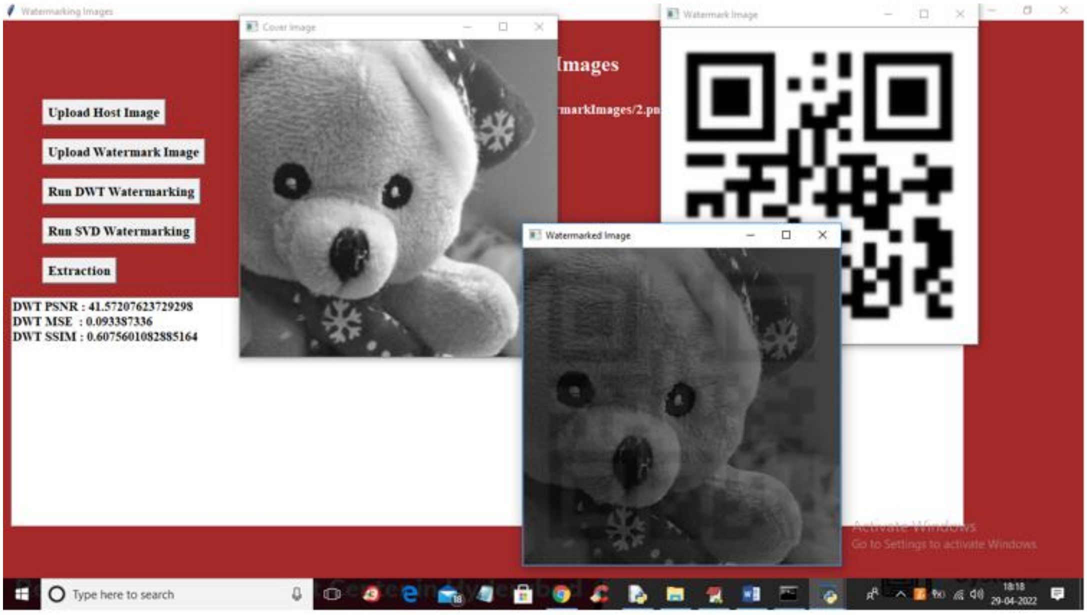


Figure 5: Uploading the Watermark image.

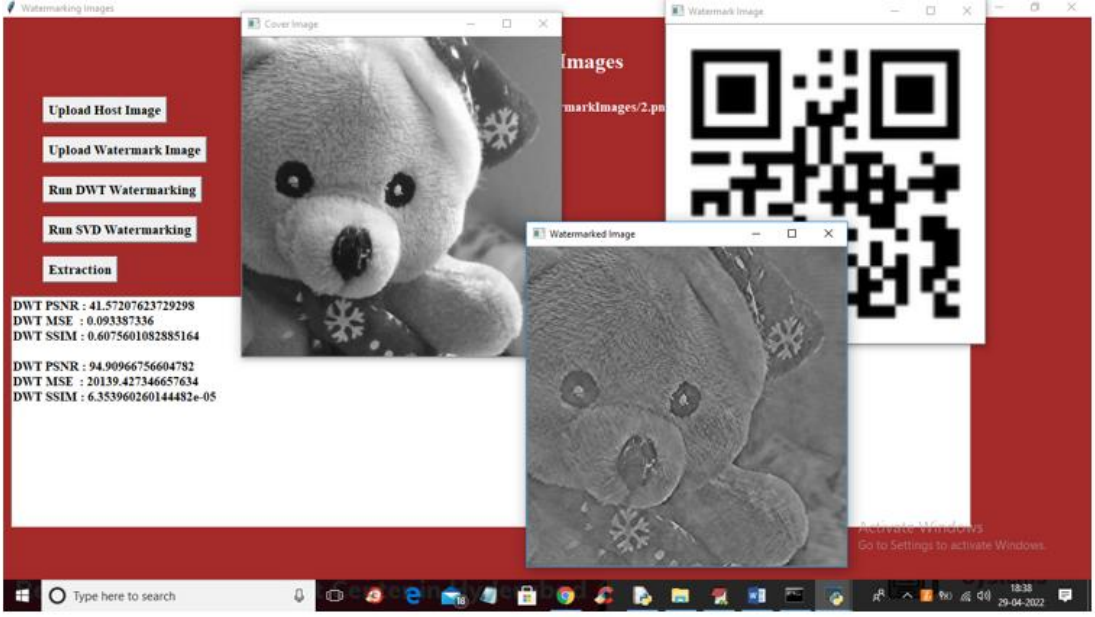
In the above image in the white colour text, we can see the watermark image is loaded now click on the ‘Run DWT Watermarking’ button to embed the image and get the below output.



```
DWT PSNR : 41.57207623729298
DWT MSE  : 0.093387336
DWT SSIM : 0.6075601082885164
```

Figure 7: Watermarking using DWT

In the above image first image is the cover image the second is the watermarking image and 3rd is the embedded watermarked image and we can see DWT PSNR and other values in the text area for DWT. Now click on the ‘Run SVD Watermarking’ button to embed watermarking using SVD.

