BLG202E Numerical Methods in Comp. Eng. Spring 2024- Term Project

* Due: May 5, 2023

1^{st} Kemal Tahir Bıcılıoğlu - 150210083
Faculty of Computer and Informatics Engineering
Department of Computer Engineering
Istanbul, Turkey
bicilioglu21@itu.edu.tr

I. Introduction

According to the Chin-Chen Chang et.al., In today's digital age, the ease and speed of manipulating digital media have made it challenging to protect intellectual property rights. With the rise of editing software and widespread internet access, activities like duplication, modification, and forgery have become prevalent. To address this issue, digital watermarking schemes have emerged as a popular method to safeguard digital images. These schemes involve embedding unique identifiers, known as watermarks, into images to establish ownership. Watermarks, such as logos, labels, or names, are embedded within the image, termed as the host image. This report includes the explanation for the given homework implementation, SVD-Based Digital Image Watermarking Scheme.

II. Implementation

A. Reading and Grayscaling Watermark Image

For the operations related to reading and manipulating images, Python libraries such as matplotlib, numpy, SciPy, and pandas were utilized. The Watermark image was selected as the IEEE logo and the host image was selected as the smurf cat. The host image resized to 512 to 512 and the watermark image resized to 32 to 32 because of the requirement of partitioning while SVD operation. After reading the watermark and host images, they are turned into grayscale images to work on afterward. They can be seen in the following figures:

Fig. 1. Host and Watermark images

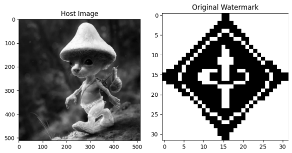

Fig. 2. Host and Watermark images grayscale

B. Singular Value Decomposition

Singular Value Decomposition (SVD) is a mathematical technique to break down a matrix into three components: U, D, and V. In watermarking, SVD is used to embed watermarks into images by modifying the singular values of the image matrix. This process preserves image quality while incorporating ownership information. During extraction, the watermark can be retrieved from the modified singular values, ensuring authentication and ownership verification of digital media.
For SVD implementation, first the eigenvalues and the eigenvectors are found and singular values are calculated as the square root of the found eigenvalues and replaced with the row of D accordingly. Since we are calculating the SVD of the matrix part by part, it was important the put the values in decreasing order to the rows of D which was not a problem since the eigenvalues were found in that order. After creating the D matrix, the V matrix is constructed by replacing the eigenvectors. Utilizing the V vector and using the formula of finding the U matrix U vector is found. After finding all the components of the SVD, it is recomposed to show its correctness. They can be seen as the following figures:

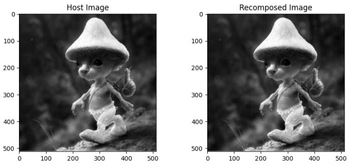

Fig. 3. Decomposed Host Image

C. Embedding Watermark

The watermark embedding procedure entails partitioning the host image into blocks, performing SVD transformation on each block, extracting the largest coefficient D(1,1) from the D component, quantizing and adjusting the coefficient based on the watermark bit, and finally, reconstructing the watermarked image through the inverse SVD transformation. These steps collectively ensure the effective embedding of the watermark while preserving image quality and resistance to image processing operations.
Implementing the described steps into a function, watermarked host images were created. It can be seen as the following figure:

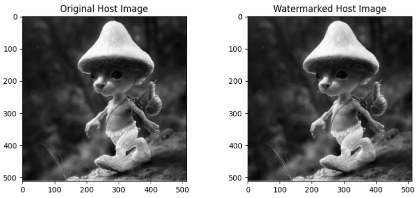

Fig. 4. Watermarked Host Image

D. Extracting Watermark

The watermark extraction procedure involves partitioning the watermarked image into blocks, performing SVD transformation on each block, extracting the largest coefficient D0(1,1) from the D component, quantizing the coefficient using a predefined quantization coefficient Q, and finally determining the bit value of the extracted watermark based on the relationship between Z and Q/2. If Z is less than Q/2, the extracted watermark bit has a value of 0; otherwise, it has a value of 1. These steps enable the extraction of the watermark image from the host image while maintaining accuracy and reliability.
Implementing the described steps into a function, watermarked host images were created. It can be seen as the following figure:

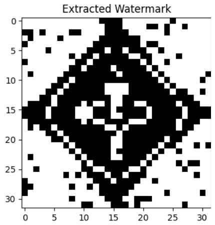

Fig. 5. Extracted Host Image

Although some distortions in the extracted image, it can easily be understood that the extracted image is the embedded image.

E. PSNR Value

In the paper, it was observed that the proposed watermarking scheme maintained high image quality, as evidenced by a peak signal-to-noise ratio (PSNR) exceeding 42 dB among the watermarked images. The PSNR measures the quality of the watermarked image by quantifying the ratio of the maximum possible power of the image to the power of the noise that affects the fidelity of its representation. A PSNR value higher than 42 dB suggests minimal image distortion resulting from the watermarking process. In my implementation, PSNR value is observed as 104 dB meaning that even though the distortion rate is bigger, they cannot be seen by the human eyes.

F. Extracting Watermark from Tampered Image

All the embedding and extracting functions are also applied for the tampered images. It can be easily seen that distortions for the extracted watermark images are more than the not tampered host images, however, the watermark image can easily be recognized. Extracted watermark images can be observed as the following images:

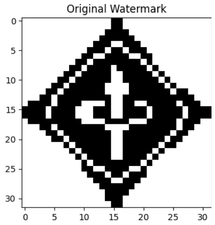

Fig. 6. Extracted Host Image

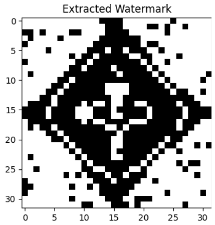

Fig. 7. Extracted Host Image

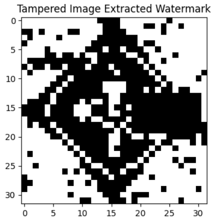

Fig. 8. Extracted Host Image

References

[1] Chang, C.-C., Tsai, P., Lin, C.-C. (2005). SVD-based digital image watermarking scheme. Pattern Recognition Letters, 26(10), 1577–1586. https://doi.org/10.1016/j.patrec.2005.01.004