



# A Systematic Review of Frequency-Domain Digital Image Watermarking: Analyzing Classical Resilience Against Modern Manipulation Tools

Dr. Shalini Animeshbhai Mali

SASCTMA English Medium Commerce College and Shri Hasmukhlal Hojiwala College of Business  
Administration (BBA) & Smt. Ushaben Jayvadan Bodawala College of Computer Application  
(BCA)

## Abstract

Digital image watermarking is still an important method for copyright protection, ownership proof, and image authentication. Among many approaches, frequency-domain watermarking has remained popular because it usually gives better balance between image quality and robustness than simple spatial-domain methods [1][2]. This paper presents a systematic review of classical frequency-domain watermarking with focus on DCT, DWT, DFT, and SVD-based hybrid methods. It also studies how these traditional methods perform when images are changed by modern manipulation tools such as AI-based enhancement, inpainting, semantic editing, and watermark removal systems [3][4]. The review combines literature analysis with an experimental synthesis based on published benchmark results. The main observation is that classical methods still perform well against common attacks like compression, filtering, resizing, and noise, but their strength becomes limited when image content is strongly regenerated or semantically modified by modern tools [1][3].

**Keywords:** digital image watermarking, frequency-domain watermarking, DCT, DWT, DFT, SVD, robustness, image manipulation, review

## I. Introduction

Watermarking means hiding useful information inside an image in such a way that the information can later be detected or extracted. In digital image security, this hidden information can be used to show ownership, verify authenticity, or detect tampering [1][2]. Over the years, watermarking in the frequency domain has become more common because transform coefficients usually give better resistance against ordinary processing than direct pixel changes [1][2].

Classical frequency-domain watermarking was mostly designed for known image attacks such as JPEG compression, cropping, rotation, filtering, scaling, and additive noise [1]. In many studies, DCT-based methods showed good performance under compression, DWT-based methods gave good multi-resolution behaviour, DFT-based methods supported geometric stability, and SVD-based embedding improved extraction reliability [1][5]. Because of these strengths, hybrid methods such as DWT-DCT-SVD and DFT-DCT-SVD became popular in research.

However, the image editing environment has changed in recent years. Images are now modified not only by normal signal processing but also by AI-assisted tools. These tools may fill missing regions, sharpen details, replace objects, remove marks, or recreate textures in a very natural way [3][4]. This raises an important research question: are classical frequency-domain watermarking methods still strong enough when they face modern manipulation tools?

This paper studies that question in a clear and practical way. It reviews classical techniques, compares their reported strengths, and examines how their robustness should be understood in the present context of AI-supported editing. The paper is written in simple academic style so that the discussion remains useful for researchers, teachers, and postgraduate students.

## II. Review Method

This review follows a structured literature-based method. The selected studies were chosen because they discuss image watermarking in the frequency domain, report experimental results, and include useful information on image quality or robustness measures [1][2][3]. Sources from 2020 to January 2025 were given preference so that the paper reflects both classical development and recent research direction.

The review gives attention to three points. First, it studies the main transform families used in classical watermarking. Second, it compares how published studies measured imperceptibility and robustness. Third, it examines how the threat model changes when modern AI-based image manipulation becomes part of the environment [3][4].

A complete statistical meta-analysis was not possible because different papers use different datasets, payload sizes, extraction assumptions, attack levels, and evaluation settings. Because of this, a narrative

synthesis was more suitable. This method allows careful comparison without forcing unlike experiments into the same numerical model [1][2].

### III. Main Frequency-Domain Methods

#### A. DCT-Based Watermarking

The discrete cosine transform is widely used in image watermarking because it works well with JPEG-based image processing. Many researchers place watermark data in middle-frequency coefficients so that the watermark does not become too visible and also does not vanish too easily after compression [1][6]. DCT-based schemes are often simple to implement and remain useful for web-shared images.

At the same time, pure DCT methods may become weak under heavy filtering, noise, or large geometric changes if the embedding design is not carefully balanced. This is why DCT is often combined with other transforms instead of being used alone [1][6].

#### B. DWT-Based Watermarking

The discrete wavelet transform divides the image into different sub-bands. This allows the system to place the watermark in parts of the image where good visual quality and useful robustness can be achieved together [1][7]. Because of this multi-resolution property, DWT-based watermarking remains one of the most studied methods.

Many recent papers show that DWT performs well when images are affected by noise and resizing, and it also gives flexibility for hybrid watermarking models [2][7]. Still, the choice of sub-band is very important. If the watermark is inserted in a weak location, performance can reduce under specific attacks [1].

#### C. DFT-Based Watermarking

The discrete Fourier transform is often selected when geometric stability is important. It supports useful behaviour under translation, scaling, and rotation, which makes it suitable for some robust watermarking tasks [1]. In many practical studies, DFT is not used alone but is combined with DCT or SVD so that the design benefits from more than one transform property [1].

#### D. SVD-Based Support

Singular value decomposition is commonly added to transform-domain watermarking because singular values are comparatively stable under moderate changes. This helps in extraction and often improves overall robustness [1][8]. SVD is therefore widely used with DWT, DCT, and other transform-based methods, especially in hybrid models.

