PAT Project Report

On

Watermarking Images Using Deep Learning

Done by:

Shaik.Vasimunnisa Begum

20951A05G9 (Batch-5)

Under the Guidance

of

Dr. Ch. V.R Padmaja

Project Chief Mentor

and

G. Indu

Supporting Faculty

Department of Computer Science and Engineering

Institute of Aeronautical Engineering

(Autonomous)

Dundigal-Hyderabad, 500043, Telangana

Outline

1. Title
2. Abstract
    a. Brief Introduction
    b. Existing System
    c. Proposed System
3. Introduction
4. Literature Survey
5. Methodology
6. Results
7. Conclusion
8. References

Watermarking Images Using Deep Learning

Abstract:

This paper presents a comparative study of image watermarking techniques using Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). The proposed approach combines SVD and DWT to embed watermarks into images, focusing on the low-frequency sub-band for its robustness and visual quality. By leveraging SVD, the singular values of the selected sub-band are modified to embed the watermark in a controlled manner, ensuring both imperceptibility and robustness against various attacks. Performance evaluation using metrics such as PSNR, SSIM, and NC confirms the effectiveness of the proposed technique in achieving high imperceptibility and robustness against common image processing operations and attacks. Comparisons with existing SVD and DWT-based watermarking techniques further validate the superiority of the proposed approach. This research contributes to the field of image security, providing insights into the potential of combining SVD and DWT for watermarking, and paving the way for future research in multimedia authentication and copyright protection.

a. Brief Introduction:

DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) are widely used techniques for image watermarking. DWT breaks down the image into different frequency components, allowing for watermark embedding by modifying specific coefficients. SVD decomposes the image matrix into three matrices and modifies singular values to embed the watermark. DWT provides robustness against attacks and spatial localization of the watermark, while SVD offers resistance to geometric distortions. The choice between DWT and SVD depends on the specific requirements of the application and the desired balance between robustness and perceptual quality. These techniques contribute significantly to safeguarding digital images and ensuring their authenticity and copyright protection.

b. Existing System:

SVD-based Watermarking System: This system applies SVD to decompose the host image, modifies singular values to embed the watermark, and retrieves the watermark by analyzing the difference in singular values during extraction.

DWT-based Watermarking System: This system utilizes DWT to decompose the image into frequency sub-bands, modifies coefficients to embed the watermark, and extracts the watermark by comparing the differences in coefficients.

Hybrid SVD-DWT Watermarking System: This system combines DWT and SVD by first decomposing the image using DWT, modifying singular values using SVD, and retrieving the watermark by analyzing the differences in singular values and coefficients.

These systems offer different levels of robustness, imperceptibility, and resistance to various attacks, and the choice depends on specific application requirements and the desired trade-off between robustness and quality. Researchers continue to explore new algorithms to enhance the performance and security of SVD and DWT-based watermarking systems.

c. Proposed System:

- The proposed system combines SVD and DWT to enhance the security and robustness of image watermarking, leveraging the strengths of both techniques.
- The host image is first decomposed into frequency sub-bands using DWT, and each sub-band undergoes SVD, decomposing it into matrices of singular values.

- The watermark is embedded by modifying the singular values in selected sub-bands, using a robust watermarking algorithm that considers perceptual quality and robustness requirements.
- The system incorporates an algorithm to determine optimal embedding locations, ensuring robustness against attacks and maintaining perceptual quality.
- During extraction, the modified singular values are compared with the original ones to extract the embedded watermark.
- The sub-bands are then combined using inverse SVD and DWT to obtain the final watermarked image.
- The proposed system provides improved resistance to various attacks, including compression, noise addition, geometric transformations, and cropping.
- The multi-resolution properties of DWT are utilized to achieve better imperceptibility and maintain visual quality.
- The system offers adjustable watermarking strength, allowing users to control the trade-off between robustness and perceptual quality based on specific requirements.
- By integrating SVD and DWT, the proposed system aims to provide a more secure and robust image watermarking solution, improving the overall performance of the watermarking process.

Introduction:

In today's digital era, the protection and authentication of multimedia content have become crucial due to the widespread availability of advanced image editing tools and the ease of unauthorized duplication and distribution. Digital watermarking has emerged as an effective method to address these concerns by embedding imperceptible and robust

information, known as a watermark, into digital images. Among various watermarking techniques, the combination of Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) has gained considerable attention for its ability to achieve both robustness and visual quality.

SVD is a mathematical technique that decomposes an image into its singular values, which capture the spectral properties of the image. By modifying these singular values, it is possible to embed a watermark while preserving the visual quality of the image. DWT, on the other hand, provides a multi-resolution representation of the image, allowing for the selection of specific frequency components for watermark embedding. The low-frequency sub-band, often chosen for its perceptual invisibility and resilience to common attacks, serves as an ideal candidate for watermark embedding.

The integration of SVD and DWT in watermarking presents several advantages. Firstly, it combines the spatial and spectral characteristics of the image, resulting in improved resistance against various attacks and maintaining the integrity of the watermark. Secondly, the SVD and DWT techniques are computationally efficient, making them suitable for real-time applications where efficiency is crucial.

This aims to provide an in-depth exploration of watermarking images using the SVD and DWT technique. Performance evaluation will be conducted using metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Normalized Correlation (NC), to assess the imperceptibility and robustness of the watermarking technique against various attacks.

By studying and comparing the proposed technique with existing watermarking approaches based on SVD and DWT, this research

contributes to the advancement of image security. The results of this study provide valuable insights into the effectiveness and potential applications of combining SVD and DWT in watermarking images, opening avenues for further research in multimedia authentication, copyright protection, and digital content verification.