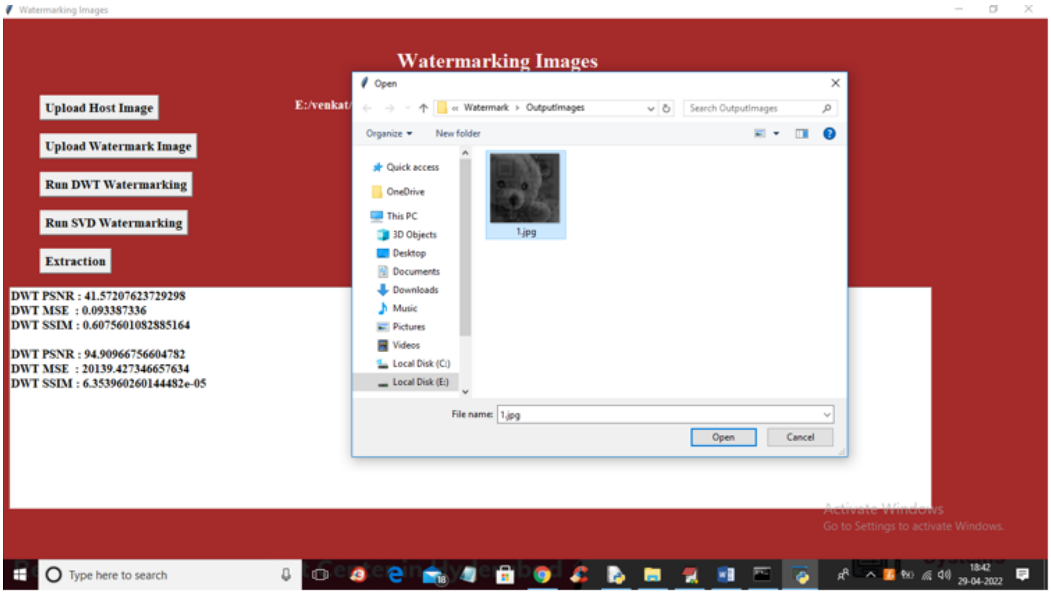


```
DWT PSNR : 41.57207623729298
DWT MSE  : 0.093387336
DWT SSIM : 0.6075601082885164

DWT PSNR : 94.90966756604782
DWT MSE  : 20139.427346657634
DWT SSIM : 6.353960260144482e-05
```

Figure 8: Watermarking using SVD

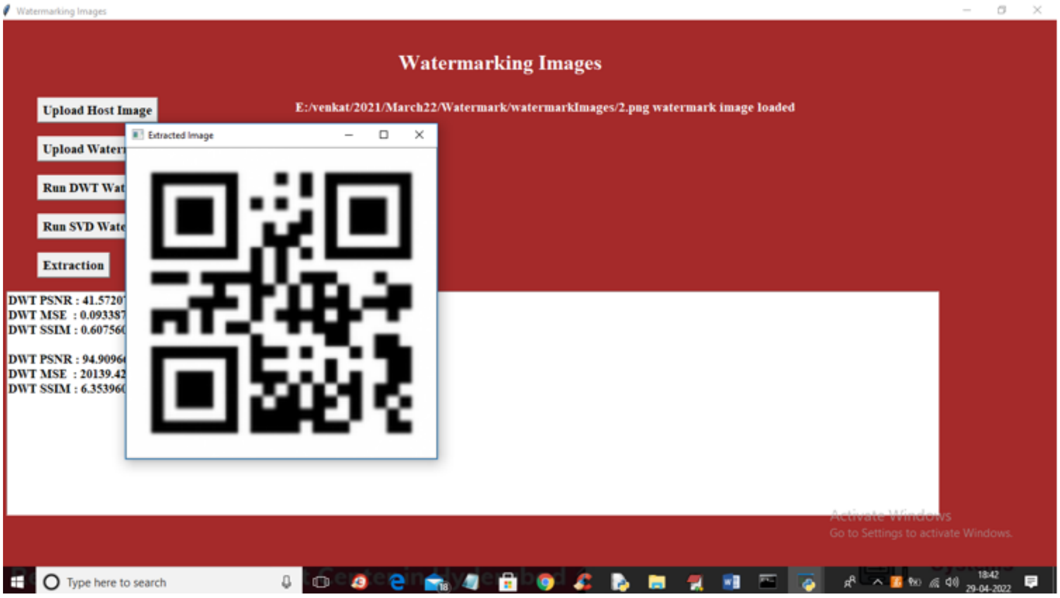
In the above image first image is the original image and second is the watermark image and 3rd is the embedded watermarked image using the SVD algorithm and we can see PSNR, MSE and SSIM for both SVD and DWT. PSNR must be closer to 100% to consider as high quality image and MSE must be closer to 0 and SSIM must be closer to 100. Now click on ‘Extraction’ button to upload Watermarked image and then extract embedded image from it.



```
DWT PSNR : 41.57207623729298
DWT MSE  : 0.093387336
DWT SSIM : 0.6075601082885164

DWT PSNR : 94.90966756604782
DWT MSE  : 20139.427346657634
DWT SSIM : 6.353960260144482e-05
```

Figure 9: Extracted original image



```
E:/venkat/2021/March22/Watermark/watermarkImages/2.png watermark image loaded
```

```
DWT PSNR : 41.5720
DWT MSE  : 0.093387
DWT SSIM : 0.60756

DWT PSNR : 94.9096
DWT MSE  : 20139.42
DWT SSIM : 6.35396
```

Figure 10: Extracted watermark

In the above image, we can see the extracted image and similarly, you can upload any image and get output.

