DIGITAL WATERMARKING IN IMAGES USING DCT: EMBEDDING, EXTRACTION AND VISUAL QUALITY PRESERVATION

Nenad Stanojević[1]*,
[0009-0004-4158-6412]
Petar Spalević[1],
[0000-0002-6867-7259]
Stefan Panić[2],
[0000-0002-5868-1764]
Đorđe Šarčević[3],
[0000-0003-0746-744X]
Srđan Mitrović[4]
[0009-0006-5105-4270]

[1]University of Priština,
Faculty of Technical Sciences,
Kosovska Mitrovica, Serbia

[2]University of Priština,
Faculty of Sciences,
Kosovska Mitrovica, Serbia

[3]Department of Medical and
Bussines-Technological Studies,
Academy of Professional Studies Šabac,
Šabac, Serbia

[4]Singidunum University
Belgrade, Serbia

Correspondence:
Nenad Stanojević

e-mail:
nenads25@gmail.com

Abstract:

This paper presents an algorithm for embedding and extracting a digital watermark in an image using the Discrete Cosine Transform (DCT). The standard Lenna image was used as the test image, while the watermark was implemented in the form of a chessboard, defined within a simple matrix structure to facilitate implementation. The simulation of the process was carried out using MATLAB software support. This approach enables the visualization of the process, significantly simplifying the embedding and extraction of the digital watermark. In addition to its application in digital image protection, this model can serve as a foundation for analyzing the impact of various transmission channels on an image, such as atmospheric channels in wireless communications. Beyond the DCT, the proposed approach can also be adapted to other frequency domain transformations, such as the Discrete Fourier Transform (DFT) or the Discrete Wavelet Transform (DWT).

Keywords:

Discrete Cosine Transform, Digital Watermark, Algorithm, Frequency Domain.

INTRODUCTION

One of the most challenging issues in today's digital era is protecting data from unauthorized access, sharing, and duplication. The modern digital environment allows easy access to documents while sharing images and video content via social media has become particularly popular. This raises the question of how to protect digital content from misuse. One possible solution is embedding a digital watermark into a selected digital asset to verify authenticity. A digital watermark is a process of embedding protective information into a digital asset, allowing this information to be later extracted for authenticity verification. Digital watermarks can be either visible or invisible. A visible watermark is immediately noticeable within the digital content, whereas detecting an invisible watermark requires appropriate computing tools and software. This technique serves a dual purpose: on one hand, it enables the identification of the source and author of the digital content, while on the other, it provides authors with protection against unauthorized use [1], [2].

DOI: 10.15308/Sinteza-2025-110-116

Various studies have been conducted to find the best approach for designing a model for embedding and extracting digital watermarks. It has been observed that after watermark extraction, distortions occur both in the image itself and in the watermark. Studies [3], [4] present different embedding and extraction models that are structurally most compatible with the human visual system.

The most suitable domains for digital watermarking are the frequency domains. To achieve imperceptibility, the watermark should be embedded in the high-frequency components of the transmitted signal. Conversely, for a robust digital watermark, embedding should be restricted to low-frequency components, with the low-frequency component serving as the 'host' for watermark insertion. In the paper [5], an algorithm combining different transformation schemes (DFT, DCT, SVD, and DWT) is presented. It has been proven that by combining different models, the resistance, robustness, and imperceptibility of the embedded digital watermarks are enhanced. However, due to their complexity, the implementation of such models can often be financially unfeasible. Paper [6] proposes a digital watermarking system for color images in the spatial domain, combining the strengths of both spatial and frequency-domain schemes. The system uses different quantization steps for embedding and blind extraction of the watermark, improving invisibility and reducing the pixel modification range. Experimental results demonstrate that this system offers better invisibility, robustness, and shorter execution time compared to existing methods.

Various methods have been considered with the aim of implementing a digital watermark that satisfies both the conditions of imperceptibility and robustness, while also addressing financial aspects. In [7], a scheme for removing visible watermarks with the possibility of reversible image recovery is presented. This model is one of the most efficient, as it allows for the complete reconstruction of the original image. However, a certain level of degradation is unavoidable.