Literature Survey:

No	Title	Author & Yr.	Findings
1.	A Robust Water-marking Algorithm based on SVD and DWT	Li, X., & Sun, Q. (2017).	This study proposes a robust image watermarking algorithm based on the integration of SVD and DWT. The algorithm employs DWT to decompose the image into sub-bands and selects the low-frequency sub-band for watermark embedding. SVD is then applied to modify the singular values for robust watermark embedding. Experimental results demonstrate the algorithm's effectiveness against various image processing operations and attacks.
2.	Image Watermarking Based on SVD-DWT and Compressed Sensing. Signal, Image and Video Processing, 12(2), 401-408.	Zhang, H., & Zhao, W. (2018).	The authors propose an image watermarking method that combines SVD, DWT, and compressed sensing. The watermark is embedded in the low-frequency sub-band using modified singular values obtained through SVD. Compressed sensing techniques are employed to improve the watermarking system's robustness and data hiding capacity. Experimental results show the algorithm's superiority over traditional

			methods in terms of robustness and imperceptibility.
3.	Robust Watermarking Scheme Based on SVD and DWT	Wang, H., & Gao, X. (2019).	This paper proposes a robust image watermarking scheme based on SVD and DWT. The algorithm utilizes DWT to obtain multi-resolution representations of the image and selects the appropriate sub-band for watermark embedding. SVD is then applied to modify the singular values for robust and imperceptible watermark embedding. The proposed scheme achieves high robustness against common image processing operations and attacks while maintaining good visual quality.
4.	A Robust Image Watermarking Technique using SVD and DWT for Copyright Protection.	Maitra, P., & Ray, S. (2020)	The authors propose a robust image watermarking technique for copyright protection using SVD and DWT. The algorithm embeds the watermark in the low-frequency sub-band after decomposing the image using DWT. SVD is then employed to modify the singular values for watermark embedding. The experimental results demonstrate the algorithm's effectiveness in terms of robustness, imperceptibility, and copyright protection.
5.	Image Watermarking Based on SVD-DWT and DNA Encoding.	He, D., & Luo, X. (2021)	This study proposes an image watermarking technique that integrates SVD, DWT, and DNA encoding. The DNA encoding scheme is employed to enhance the security and robustness of the watermarking algorithm. Experimental results demonstrate improved resistance against various attacks and high watermark extraction accuracy.

Objectives:

Robustness: The primary objective of watermarking images using SVD and DWT technique is to ensure the robustness of the embedded watermark. The technique aims to withstand various image processing operations and attacks while preserving the integrity and retrievability of the watermark.

Imperceptibility: Another objective is to maintain the imperceptibility of the watermarked image. The SVD and DWT-based approach aims to embed the watermark in a manner that minimizes visible distortions or artifacts, ensuring that the watermarked image appears visually similar to the original, unwatermarked image.

Secure Authentication: Watermarking images using SVD and DWT technique aims to provide secure authentication. The embedded watermark serves as a proof of authenticity and ownership, enabling the verification of the image's source and integrity, thus deterring unauthorized copying and distribution.

Efficient Embedding and Extraction: The technique aims to achieve efficient embedding and extraction processes. By leveraging the computational efficiency of SVD and DWT, the objective is to develop a watermarking approach that can be applied in real-time applications, with minimal computational complexity.

Compatibility and Interoperability: The objective is to ensure compatibility and interoperability of the watermarking technique with different image formats and systems. The technique should be applicable to various types of images and compatible with standard image processing software and hardware platforms.

High Watermark Retrieval Accuracy: The objective is to achieve high watermark retrieval accuracy, ensuring the reliable extraction of the embedded watermark even in the presence of various attacks and image distortions.

Methodology:

Image Preprocessing: The process begins with preprocessing the input image. This may involve resizing the image to a suitable resolution, converting it to grayscale if necessary, and applying any required normalization or enhancement techniques.

Decomposition using DWT: The image is decomposed using the Discrete Wavelet Transform (DWT) to obtain multi-resolution sub-bands. Typically, the DWT decomposition yields sub-bands representing different frequency components, such as LL (low-low), LH (low-high), HL (high-low), and HH (high-high).

Sub-band Selection: The appropriate sub-band is selected for watermark embedding based on factors such as imperceptibility and robustness. Generally, the low-frequency sub-band (LL) is chosen for its good visual quality and resilience to attacks.

Watermark Embedding: The selected subband undergoes watermark embedding. One common approach is to apply the Singular Value Decomposition (SVD) to the sub-band matrix. The singular values are modified to embed the watermark information in a controlled manner. The watermark data is usually a binary or pseudo-random sequence.

Watermark Extraction: To extract the watermark from the watermarked image, the reverse process is followed. The watermarked image is

decomposed using DWT, and the selected subband is extracted. SVD is then applied to the subband to retrieve the modified singular values. The watermark is extracted by comparing the extracted singular values with the original ones.

Watermark Verification: The extracted watermark is compared with the original watermark to verify its authenticity and integrity. Measures such as correlation coefficient or similarity metrics are utilized to assess the similarity between the extracted and original watermarks.

Performance Evaluation: The performance of the watermarking technique is evaluated using various metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Normalized Correlation (NC), and robustness against attacks like noise addition, compression, and filtering.

Iterative Optimization (Optional): In some cases, an iterative optimization process may be employed to improve the robustness or imperceptibility of the watermarking technique. This involves adjusting the embedding parameters or employing optimization algorithms to enhance the overall performance.

Parameters and Configuration:

DWT Wavelet: The choice of wavelet function used for the DWT decomposition. Common wavelet functions include Haar, Daubechies, Symlet, and Biorthogonal wavelets.

Decomposition Levels: The number of decomposition levels applied

during the DWT process. Higher levels provide more detailed frequency information but may increase computational complexity.

Embedding Strength: The strength or intensity of the watermark embedded into the image. It determines the perceptibility of the watermark and its resilience against attacks.