#### IV. Classical Hybrid Methods

Hybrid watermarking became popular because no single transform could handle all attack types equally well. Researchers therefore combined multiple transforms so that one stage controls image decomposition, another manages coefficient selection, and another improves stability during extraction [1][8].

A common example is DWT-DCT-SVD. In this model, DWT divides the image into sub-bands, DCT handles compact coefficient representation, and SVD supports stable embedding [8][9]. Another important model is DFT-DCT-SVD, which combines geometric support with strong compression behaviour and stable extraction [1].

Such hybrid approaches usually report better balance between invisibility and robustness than single-transform methods. But this does not mean they are always best. Their success still depends on host image type, embedding strength, attack condition, and whether extraction is blind or non-blind [1][2].

#### V. Measures Used in Studies

Most watermarking papers study two major properties: imperceptibility and robustness. Imperceptibility tells whether the watermarked image still looks natural. Robustness tells whether the watermark can still be detected or extracted after attack [1][2].

The most common image-quality measures are PSNR, SSIM, MSSIM, and FSIM. The most common robustness measures are NCC, NC, BER, and in some cases PCC [1]. These measures are useful and still important, but they mainly reflect performance against ordinary image processing.

This point becomes important in the present context. A watermark may score very well under JPEG compression, noise, blur, or scaling, but that does not guarantee survival under AI-based object replacement, texture rewriting, or semantic editing [3][4]. So the meaning of robustness now needs wider interpretation.

#### VI. Experimental Synthesis

This paper includes experimental discussion through published benchmark results. A detailed 2023 study compared DWT-DCT-SVD, DWT-DFT-SVD, and DFT-DCT-SVD using several image sets and many attacks such as Gaussian noise, Gaussian filtering, histogram equalization, JPEG compression, rotation, resizing, gamma correction, pixelation, and impulse noise [1].

The reported average results showed that the DFT-DCT-SVD model achieved PSNR of 33.045, MSSIM of 0.989, and FSIM of 0.972 across the tested images [1]. These values show that strong hybrid watermarking can preserve visual quality well. In many attack conditions, the same method also gave high NCC and PCC values, which suggests stable watermark recovery [1].

For JPEG compression at 75 percent quality, the same model reported NCC of 0.983, and at 50 percent quality it reported NCC of 0.975 [1]. Under Gaussian filtering with a 3 x 3 filter, NCC reached 0.994, and under pixelation with 4 x 4 tiles, NCC reached 0.998 [1]. These results clearly support the idea that classical frequency-domain hybrid methods remain effective against many ordinary attacks.

A separate comparison repository also showed that DWT performs strongly under noise, while DWT plus SVD can be better than DCT under crop and resize attacks, though weaker in some rotation and blur cases [2]. This is useful because it shows that there is no single universal best method. Robustness always depends on the type of attack.

## VII. Modern Manipulation Tools

The biggest change in the present situation is not only stronger image editing but different image editing. In classical attack models, the image was mostly distorted. In modern editing, the image may be re-created in parts or even changed in meaning while still looking natural [3][4].

AI-assisted inpainting can fill removed parts, enhancement tools can reconstruct texture, restoration models can smooth or sharpen content, and watermark removal systems can learn patterns that should be suppressed [3][4]. In such cases, the watermark may disappear not because it was weak under noise or compression, but because the original local structure of the image was replaced.

This means that a watermark surviving blur, JPEG, and resizing may still fail under strong semantic editing or content regeneration. Therefore, classical robustness results should now be read with caution. They are still valid, but mainly within the attack model for which they were originally designed [1][3].

## VIII. Discussion

The review shows that classical frequency-domain watermarking still has practical value. It remains useful in archive systems, copyright marking, controlled image-sharing workflows, and educational research where normal processing attacks are more common than advanced AI regeneration [1][2]. It is also easier to explain and implement than many deep learning approaches, which is useful for teaching and baseline comparison.

At the same time, modern deployment needs stronger evaluation. A watermarking paper written in 2025 should not stop at JPEG, cropping, blur, and scaling. It should also consider AI-assisted editing, image restoration, semantic replacement, and learning-based removal when such threats are relevant [3][4].

The review therefore supports a balanced position. Classical watermarking is not outdated, but it is no longer enough to claim strong robustness only on the basis of traditional attacks. In present conditions, layered image protection is more realistic, where watermarking may work together with authentication, metadata linking, and other security methods [3][4].

## IX. Ten Review Points

1. Frequency-domain watermarking remains more reliable than simple spatial-domain watermarking for many normal image-processing attacks [1][2].
2. DCT-based methods are still useful in JPEG-heavy environments because of their close relation with compression behaviour [1][6].
3. DWT-based methods remain popular because they support multi-resolution embedding and often perform well under noise and resizing [1][2][7].
4. DFT-based methods are valuable when some geometric stability is required, especially in hybrid designs [1].
5. SVD improves extraction stability and is one of the most common supporting techniques in robust watermarking models [1][8].
6. Hybrid methods such as DWT-DCT-SVD and DFT-DCT-SVD usually provide better overall balance between invisibility and robustness than single-transform methods [1][8][9].
7. Published experimental results show that classical hybrids still perform strongly under compression, filtering, pixelation, and several routine attacks [1].
8. There is no single best classical method for all conditions; the attack type strongly influences performance [1][2].
9. Modern AI-based editing changes the threat model because image content may be rewritten or regenerated instead of only being distorted [3][4].
10. For research from 2025 onward, classical watermarking should be evaluated against both conventional attacks and modern AI-assisted manipulation tools [3][4].

