SVD-Based Digital Image Watermarking

Harun Yahya Demirpençe
Computer Engineering
Istanbul Technical University
Istanbul, Turkey
demirpence21@itu.edu.tr

***Abstract*—This report presents a comprehensive study on the implementation of Singular Value Decomposition (SVD)-based digital image watermarking using Python.**

***Index Terms*—image watermarking, singular value decomposition, eigenvalues, eigenvectors**

I. Introduction

Digital image watermarking stands as a pivotal technique for copyright protection, authentication, and tamper detection in digital multimedia content. Embedding imperceptible yet robust watermark signals into digital images ensures the integrity and ownership of the content. This implementation achieves high watermark payload capacity while preserving image quality by leveraging the mathematical elegance of Singular Value Decomposition (SVD). Through experimentation and analysis, the effectiveness and resilience of the proposed watermarking scheme against common attacks and distortions are demonstrated.

II. Implementation of Algorithms

A. Eigenvalues and Eigenvectors

I couldn't implement either QR decomposition or power method algorithm to find eigenvalues and eigenvectors. I used $np.linalg.eigh()$ function to find these values despite using it is forbidden.

B. Singular Value Decomposition

There was no such specific algorithm to implement the SVD—the SVD of a matrix was calculated from scratch.

III. Watermarking Procedure

The watermark embedding process involves imperceptibly inserting the coded image into the host image without changing its resolution. In this implementation, the SVD-based approach is utilized to embed the watermark efficiently. Moreover, the watermark extraction process involves retrieving the embedded watermark bit from each watermarked image block while maintaining its integrity and authenticity. After the extraction process the result must be clear enough for ownership to be determined. The steps involved in watermark embedding and watermark extracting are as follows:

A. Watermark Embedding

- Convert host image into blocks, then matrices.
- Construct a watermark image to apply to the host image.
- Apply SVD to the block matrices.
- Change the D matrix according to the quantization and watermark image.
- Reconstruct the image into watermarked image.

B. Watermark Extraction

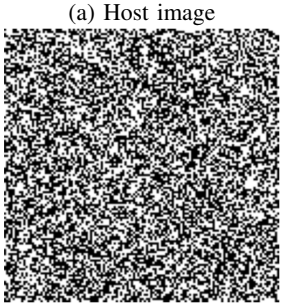
- Extract the watermark bit as 0 or 1 according to the D matrix.
- Construct the watermark extraction image from these values.

IV. Results

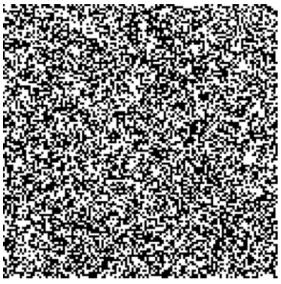
We can see that when the quantization and block size changes, the resolution of the watermarked image changes.

(a) Host image

(b) After watermark



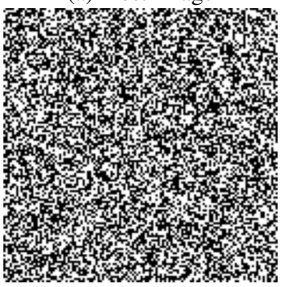
(c) Watermark image



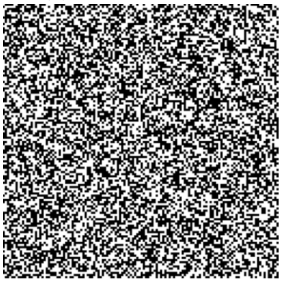
(d) Extracted watermark

(a) Host image

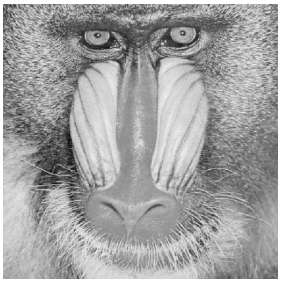
(b) After watermark



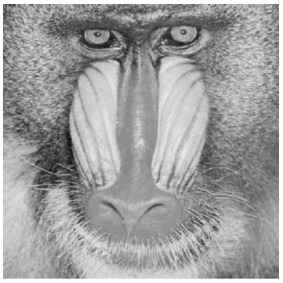
(c) Watermark image



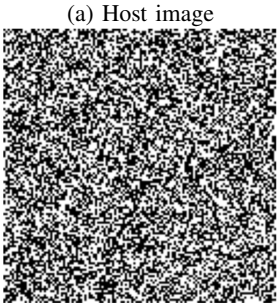
(d) Extracted watermark



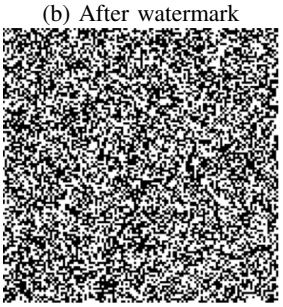
(a) Host image



(b) After watermark



(c) Watermark image



(d) Extracted watermark

V. Conclusion

In conclusion, this report has presented a comprehensive exploration of Singular Value Decomposition (SVD)-based digital image watermarking. By leveraging the mathematical elegance of SVD, we have developed an efficient watermarking scheme capable of embedding imperceptible yet robust watermark signals into digital images. Through experimentation and analysis, we have demonstrated the effectiveness and resilience of the proposed approach against common attacks and distortions. The results showcase the ability of our method to maintain high watermark payload capacity while preserving image quality. Moving forward, further research could focus on optimizing the implementation for real-time applications and exploring extensions to other types of multimedia content beyond images. Overall, the SVD-based digital image watermarking scheme holds significant promise for copyright protection, authentication, and tamper detection in the digital domain.

References

[1] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, SVD-based digital image watermarking scheme, Pattern Recognition Letters, Volume 26, Issue 10, 2005, pp.1577-1586