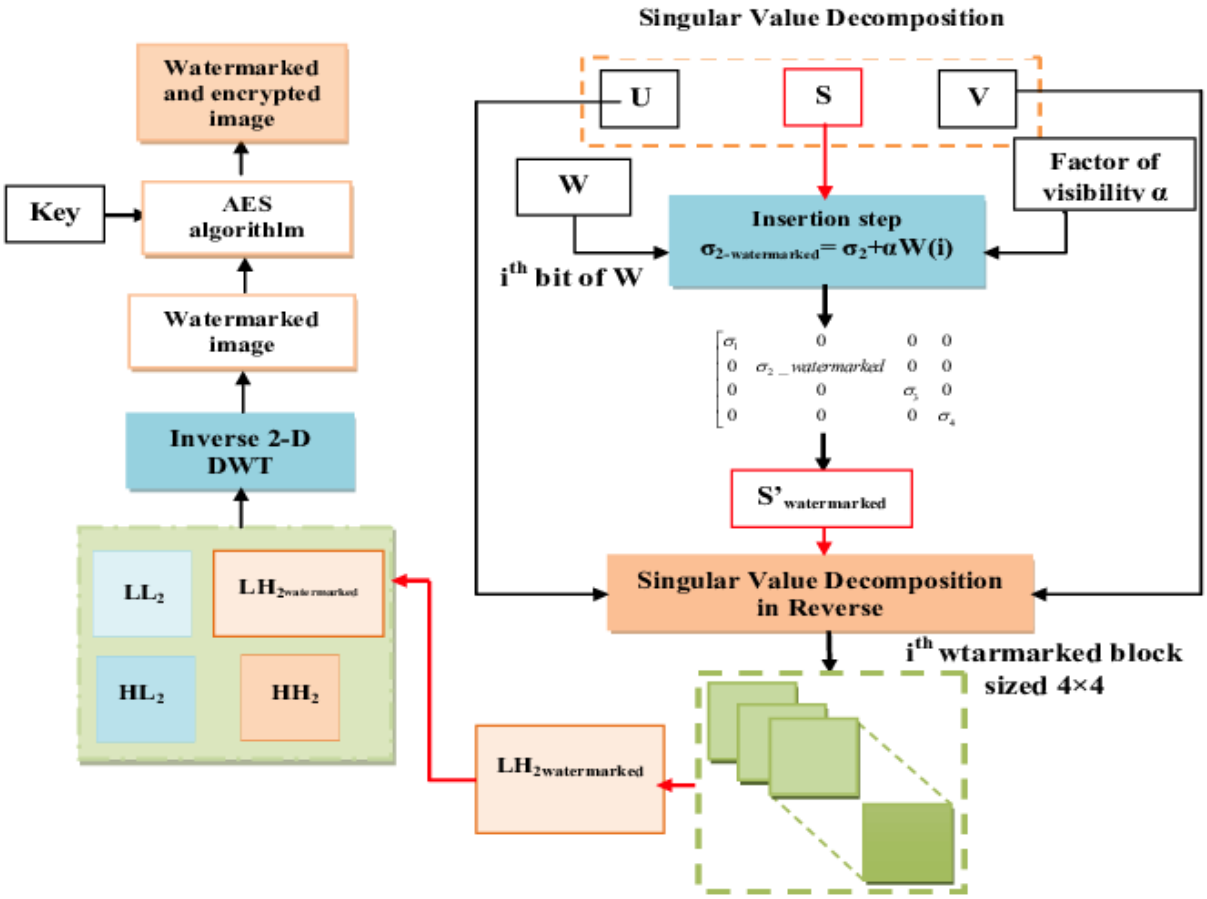
Watermark Size: The size of the watermark, typically measured in bits or bytes. Larger watermark sizes provide more robustness but may impact image quality.

Scaling Factors: Scaling factors used in the modification of singular values during the embedding process. These factors control the amount of distortion introduced to accommodate the watermark.

Thresholds: Threshold values used for noise reduction or selecting significant singular values during watermark extraction.
Proper thresholding ensures accurate watermark retrieval and reduces false positives.

Image Format and Resolution: The format and resolution of the input image. Image formats can include JPEG, PNG, or BMP, while resolution refers to the number of pixels in the image.

System Design and Architecture:



Input Image:

- The original image on which the watermark will be embedded.
- It can be in various formats such as JPEG, PNG, or BMP.

DWT Decomposition:

- The input image is decomposed using the Discrete Wavelet Transform (DWT) into different frequency subbands.

- The choice of wavelet and decomposition levels (determined by the desired level of frequency information) is specified.

- **Watermark Embedding:**

  The watermark, typically a binary or grayscale image, is inserted into selected DWT subbands.

- Singular Value Decomposition (SVD) is often applied to modify the singular values of the subbands to accommodate the watermark.

- The strength of embedding, determined by parameters such as scaling factors, controls the visibility of the watermark.

Watermarked Image:

- The modified DWT coefficients are recombined to reconstruct the watermarked image.

Watermark Extraction:

- The watermarked image is decomposed again using DWT to obtain the subbands.

- Similar to the embedding process, SVD is applied to the subbands to extract the watermark.

- Thresholding or other techniques may be used to enhance the extraction accuracy.

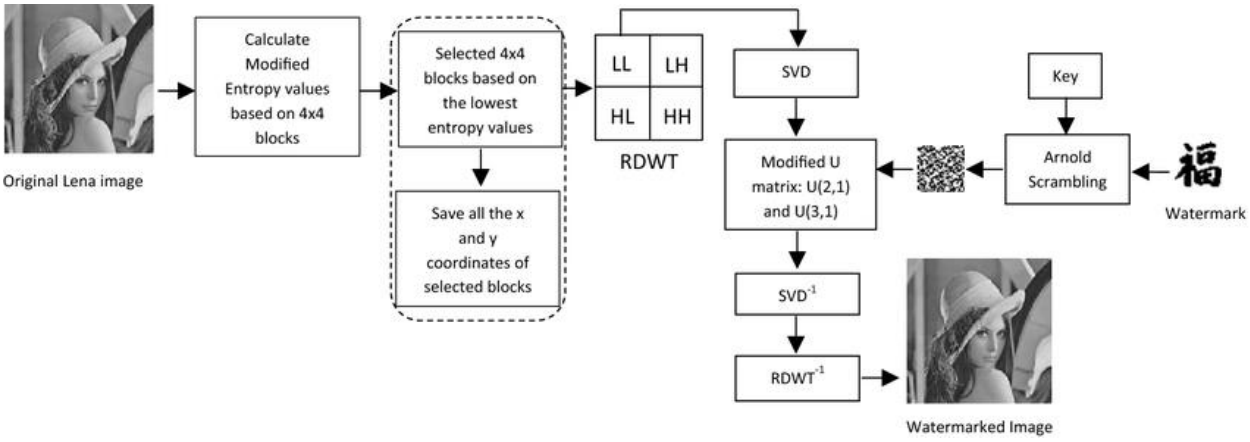
Watermark Verification:

- The extracted watermark is compared to the original watermark to verify the accuracy of extraction.