This paper analyzes the process of embedding and extracting a digital watermark using the Discrete Cosine Transform (DCT), which belongs to the class of frequency domain transformations. The MATLAB environment was used for process analysis, providing a simplified representation of the embedding and extraction procedures for digital watermarking.

2. RELATED WORK

In this section, we examine modern techniques for embedding digital watermarks, focusing on frequency-domain-based methods. We analyze the efficiency and limitations of existing techniques to identify gaps in this key research field.

In [8], [9], a two-dimensional discrete cosine transform (2D-DCT) model for embedding digital watermarks is presented. This method uses mid-frequency components for watermark embedding, ensuring its imperceptibility. The model employs color images for both the original image and the watermark, providing high resistance to attacks, minimal visibility of the embedded watermark, and enabling a high embedding capacity. This approach is particularly suitable for embedding company color logos, contributing to copyright protection. To enhance security and robustness, the color watermark is divided into its primary components (red, blue, and green), followed by Arnold transformation to permute pixels using a private key. Experimental analysis has demonstrated high resistance to compression, filtering, cropping, and scaling. Peak signal-to-noise ratio (PSNR) values exceeded 36 dB, indicating high imperceptibility of the embedded watermark.

In [10], a robust and secure system for embedding digital watermarks based on the encryption of a random binary sequence is presented. This model utilizes second-level DWT (2DWT) combined with DCT to enhance watermark protection and reduce image distortion. DWT is used to decompose the image and isolate low-frequency sub-bands (LL), while 2DWT is applied to improve resistance to filtering and reduce visual artifacts. The use of DCT further enhances watermark embedding by modifying AC coefficients without significantly degrading image quality. Experimental analysis has demonstrated the high robustness of the method against various image processing attacks, including scaling, filtering, compression, sharpening, and noise addition. The advantage of this approach lies in its low error rate in watermark reconstruction along with high imperceptibility, proving its suitability for copyright protection and cybersecurity applications. R. Soundrapandiyan et al. in [11] proposed a model that also employs the DWT-DCT transformation but applies different protection strategies. The model divides the image into regions of interest (ROI) and non-interest regions (NIR), embedding watermarks by quantizing low-frequency coefficients and using zigzag sorting for DCT coefficients. This model has been particularly useful in securing clinical medical images, where watermarks are

used to store sensitive patient data. The system not only ensures the confidentiality and integrity of the medical data but also exhibits high robustness, with PSNR values exceeding 40 dB after watermark extraction. The method has shown resilience against common image processing attacks, ensuring the security of medical images in applications such as telemedicine and patient data protection.

H. Cao et al. [12] present a model for embedding a robust reversible digital watermark using DFT in the spatial domain. The proposed approach utilizes the relationship between the DC component of the DFT and pixel values in the spatial domain to avoid explicit DFT and IDFT transformations, significantly reducing execution time compared to traditional DFT-based watermarking methods. The quantization step is optimized to achieve a balance between imperceptibility and robustness. Robustness ensures copyright protection, while reversibility preserves image integrity and authentication. Experimental analysis has shown that the model enables watermark extraction without loss of original image quality, with good robustness, imperceptibility, and high embedding capacity. Key concepts of this approach include two-dimensional discrete Fourier transform (2D-DFT), DC component modification, and encryption based on logistic chaotic mapping. However, the model's resistance to noise attacks and pixel cropping requires further optimization.

The presented models demonstrate different approaches to digital watermark embedding. Most of the examined approaches achieve good resistance to attacks, high embedding capacity, and reliability; however, they share a common characteristic - focusing solely on invisible watermarks. Invisible watermarks are desirable in many scenarios, particularly in copyright protection, forensic analysis, and digital content authentication, where the goal is to preserve image quality without noticeable alterations. However, in certain cases, there is a need for visible watermarks, such as preventing unauthorized use of images online, marking ownership of digital content, or branding media materials. Visible watermarks enable direct ownership identification and are frequently used in news agencies, stock photo databases, and video platforms, where it is crucial to emphasize the source of an image or video.