VI. CONCLUSION

This study explores various watermarking techniques, culminating in the proposal of a fundamental approach known as DWT-SVD, specifically tailored for RGB images. The implemented algorithm was tested under diverse attacks, which allowed performance evaluation. The study has provided the following key insights: a) Image segmentation into different bands to facilitate watermark embedding. b) Utilization of various filters, such as Haar, Sym4, Db5, and Bior for watermarking, with different filters selected based on specific scenarios. c) Integration of Singular Value

Decomposition (SVD) with Discrete Wavelet watermarking. Transform (DWT) in digital d) Examination of structural similarity (SSIM) as a novel method for image quality assessment, noted for its robust performance and straightforward calculations. e) Exploration of genetic algorithms in conjunction with DWT to determine optimal locations for watermark insertion in host images. Further enhancements can be achieved through the application of Fuzzy Logic or Neural Network methods, thereby improving optimization and performance.

REFERENCES

[1] Yang, Lai-Man Po, Wen-Rui Gao, and Chun-Ling. 'Discrete wavelet transform-based structural similarity for image quality assessment' was the title of an article that appeared in the journal Image Processing in 2008.IEEE 15th International Conference on IEEE (2008), ICIP 2008.

[2] Potdar, Elizabeth Chang, Song Han, and Vidyasagar M. "A survey of digital image watermarking techniques." Third IEEE International Conference on Industrial Informatics, INDIN'05, IEEE, 2005.

[3] Mei Rui, Guan, Zhang Wenying, and Jinyu. The work was presented at the 2010 2nd International Conference on Computer and Automation Engineering (ICCAE) with the title "Research of digital watermarking based on wavelet transform." IEEE, Vol. 4, 2010.

[4] Rege, P. P., and M. S. Raval. The Conference on Convergent Technologies for the Asia-Pacific Region, TENCON 2003, Vol. 3, IEEE, 2003, featured a paper titled 'Discrete wavelet transform based multiple watermarking technique'.

[5] Xiangui et al. and Kang et al. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression." 13.8 (2003): 776-786. IEEE Transactions on Circuits and Systems for Video Technology.

[6] Saeed K. Amirgholipour, Ahmad Reza Naghsh-Nilchi, and JDCTA 3.2 (2009): 42-54. "Robust Digital Image Watermarking Based on Joint DWT DCT."

[7] In Convergence and Hybrid Information Technology, 2008, ICCIT'08 Third International Conference on the Vol. 2, IEEE, Kasmani, Saied Amirgholipour, and AhmadrezaNaghsh Nilchi, "A new robust digital image watermarking technique based on joint DWT-DCT transformation."

[8] Jain, Tapan, and Preeti Sharma. In 2014, the IEEE International Advanced Computing Conference (IACC) hosted a paper titled "Robust digital watermarking for coloured images using SVD and DWT technique," which was later published by IEEE.2014 IEEE.

[9] The Poonam, P., et al. International Conference on the "Efficient genetic algorithmbased image watermarking using DWT-SVD techniques." IEEE, 2012. International Conference on Computer Science (ICCS), 2012.

[10] "Efficiently self-synchronized audio watermarking for assured audio data transmission," Wu, Shaoquan, et al. 51.1 (2005) IEEE Transactions on Broadcasting: 69-76.

[11] Gonzalo R. Arce, Charles G. Boncelet, Xia, Xiang-Gen, and Boncelet. IEEE, 1997. Proceedings of the International Conference on. Vol. 1.

[12] Zhang, Daxing, Haihua Li, and Zhigeng Pan [12]. "A contour based semi-fragile image watermarking algorithm in DWT domain." Second International Workshop on Education Technology and Computer Science (ETCS), Vol. 3, IEEE, 2010.

[13] Qiang Wang and colleagues, "Digital image encryption research based on dwt and chaos." IEEE, 2008. Vol. 5 of Natural Computation, ICNC'08: Fourth International Conference on.

[14] Wolfgang Meerwald, Andreas Uhl, Roland Kwitt, and Peter Meerwald. "Lightweight detection of additive watermarking in the DWT-domain." 20.2 (2011) IEEE Transactions on Image Processing, 474–484.

[15] Li et al., et al., "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD." 2007 IEEE International Conference on Multimedia and Expo, IEEE, 2007.