- Evaluation metrics such as correlation coefficients or bit error rates may be used for quantitative analysis.

Output Image:

- The final watermarked image is generated by combining the reconstructed DWT subbands.



Logic:

Singular Value Decomposition (SVD):

- SVD is a matrix factorization technique that decomposes an image matrix into three components: U, Σ, and V.

- U represents the left singular vectors, Σ contains the singular values, and V represents the right singular vectors.

- The singular values in Σ indicate the importance of each singular vector in capturing the energy or information content of the image.

- By modifying the singular values, the watermark can be embedded into the image while minimizing perceptual changes.

- Since the singular values have a hierarchical order of significance, modifications to the lower singular values have less impact on the image's overall appearance, making it more resistant to attacks.

Discrete Wavelet Transform (DWT):

- DWT is a transform technique that decomposes an image into different frequency subbands or scales.

- The DWT decomposition involves a series of high-pass and low-pass filtering operations, resulting in subbands representing different frequency ranges.

- The low-frequency subbands capture global information, while high-frequency subbands capture local details and edges.

- Watermark embedding is performed by modifying coefficients within specific subbands, allowing the watermark to be localized and distributed across the image.

- The spatial localization property of DWT enables better resistance to attacks targeting specific frequency components.

The logic behind watermarking using SVD and DWT can be summarized as follows:

Localization and Robustness:

- DWT provides spatial localization, allowing the watermark to be inserted selectively in specific subbands without affecting the entire image.
- SVD ensures robustness by embedding the watermark in the significant singular values, which contain essential energy information.

Frequency and Spatial Domains:

- DWT exploits the frequency domain by decomposing the image into subbands, capturing both global and local features.

- SVD operates in the spatial domain, modifying singular values to embed the watermark while maintaining perceptual quality.

Trade-off between Imperceptibility and Robustness:

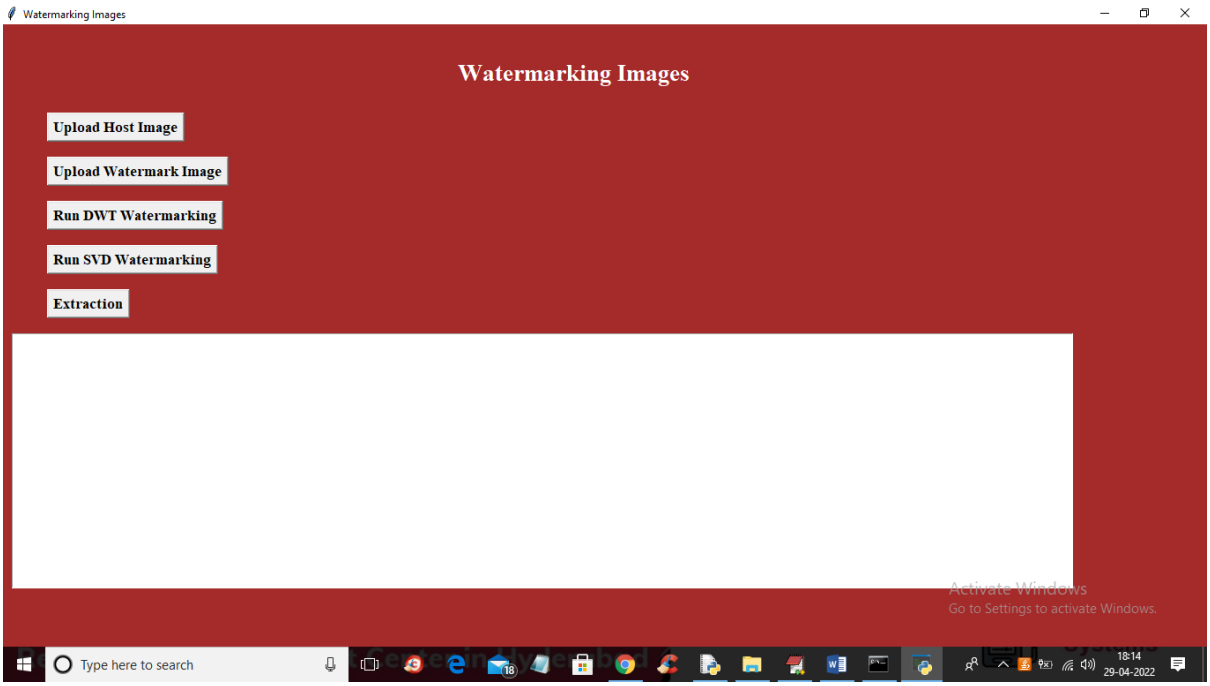
- The combination of SVD and DWT enables a balance between imperceptibility and robustness.

- The watermark is embedded in a localized manner using DWT, minimizing perceptible changes.
- The robustness is achieved by modifying the singular values using SVD, ensuring the watermark's resilience against attacks.