While invisible watermarks are effective for hidden content protection, current methods lack flexibility in choosing between visible and invisible watermarking. The development of adaptive techniques that allow controlled watermark visibility could represent a significant advancement in this field. Integrating existing frequency-domain methods with adaptive techniques could enable dynamic selection of watermark visibility depending on the application.

3. DCT (DISCRETE COSINE TRANSFORM)

DCT is one of the most commonly used transformations in the frequency domain. This transformation operates only with real values and decomposes a signal into a combination of cosine functions of different frequencies.

If an image in the spatial domain is represented as the function $f(x, y)$, where it is defined in two dimensions (x and y), the Discrete Cosine Transform (DCT) projects this image into the frequency domain, where the transformed function is denoted as $F(u, v)$.

$$f(x,y) \overset{DCT}{\rightarrow} F(u,v)$$

Equation 1. Transformation from the spatial domain to the frequency domain using DCT

If observation is performed in a one-dimensional domain, the transformation can be represented by the expression:

$$F(u) = c \cdot f(x)$$

Equation 2. One – dimensional DCT

Where c is the cosine transformation matrix. When the matrix c is multiplied by the function $f(x)$, the entire expression takes the form:

$$F(u) = a(u)\sum_{x}^{n-1} f(x)cos\left[\frac{(2x+1)\pi u}{2n}\right] \text{ for } 0 \le u \le n\text{-}1$$

Equation 3. DCT - transform expression

where: $\begin{cases} a(u) = \sqrt{\frac{1}{n}} \text{ if } u = 0 \\ a(u) = \sqrt{\frac{2}{n}} \text{ if } u \neq 0 \end{cases}$

The previous expression represents the matrix used for the 1-D DCT transformation. The process of the 2-D DCT transformation is implemented using the expression:

$$F(u,v) = c \cdot f(x,y) \cdot c^T$$

Equation 4. Two – dimensional DCT

Where c^Trepresents the transposed matrix, and the expression for the 2-D DCT transformation is [4], [13]:

$$F(u,v) = a(u)a(v)\sum_{x}^{n-1}\sum_{y}^{m-1} f(x,y)cos\left[\frac{(2x+1)\pi u}{2n}\right]cos\left[\frac{(2y+1)\pi v}{2m}\right]$$

Equation 5. Two – dimensional DCT – transform expression

where: $\begin{cases} a(u) = \sqrt{\frac{1}{n}} \text{ if } u = 0 \\ a(u) = \sqrt{\frac{2}{n}} \text{ if } u \neq 0 \end{cases}$

where: $\begin{cases} a(v) = \sqrt{\frac{1}{m}} \text{ if } v = 0 \\ a(v) = \sqrt{\frac{2}{m}} \text{ if } v \neq 0 \end{cases}$

If the image is divided into blocks, and each of these blocks is made up of pixels, each pixel represents a small part of the image. The DCT transformation allows these pixels to be represented through a cosine function, and what the previous expression enables is the calculation of coefficients that carry information about the details of the image [13], [14].

The process of embedding a digital watermark into an image using the DCT

For the implementation of this procedure, MATLAB programming support was used. The process of embedding a digital watermark into the image was carried out using the appropriate algorithm.

Step 1: Loading the original image (Figure 1).

Step 2: In this step, the image is vectorially separated into its basic RGB components. Then, using DCT, each component is individually transformed into the frequency domain. The DCT transformation allows the pixels to be represented through a cosine function, and equation (5) enables the calculation of coefficients that carry information about the details of the image [14], [15], [16], [17]. The selected image of dimensions MxN is decomposed into non-overlapping blocks of size m x n, and then each block is transformed into the corresponding DCT coefficients from equation (5).

