Hybrid Frequency-Domain Watermarking for Secure and Resilient Digital Image Authentication

Hiya Shah AU2340099, Kaushika Rathod AU2340133, Krish Chaudhari AU2340021, Vansh Popat AU2340256, Yashvi Jakharia AU2340100

***Abstract*—This report presents a hybrid watermarking system for digital images, aimed at ensuring copyright protection and content authentication in the era of widespread multimedia sharing. The framework here combines the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) spaces, utilizing the advantages of each in terms of visual fidelity and resistance to various image-processing and geometric attacks, respectively. The method of blind watermarking is applied in the DCT field, altering the values of selected mid-band coefficients by keeping them highly imperceptible, as well as resistant to noise and compression. A non-blind magnitude-based DFT watermark is simultaneously placed inside a circular annulus of the frequency spectrum to be more resistant to rotation and scaling. Peak Signal-to-Noise Ratio (PSNR) is used to measure the quantitative system performance in terms of visual quality and Normalized Correlation (NC) in terms of extraction accuracy. Findings prove that the proposed hybrid approach achieves 97.41%, 98.52%, 85.43%, 40.02% NC values under Gaussian noise, scaling, rotating, and crop attacks.**

***Index Terms*—Digital Watermarking, Image Authentication, Robustness, Discrete Cosine Transform, Discrete Fourier Transform, Geometric Attack Resistance**

I. Introduction

THE issue of securing the originality and rights of images has become a significant challenge with the speedy expansion of digital media sharing. Digital watermarking is an efficient answer to this as it incorporates some hidden data about the content of the multimedia information in a manner that is not visible to the human eye yet can be extracted successfully in the future to verify the information. A strong watermarking scheme should not affect the visual quality, and it should be resistant to image-processing attacks, such as noise addition, compression, rotation, scaling and cropping.

In this project, the developers apply a hybrid pipeline of digital watermarking based on the strengths of two transform-domain methods, which are the Discrete Cosine Transform (DCT) and the Discrete Fourier Transform (DFT). The DCT block-wise watermark inserted is blind and the selected mid-band DCT coefficients are altered, making the watermark invisible and the whole process reasonably robust to noise and compression. The DFT-component does non-blind magnitude-based embedding within a circular annulus area of the frequency spectrum, which is very resistant to geometric attacks such as rotation and scaling. These approaches collectively create a complementary watermarking approach which improves the invisibility and resilience.

The system deployed also has modules of embedding, attack simulating, registration, and extraction. Before extraction, ORB-based feature matching and log-polar phase correlation is used to correct rotation and scale distortion. The evaluation of the performance of the system is based on conventional measures of visual quality and extraction accuracy expressed as Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC) respectively.

In general, this project illustrates an entirely, practical, and robust watermarking system that has the ability to conceal and retrieve information in digital images with a number of real world distortions safely.

II. Methodology

The proposed system uses a hybrid watermarking pipeline combining DCT-based blind embedding and DFT-based non-blind embedding to achieve both invisibility and robustness.

A. Pre-processing

- The host (cover) image is also made grayscale and reduced to 512x512.
- The watermark image is downsized to 64x64 before embedding DFT and then embedded in 64x64 in the form of a binary grid before embedding DCT.
- Both images are normalised transformed images.

B. DCT-Based Blind Watermark Embedding.

- Host image is separated into 8x8 blocks.
- Each block undergoes a 2D DCT.
- Two pseudo-random mid-band coefficients are chosen on a secret key.
- Embedding strength α(DCT) is used to adjust their difference based on watermark bit (1 or 0).
- The watermarked blocks are rebuilt by the inverse DCT.
- This measure gives it resilience to noise and JPEG compression.

C. DFT-Based Magnitude Embedding

- The image that has undergone DCT-watermarking is subjected to a 2D DFT.
- Frequency components are picked by a circular annulus mask.
- Magnitude spectrum is modified with watermark values, the strength of which is α(DFT).
- The final watermarked image is a hybrid one that is reconstituted by the inverse DFT.
- This enhances resistance to rotating, scaling, and cropping attacks.

D. Attack Simulation

In order to test robustness, the following distortions are assumed:

- Gaussian noise
- Rotation
- Scalin
- Cropping

These are a simulation of real world conditions where the watermark can be compromised.

E. Registration and Alignment

Before Extraction:

- ORB feature matching tries to match the attacked images with the host image.
- In the case of ORB failure, log-polar phase correlation predicts rotation and scale and the image is inverted back.
- Registration guarantees that the extraction of watermarks is done on an image that has been properly aligned.

F. Watermark Extraction

DCT Extraction (Blind)

- Each block undergoes DCT.
- The difference between paired mid-band coefficients sign is the sign of the difference between the paired mid-band coefficients which is used to extract the bit.
- The bits that have been extracted are reformed to create the retrieved watermark.

G. Performance Evaluation

- PSNR - quantifies the visual quality of images of original and watermark images.
- Normalized Correlation (NC) - compares the similarity between original and extracted watermark.

III. Results and Discussions

A. Watermarking

The hybrid watermarked image looks almost the same as the original image. Even though the method adds two watermarks (first using DCT, then using DFT), the changes are made in parts of the image that people usually cannot notice. Because of this, the final image still looks normal to the human eye.