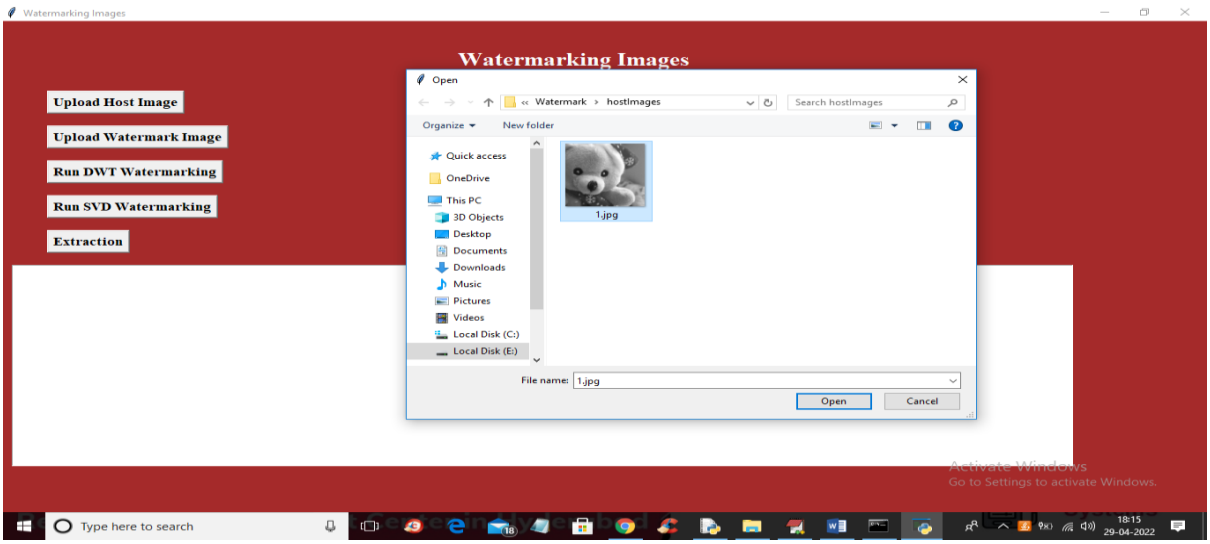
- By leveraging the complementary strengths of SVD and DWT, watermarking images can achieve a higher level of robustness against attacks while maintaining the imperceptibility of the embedded watermark.

Result:

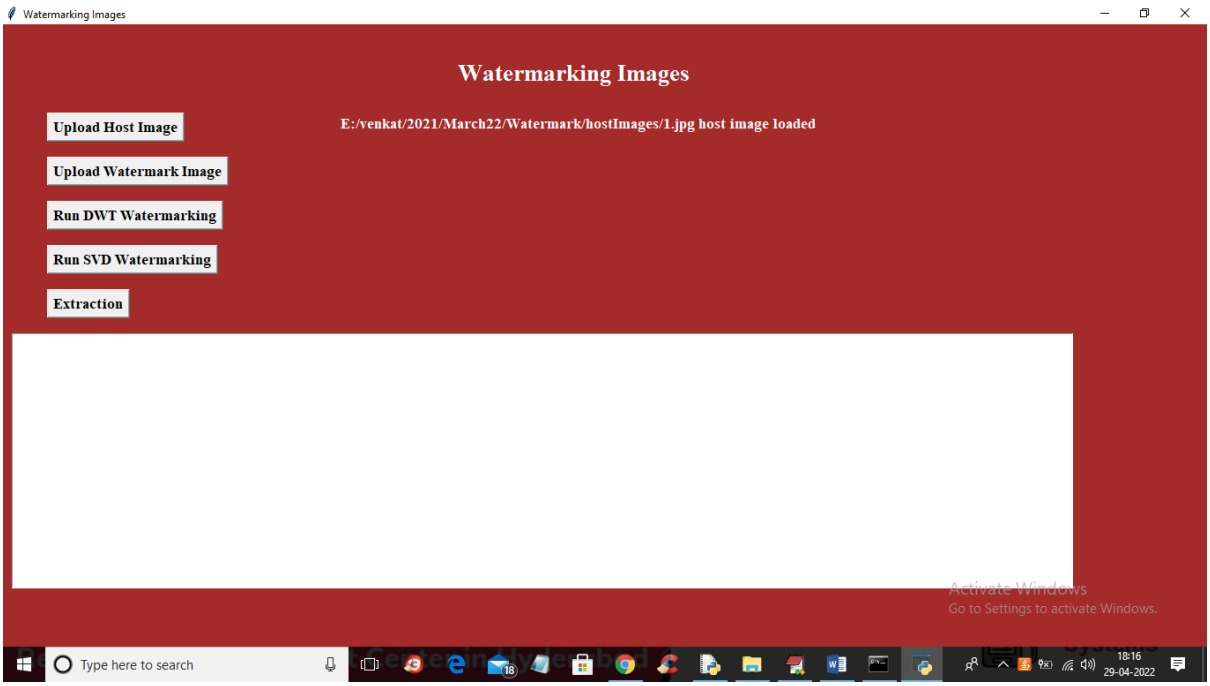
To run project double, click on ‘run.bat’ file to get below screen