The blocks resulting from the DCT transformation can be divided into three distinct frequency ranges: low, medium, and high. The low-frequency range contains the most significant information about the image, and modifying it leads to perceptual changes in the image. On the other hand, the high-frequency components have less importance and can be removed for compression purposes [15], [18]. When determining the coefficients, each value is divided according to its weighting factor. Quantization groups the weighting factors in such a way that it maximizes the number of components close to zero while maintaining the image quality. After quantization, a zig-zag transformation is applied, grouping identical values [18], [19], [20], [21], [22]. Figure 2 shows the arrangement of coefficients and their graphical representation.

Step 3: A digital watermark in the form of a chessboard is created by appropriately arranging binary codes "1" and "0" in a matrix structure. The watermark A is created with a resolution of 256x256 (a x b). The matrix is created based on the principle of arranging the fields of a chessboard, where each field consists of 32x32 binary codes, with "1" representing white squares and "0" representing black squares (Figure 3).

Step 4: In this step, the digital watermark is embedded. The embedding process is straightforward, where the binary components in the matrix of the digital watermark are added to the selected DCT coefficients, thus modifying the coefficient values.

$$F'(u,v) = \begin{cases} F(u,v) + Ku \cdot A(a,b) & \text{for } 0 \leq u < a \text{ and } 0 \leq v < b \\ F(u,v) & \text{For all other values} \end{cases}$$

Equation 6. Expression for digital watermark embedding

Where $F'(u,v)$ is the image with the binary digital watermark in the frequency domain. The selection of coefficients is done by adding the first 256×256 elements of the DCT image (for each component individually) to the elements of matrix A. During the addition of the elements of the matrix, the embedding coefficient Ku is also defined, which represents the level of transparency of the digital watermark.

Step 5: After applying the inverse DCT (iDCT), the image with the embedded digital watermark is obtained (Figure 4). The embedding coefficient Ku plays a crucial role in the implementation of the watermark - at certain minimal values, the digital watermark remains imperceptible, while at certain maximal values, it can significantly degrade the image quality, making it unusable until the watermark extraction is performed.

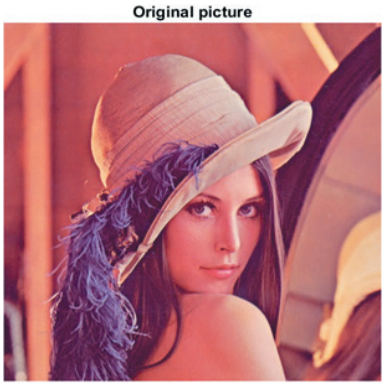

Figure 1. Original picture

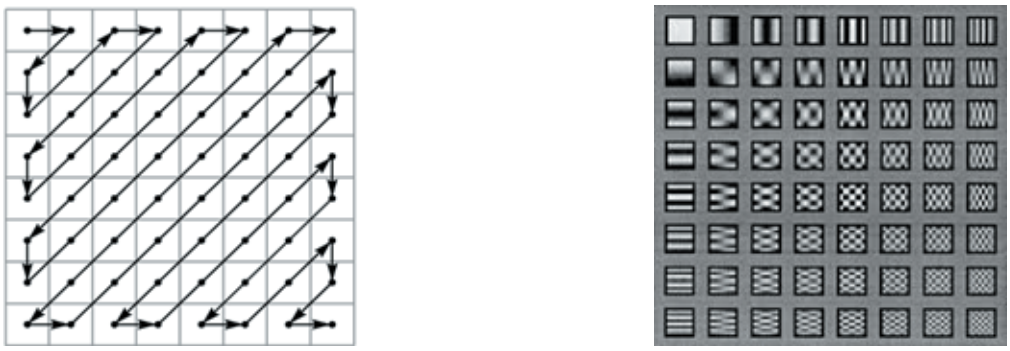

Figure 2. DCT zig-zag distribution of coefficients and frequency distribution of coefficients, respectively [23]