## X. Conclusion

This review finds that classical frequency-domain watermarking still holds strong academic and practical importance. DCT, DWT, DFT, and SVD-based hybrid methods continue to show useful robustness against ordinary attacks such as compression, filtering, resizing, and noise [1][2]. Their reported image quality is also generally high when embedding is done carefully [1].

However, present-day image manipulation tools have changed the meaning of robustness. AI-based editing can alter local or global content in a way that traditional benchmarks did not fully consider [3][4]. For this reason, the best path for current research is not to discard classical methods, but to evaluate them more honestly and integrate them into wider image-authentication frameworks.



## References

1. Justin, J. R., Rani, E. P., & Kumar, M. R. G. (2023). An effective digital image watermarking scheme incorporating DCT, DFT and SVD transformations. *PeerJ Computer Science*, 9, e1427. <https://peerj.com/articles/cs-1427/>
2. Lucasjvds. (2024, February 17). *classic-watermark-analysis: Test & compare classic frequency domain watermarking techniques: DCT, DWT and DWT-SVD*. GitHub. <https://github.com/lucasjvds/classic-watermark-analysis>
3. Frequency-domain attention-guided adaptive robust watermarking model. (2025). *Journal of the Franklin Institute*. <https://www.sciencedirect.com/science/article/abs/pii/S0016003225000055>
4. Cai, Z., Liu, Y., Yuan, H., & Zhang, J. (2024). Robust deep image watermarking: A survey. *Computers, Materials & Continua*, 81(1), 133-160. <https://www.techscience.com/cmc/v81n1/58332>
5. Ray, A., & Roy, S. (2020). Recent trends in image watermarking techniques for copyright protection: A survey. *International Journal of Multimedia Information Retrieval*, 9(4), 249-270. <https://doi.org/10.1007/s13735-020-00197-9>
6. Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023). A blind and robust color image watermarking scheme based on DCT and DWT domains. *Multimedia Tools and Applications*. <https://doi.org/10.1007/s11042-023-14797-0>
7. Alzahrani, A. (2022). Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD. *Applied Bionics and Biomechanics*, 2022, Article 5271600. <https://doi.org/10.1155/2022/5271600>
8. Zear, A., & Singh, P. K. (2022). Secure and robust color image dual watermarking based on LWT-DCT-SVD. *Multimedia Tools and Applications*, 81(19), 26721-26738. <https://doi.org/10.1007/s11042-020-10472-w>
9. Makbol, N. M., Khoo, B. E., & Khoo, H. J. (2012). Robust image watermarking based on the DCT-DWT-SVD transformation technique. *Journal of Visual Communication and Image Representation*, 25(5), 1059-1067. <https://research.ijcaonline.org/volume58/number21/pxc3883798.pdf>
10. Durafe, A., & Patidar, V. (2022). Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. *Journal of King Saud University - Computer and Information Sciences*, 34(7), 4483-4498. <https://doi.org/10.1016/j.jksuci.2020.10.008>
11. Aberna, P., & Agilandeewari, L. (2023). Digital image and video watermarking: Methodologies, attacks, applications, and future directions. *Multimedia Tools and Applications*. <https://doi.org/10.1007/s11042-023-15806-y>

12. Digital image watermarking using deep learning: A survey. (2024). *Computer Science Review*. <https://www.sciencedirect.com/science/article/abs/pii/S1574013724000467>
13. Robust image watermarking algorithm using chaotic sequences. (2022). *Egyptian Informatics Journal*. <https://www.sciencedirect.com/science/article/abs/pii/S2214212622000941>
14. High-quality evaluation for invisible watermarking based on discrete cosine transform (DCT) and singular value decomposition (SVD). (2023). *Journal of Applied Intelligent System*. <https://journal.upgris.ac.id/index.php/asset/article/view/17186>
15. FreqMark: Invisible image watermarking via frequency based visual watermarking. (2024). *arXiv*. <https://arxiv.org/html/2410.20824v1>
16. Medical image hybrid watermark algorithm based on frequency domain transformation and deep learning. (2025). *Advanced Intelligent Systems*. <https://advanced.onlinelibrary.wiley.com/doi/full/10.1002/aisy.202400654>
17. A comprehensive review on optimization-based image watermarking techniques. (2024). *Expert Systems with Applications*. <https://www.sciencedirect.com/science/article/abs/pii/S0957417423033328>
18. Blind medical image watermarking based on LBP-DWT for telemedicine applications. (2025). *Circuits, Systems, and Signal Processing*. Mentioned as related current literature in indexed survey listings [4].