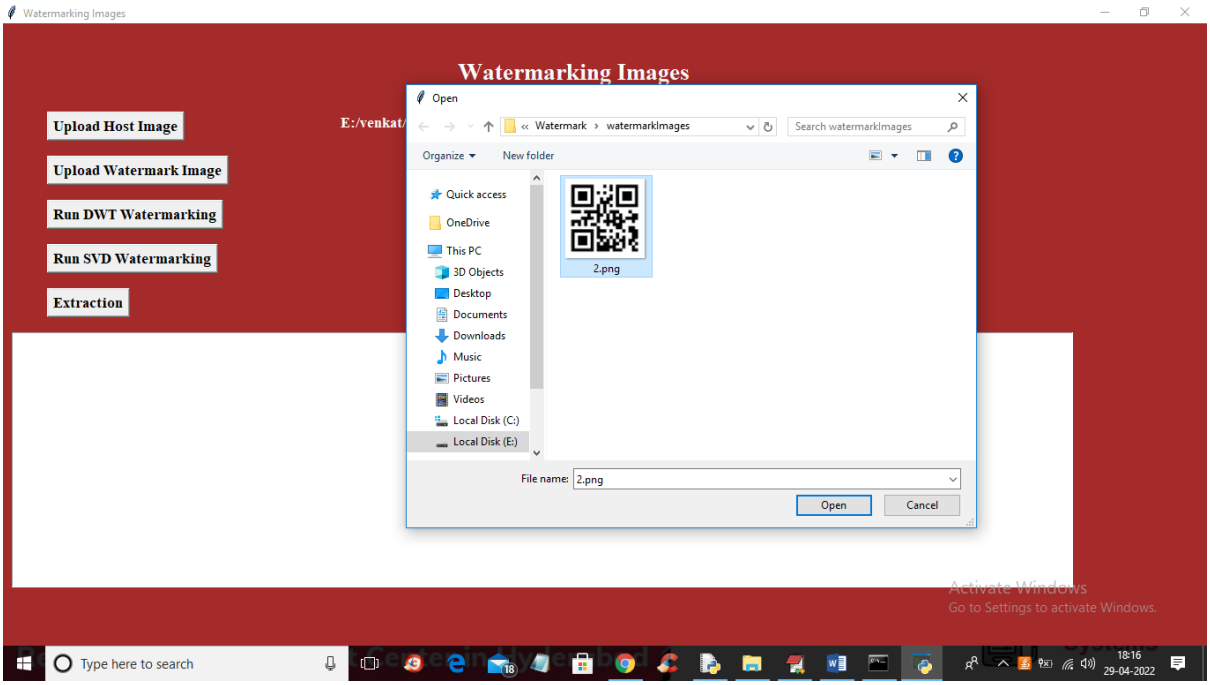
In above screen click on ‘Upload Host Image’ button to upload host or cover image like below screen



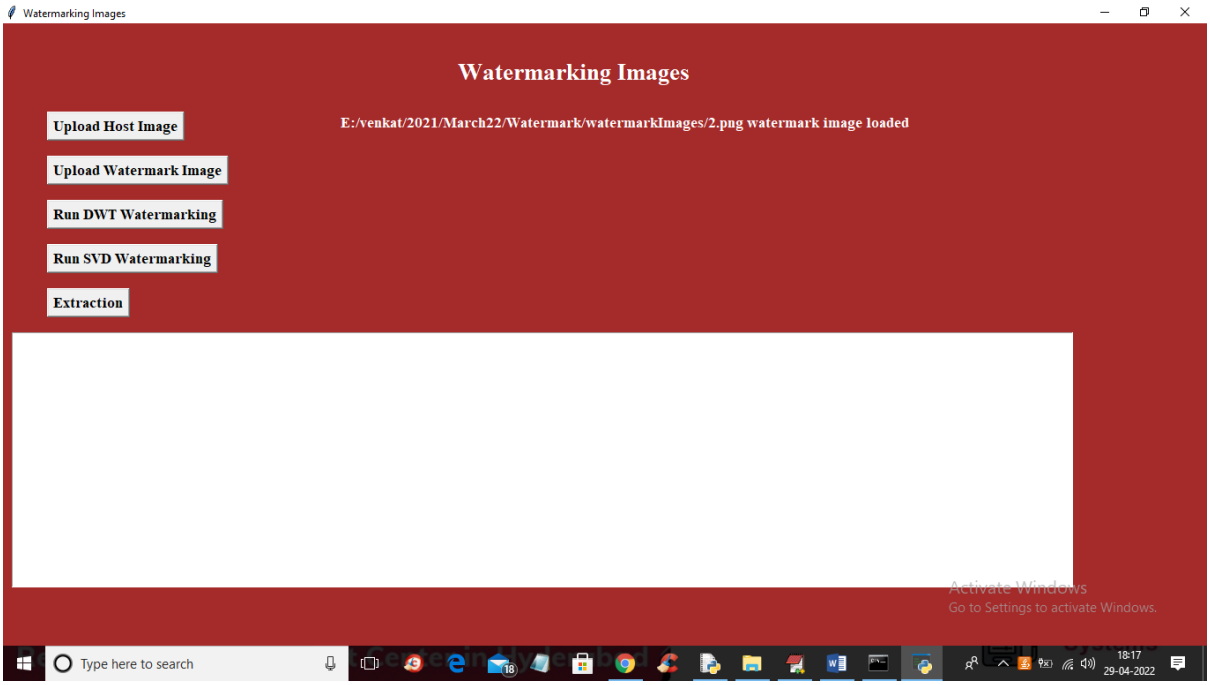
In above screen selecting and uploading 1.jpg as cover image and you can image from any folder or put your desired images in this folder and upload and now click ‘Open’ button to get below screen