Figure 3. Digital watermark chessboard

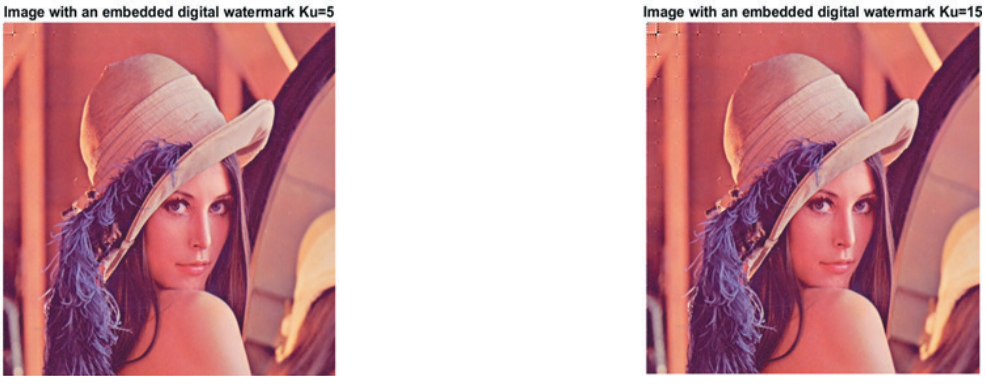

Figure 4. Images with the embedded digital watermark for *Ku*=5 and *Ku*=15, respectively

5. ALGORITHM FOR EXTRACTING THE WATERMARK FROM THE IMAGE

When extracting a watermark from an image, three methods are typically used [16], [19]:

1. Blind method – this approach does not require the original image for watermark extraction.
2. Non-blind method –the original image is necessary for extracting the watermark.
3. Semi-blind method – this method utilizes the original digital watermark or other relevant information for detection.

According to the method of watermark extraction, the Semi-blind method is used in this paper. The extraction process consists of the following steps:

Step 1: The process of determining the coefficients in the frequency domain using DCT is repeated, but this time it is performed on the image with the embedded digital watermark.

Step 2: From the image composed of coefficients created by DCT, the matrix of the digital watermark is subtracted with the same transparency coefficient as in the implementation.

$$F(u,v) = \begin{cases} F'(u,v) - Ku \cdot A(a,b) & \text{for } 0 \le u < a \text{ and } 0 \le v < b \\ F'(u,v) & \text{For all other values} \end{cases}$$

Equation 7. Expression for digital watermark extraction

Step 3: After removing the watermark, the final step involves applying the iDCT, which returns the coefficients to their original state, as before the transformation (Figure 5).

The image obtained after extraction demonstrates exceptional quality, with no visible signs of damage that could have resulted from the application of the DCT transformation and the process of embedding the digital watermark.

However, the proposed model has a certain drawback in terms of security. In addition to the simple scheme of the watermark itself, an additional challenge is the fact that the digital watermark is embedded in the lower frequencies of the DCT image, which can reduce its resistance to attacks. The level of security can be significantly improved by embedding the digital watermark into the middle or higher frequency components of the DCT transformation. Moreover, adding an encryption element, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), or chaos-based encryption methods, could further strengthen the protection and eliminate this drawback. The effectiveness of these methods can be further enhanced by combining them with appropriate transformation domains, such as DWT (Discrete Wavelet Transform) or SVD (Singular Value Decomposition), achieving greater resistance to various attacks and signal degradation.

These possibilities provide a potential foundation for further development of the model and future research in this area.

Figure 5. Code for iDCT and the image after watermark extraction

6. CONCLUSION

This paper explores the process of embedding and extracting a digital watermark in images using the Discrete Cosine Transform (DCT). A method is presented that enables watermark embedding while preserving high image quality. The extraction is performed using the semi-blind method, without requiring the original image, while the inverse DCT (iDCT) is used to restore the image to its original state.

The results show that the proposed method does not degrade image quality after watermark extraction. Additionally, by increasing the embedding coefficient Ku, the transparency level of the digital watermark can be adjusted. Due to its simplicity and ability to preserve visual quality, this approach can facilitate image transmission through communication channels.

The proposed method has potential applications in copyright protection and digital content authentication. Future research could focus on enhancing its robustness against compression and extending its application to dynamic media, such as video.

REFERENCES

[1] I. J. Cox, M. . L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography," *Morgan Kaufman Publisher*, 2008.