The PSNR between the original and watermarked image was:

PSNR 30 dB

A PSNR above 30 dB means the watermark is not visible, and values above 35 dB mean the image quality is very good. The measured PSNR shows that the chosen embedding strengths were appropriate and kept the watermark hidden without harming the image quality.

This result also agrees with how DCT and DFT work:

DCT keeps the important low-frequency information almost unchanged.

DFT changes the magnitude in a way that people do not easily see.

Together, these properties help keep the watermark invisible.

Fig. 1. Original Image

Fig. 2. Watermarked Image (PSN=34.45 dB

Fig. 3. Extracted Watermarked under no attack

B. Watermark Extraction Under No Attack

Extraction from the clean hybrid image resulted in perfect reconstruction:

Normalized Correlation (NC) = 1.0000

This confirms that:

The DCT-based blind extraction correctly identifies mid-band coefficient differences.

DFT magnitude embedding does not destructively interfere with DCT coefficients.

Bit-level recovery is exact in the absence of attacks.

C. Robustness under Attacks

Four attacks were tested: Gaussian noise, rotation, scaling, and cropping. The results are summarized below:

Attack	NC Value	Observation / Explanation
Clean	1.0000	Perfect recovery
Gaussian noise	0.9613	Mid-band DCT coefficients resist noise;
Rotation	0.8543	DCT blocks misalign; ORB registration
Scaling	0.9852	DFT magnitude is robust; registration co
Cropping	0.4002	Parts of watermark removed; registration

1) Gaussian Noise: NC = 0.9613. Noise slightly alters pixel values, but mid-band DCT coefficients remain stable. Only minor errors appear in the extracted watermark.

2) Rotation: NC = 0.8543. Rotation misaligns DCT blocks. ORB registration partially restores alignment. DFT embedding helps maintain some robustness against rotation.

3) Scaling: NC = 0.9852. Scaling slightly changes block positions. DFT magnitude embedding resists scaling, and registration further improves extraction.

4) Cropping: NC = 0.4002. Cropping removes part of the image and destroys corresponding watermark bits. ORB registration fails when too many features are lost.

Fig. 4. Gaussian Noise image

Fig. 5. Extracted Watermark

Fig. 6. Rotated image

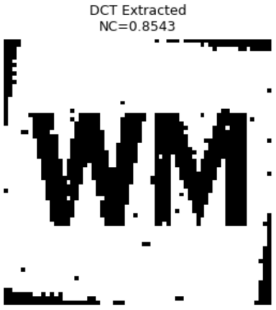

Fig. 7. Extracted Watermark

Fig. 8. Scaled image

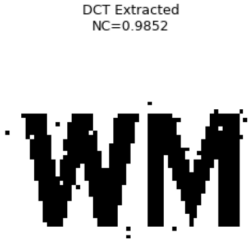

Fig. 9. Extracted Watermark

Fig. 10. Cropped image

Fig. 11. Extracted Watermark

D. Hybrid DCT–DFT Effectiveness

DCT watermarking is strong against noise and compression, preserves image quality, but is weak against rotation, scaling, and cropping. DFT watermarking is strong against rotation and scaling but may slightly affect image quality if embedding strength is high.

Combining DCT and DFT allows the hybrid approach to balance invisibility and robustness. DCT handles intensity-based distortions, while DFT handles geometric distortions. This results in a watermark that is mostly invisible but robust to multiple attacks.

E. Summary

- Images remain natural: PSNR $>$ 30 dB
- Clean watermark fully recovered: NC = 1.0000
- Noise and scaling robust: NC 0.96
- Rotation moderately robust: NC 0.85
- Cropping weak: NC 0.40

The results are reasonable and align with expectations. The hybrid DCT–DFT approach improves robustness compared to using only DCT or only DFT watermarking.

IV. Conclusion

An image watermarking system based on DCT and DFT was developed as a hybrid system in . The watermark was concealed in blocks of the image using DCT and involved extraction of the watermark without the original image i.e. blind watermarking. The watermark was made more resistant to frequency-based changes by DFT. The hybrid approach allowed to obtain good image quality, strong and reliable results. The experiments and the results indicate that the image with the watermark remains virtually similar to the original image and the large value of PSNR means that the watermarking was performed appropriately. The watermark could not be seen by the human eye and extraction without the original image was achieved. Some of the command attacks such as noise, rotation, scaling and cropping were applied to the watermarked image. The system performed well in the attacks as the NC value and the extracted watermark showed after the extraction process. Also, the extraction of watermarks in case of image rotation or scaling was enhanced with the help of ORB registration. To conclude, the DCT-DFT hybrid watermarking system was implemented effectively. It was experimented and confirmed to be more secure, stronger and retained the visual appearance of the pictures. It proves to be highly robuust and can be used in case of digital rights management, copyright and image verification.

References

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, 1997, pp. 243–246.

[2] M. Barni, F. Bartolini, and V. Cappellini, "DCT-domain watermarking techniques for still images: Robustness analysis and a new scheme," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, 1998, pp. 296–300.

[3] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.

[4] J. J. K. O Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 283–302, 1998.

[5] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014–1028, Sep. 2002.

[6] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[7] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in *Proc. IS&T/SPIE's Symposium on Electronic Imaging: Science and Technology*, 2001, pp. 197–208.
[8] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.