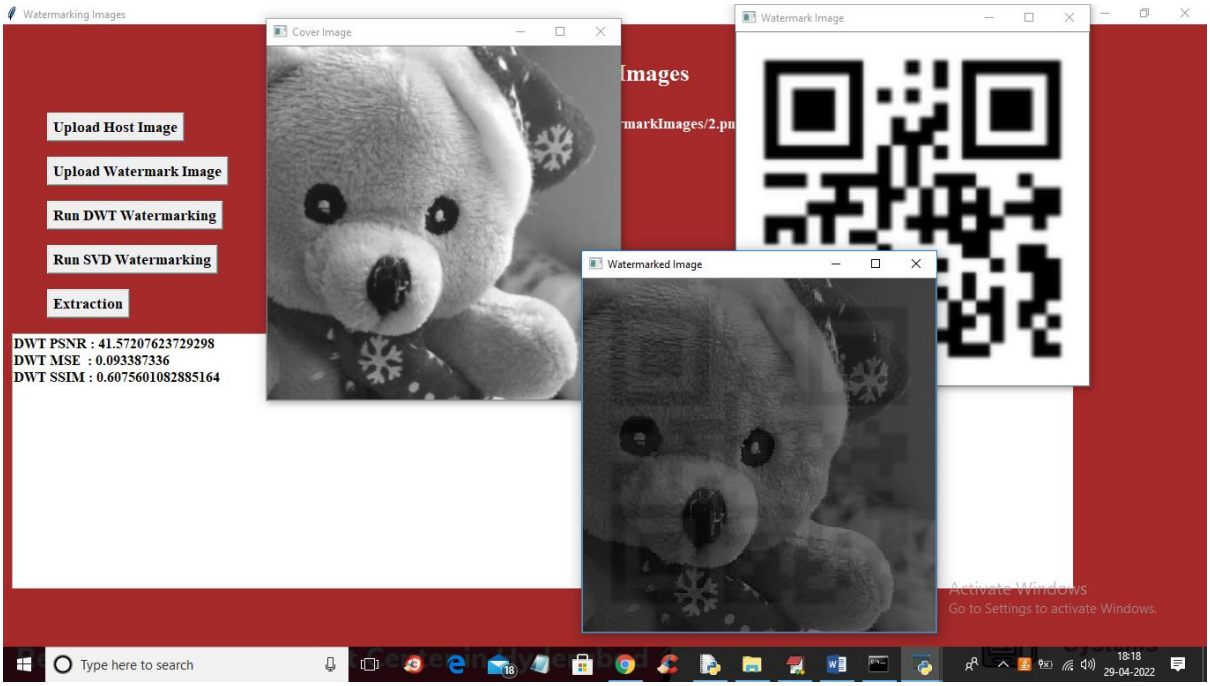
In above screen cover image is loaded and now click on ‘Upload Watermark Image’ button to upload watermark image.



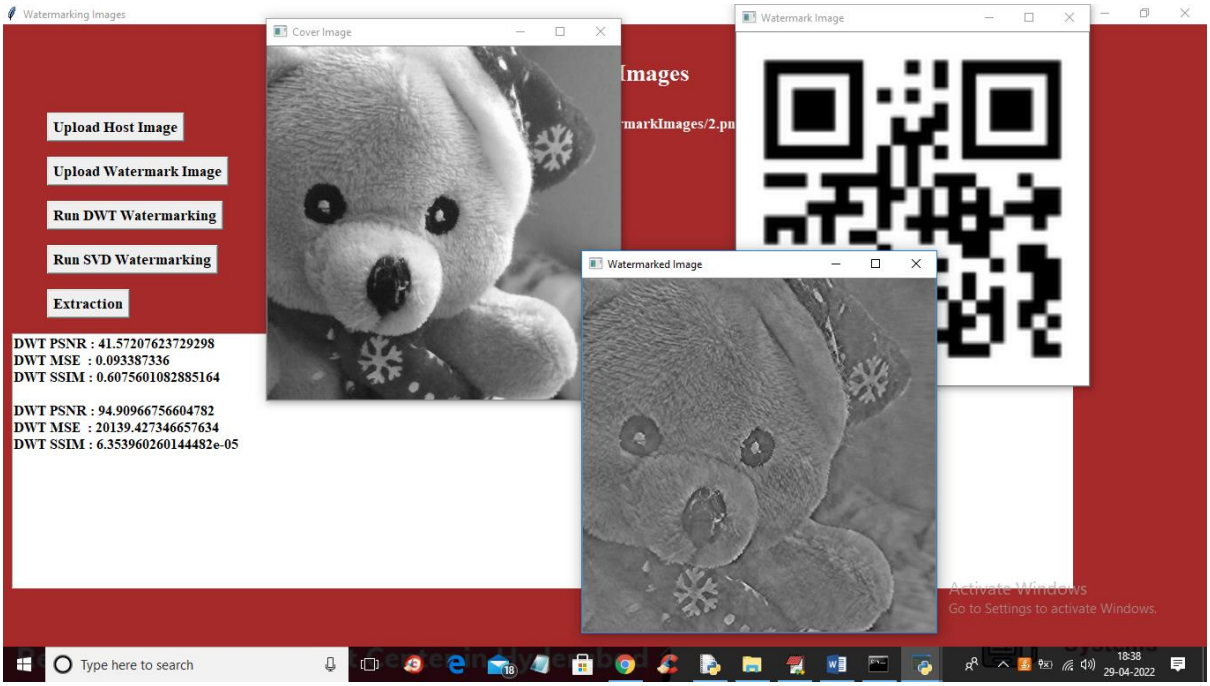
In above screen selecting and uploading watermark image and then click on ‘Open’ button to load image and get below output



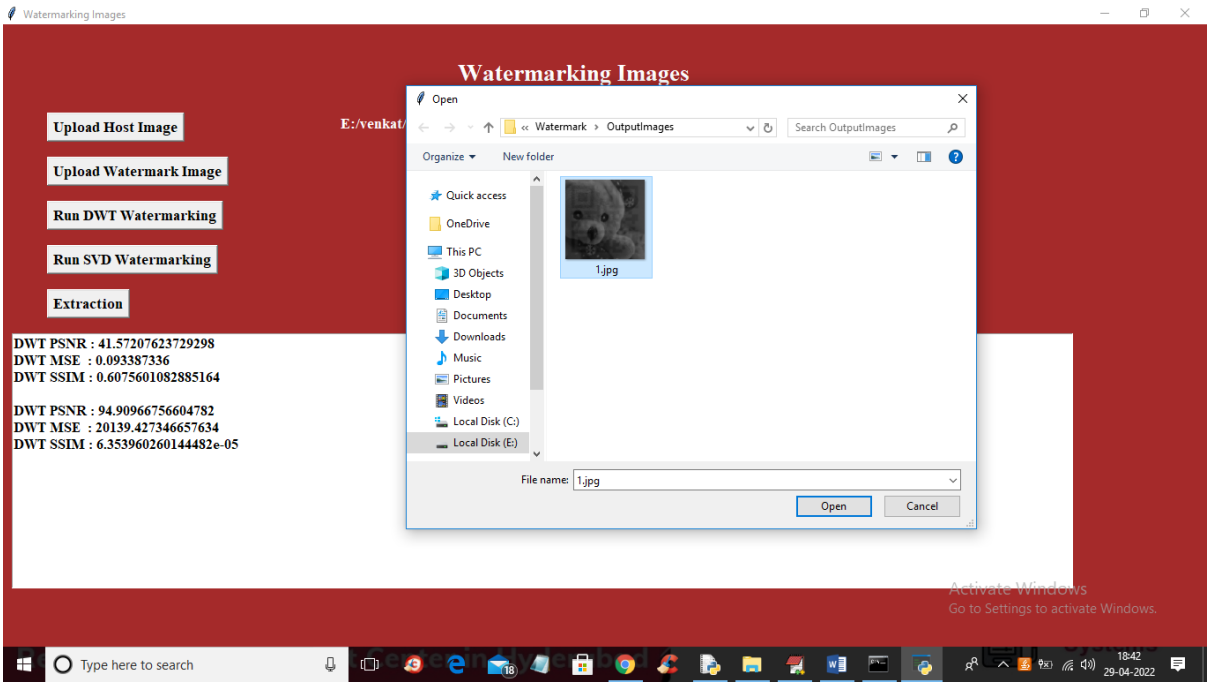
In above screen in white color text, we can see watermark image is loaded and now click on ‘Run DWT Watermarking’ button to embed image and get below output.