[2] O. Evsutin, A. Melman and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access,* vol. 8, pp. 166589-166611, 2020.

[3] A. Dixit and R. Dixit, "A Review on Digital Image Watermarking Techniques," *International Journal of Image, Graphics and Signal Processing,* pp. 56-66, 2017.

[4] M. Kaur, S. Jindal and S. Behal, "A study of digital image watermarking," *IJREAS,* vol. 2, p. 126–136, 2012.

[5] J. Varghese, B. O. Hussain, A. Razak T. and S. Sabash, "A Hybrid Digital Image Watermarking Scheme Incorporating DWT, DFT, DCT and SVD Transformations," *PeerJ Computer Science*, vol. 10, no. 1A, pp. 113-130, 2022.

[6] Z. Yuan, O. Su, D. Liu and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *The visual computer*, vol. 37, p. 1867–1881, 2021.

[7] C. C. Chen, Y. H. Tsai and H. C. Yeh, "Difference-expansion based reversible and visible image watermarking scheme," *Multimedia Tools Appl.*, vol. 76, p. 8497–8516, 2017.

[8] Z. Yuan, D. Liu, X. Zhang and Q. Su, "New image blind watermarking method based on two-dimensional discrete cosine transform," *Optik*, 2020.

[9] H. Wang, Z. Yuan, S. Chen and Q. Su, "Embedding color watermark image to color host image based on 2D-DCT," *Optik*, 2023.

[10] N. Hasan, M. S. Islam, W. Chen, M. A. Kabir and S. Al-Ahmadi, " Encryption Based Image Watermarking Algorithm in 2DWT-DCTDomains," *Sensors*, vol. 21, no. 16, 2021.

[11] R. Soundrapandiyan, K. Rajendiran, A. Gurunathan, A. Victor and R. Selvanambi, "Analysis of DWT–DCT watermarking algorithm on digital medical imaging," *Journal of Medical Imaging*, vol. 11, no. 1, 2024.

[12] H. Cao, H. Fu, Y. Sun, S. Chen and Q. Su, "Robust and reversible color image watermarking based on DFT in the spatial domain," *Optik*, 2022.

[13] A. B. Watson and NASA Ames Research Center, "Image compression using discrete cosine transform," *Mathematica journal,* vol. 4, no. 1, pp. 81-88, 1994.

[14] V. Singh, "Digital Watermarking: A Tutorial," *JSAT*, 2011.

[15] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU-International Journal of Electronics and Communications,* vol. 72, pp. 149-161, 2017.

[16] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," In *Information hiding,* pp. 43-78, 2000.

[17] W. Chu, "DCT-based image watermarking using subsampling," *IEEE Trans. Multimedia*, vol. 5, no. 1, p. 34 – 38, 2003.

[18] M. Jiansheng, L. Sukang and T. Xiaomei, "A digital watermarking algorithm based on DCT and DWT," *In Proceedings. The 2009 International Symposium on Web Information Systems and Applications*, (WISA 2009), p. 104, 2009.

[19] M. I. Khan, M. M. Rahman and M. I. Sarker, "Digital watermarking for image authenticationbased on combined dct, dwt and svd transformation," *arXiv preprint arXiv:1307.6328*, 2013.

[20] R. A. Asmara, and R. Agustina, "Comparison of discrete cosine transforms (DCT), discrete Fourier transforms (DFT), and discrete wavelet transforms (DWT) in digital image watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 2, 2017.

[21] S. Katzenbeisser and F. Petitcolas, "Information hiding," *Artech house*, 2016.

[22] S. M. Aghajanzadeh and M. Uysal, "Diversity-multiplexing trade-off in coherent free-space optical systems with multiple receivers," *J. Opt. Commun. Netw*, vol. 2, pp. 1087-1094, 2010.

[23] M. Baechler and J. L. Bloechle, "Labeled images verification using gaussian mixture models," In *Proceedings of the 2009 ACM symposium on Applied Computing*, pp. 1331-1335, 2009.