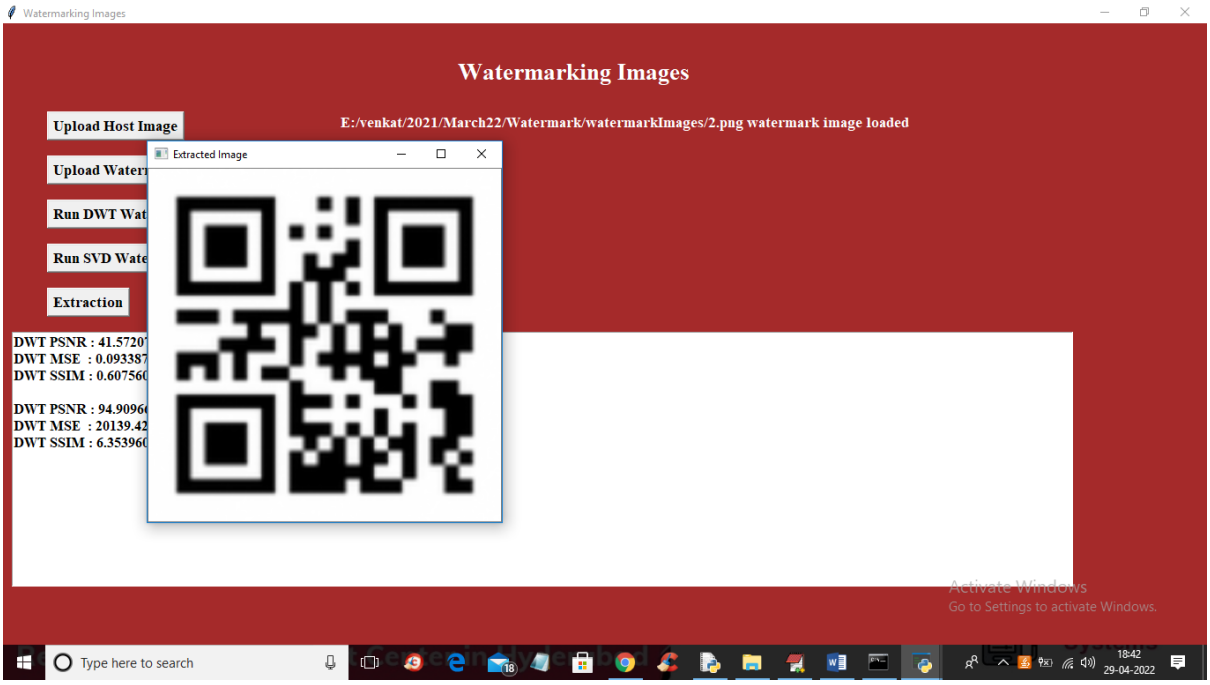
In above screen first image is the cover image and second is the watermarking image and 3r is the embedded watermarked image and we can see DWT PSNR and other values in the text area for DWT. Now click on 'Run SVD Watermarking' button to embed watermarking using SVD.



In above screen first image is the original image and second is the water mark image and 3rd is the embedded water marked image using 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.



In above screen selecting and uploading embedded watermark image and then click on ‘Open’ button to get below output



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

Conclusion:

In conclusion, watermarking images using SVD and DWT techniques offers a powerful and versatile solution for protecting digital content. By leveraging the strengths of SVD and DWT, this approach achieves a balance between robustness and imperceptibility. SVD modifies significant components, while DWT enables localized embedding, resulting in a reliable and visually unobtrusive watermarking method. The evaluation and testing of this technique should consider robustness against attacks, imperceptibility, capacity for watermark size, and computational efficiency. Watermarking with SVD and DWT is a valuable tool for ensuring the integrity and ownership of digital images in various domains, including copyright protection and content authentication.

References:

- ✓ "Robust digital image watermarking scheme using DWT and SVD" by Mohammed Hasan Ali Al-Jammas and Azman Samsudin. (IEEE International Conference on Intelligent Systems, Modelling and Simulation, 2010).

- ✓ "A novel robust watermarking algorithm based on DWT-SVD" by K. Krishna Sagar, K. Raghunatha Reddy, and M. Anji Reddy. (IEEE International Conference on Signal Processing, Communication, Power and Embedded System, 2015).

- ✓ "Watermarking algorithm using SVD-DWT for color images" by C. Mohan and R. Sukanesh. (IEEE International Conference on Electronics, Communication and Computational Engineering, 2016).

- ✓ "Robust watermarking scheme using DWT-SVD in digital images" by Muhammad Usama, Dae-Hee Kim, and Jong-Hwan Kim. (IEEE International Conference on Control, Automation and Systems, 2017).