




Open Access Article

 <https://doi.org/10.55463/issn.1674-2974.50.10.13>

Triple Watermarking Scheme for Digital Images

Emmanuel Oluwatobi Asani^{1,2,3}, Moyinoluwa Gbenga-Degun¹, Sunday Adeola Ajagbe^{4,5*}, Peace Busola Falola⁶, Emmanuel A. Adeniyi⁷, Matthew O. Adigun⁴

¹ Department of Computer Science, Landmark University, Nigeria

² Landmark University SDG 11 Group, Landmark University, Nigeria

³ Department of Computing, MIVA University, Nigeria

⁴ Department of Computer Science, University of Zululand, Kwadlangezwa, 3886, South Africa

⁵ Department of Computer Engineering, First Technical University, Ibadan, 200255, Nigeria

⁶ Department of Computer Sciences, Precious Cornerstone University, Ibadan, Nigeria

⁷ College of Computing & Communication Studies, Bowen University, Iwo, Nigeria

* Corresponding author: 230015266@stu.unizulu.ac.za

Received: July 5, 2023 / Revised: August 1, 2023 / Accepted: September 9, 2023 / Published: October 31, 2023

Abstract: Digital watermarking of text, image, and video data has become an indispensable strategy for the authentication, validation, and ultimate protection of digital content. This study aims to develop a resilient, imperceptible watermarking scheme for digital images. A triple transform domain watermarking scheme based on stationary wavelet transform (SWT), discrete cosine transform (DCT), and singular value decomposition (SVD) is presented as a comprehensive, adaptable, and resilient solution for safeguarding digital content in a dynamic digital environment. The proposed scheme leverages the unique strengths of SWT, DCT, and SVD. SWT was used to decompose the image into various frequency bands, whereas DCT was applied to these high-frequency components, enhancing the security of the watermark. SVD was then used to decompose the image matrix into singular values, providing further robustness. The watermarking algorithm was designed to be both imperceptible and robust against various attacks. The imperceptibility and robustness of the scheme were evaluated on three publicly available datasets using metrics such as mean square error (MSE), peak signal-to-noise ratio (PSNR), normalized cross correlation (NCC), and bit error ratio (BER). The results indicate that the SWT-DCT-SVD watermarking scheme is both robust and imperceptible and compares relatively well with state-of-the-art schemes.

Keywords: watermarking, zigzag process, stationary wavelet transform, discrete wavelet transform, discrete cosine transform, embedding, extraction.

数字图像三重水印方案

摘要：文本、图像和视频数据的数字水印已成为数字内容的认证、验证和最终保护不可或缺的策略。本研究旨在为数字图像开发一种有弹性、难以察觉的水印方案。基于平稳小波变换(斯威特)、离散余弦变换(离散余弦变换)和奇异值分解(奇异值分解)的三重变换域水印方案被提出，作为一种全面的、适应性强且有弹性的解决方案，用于在动态数字环境中保护数

字内容。所提出的方案利用了斯威特、离散余弦变换和奇异值分解的独特优势。斯威特用于将图像分解为各个频段，而离散余弦变换则应用于这些高频分量，增强了水印的安全性。然后使用奇异值分解将图像矩阵分解为奇异值，从而提供进一步的鲁棒性。水印算法被设计为既难以察觉又对各种攻击具有鲁棒性。使用均方误差(均方误差)、峰值信噪比(峰值信噪比)、归一化互相关(NCC)和误码率(误码率)等指标在三个公开可用的数据集上评估该方案的不可感知性和鲁棒性。结果表明，斯威特-离散余弦变换-奇异值分解水印方案既稳健又不易察觉，并且与最先进的方案相比效果较好。

关键词： 水印、锯齿形处理、固定小波变换、离散小波变换、离散余弦变换、嵌入、提取。

1. Introduction

With the rapid adoption and proliferation of Information and Communication Technologies (ICT) and allied infrastructure, there has been an astronomical explosion in the volume of data creation, usage, processing, and transmission. Multimedia data such as images, audio, and video are being processed, stored, and transmitted in unprecedented volumes and at low cost [1]. This has had a devastating impact on data security and integrity, as instances of data breach, theft, and copyright infringement have increased astronomically, resulting in an increased drive for digital data protection [2]-[4]. Two complementary techniques, encryption and watermarking, have been used in research and practice to combat data infringements and copyright breaches for digital material. Digital data can be protected via encryption as it is being transferred from the source to the recipient. However, encryption is limited in providing in-storage protection of decoded data from infringements and unauthorized use [3], [5]. Digital watermarking, on the other hand, protects against data theft and copyrighting and helps in image marking, verification, and data hiding [6].

The primary goal of digital watermarking is to relay undetectable user-unique graphic imprints that function by slightly modifying the content of the media. The embedded watermark should be unnoticeable and strong enough to withstand hostile assault distortions and regular signal distortions. Because the watermark is obscure, a robustness attribute must be present to ensure that the watermark data are preserved if the image is altered [1], [6]. Additionally, it is important to develop a watermark embedding method that gives an imperceptible mark, i.e., one that does not substantially alter the original host signal. Invariably, imperceptibility and robustness are two important design considerations in the development of watermarking systems. Generally, watermarking can be done on text, audio, images, and videos [7].

The core requirements/design considerations for the development of an effective watermarking scheme include imperceptibility, robustness, security, and computational cost. It is critical for a watermark to be imperceptible. In essence, the watermarked image must appear exactly like the original image. They should be perceptually indistinguishable by humans despite minor variations in luminance or visual contrast. As a result, the image quality must not be sacrificed [3]. Robustness is the capacity of a watermark to be recognized even after the use of many common signal processing alteration techniques. Lossy compression, spatial filtering, color mapping, examining and publishing, scaling, interpreting, and spinning are some examples of these methods. Several generic ways to achieve high robustness include watermarks for duplicated integration, spread spectrum, embedding, and so on. Invariably, an effective digital picture watermarking system should be resistant to a variety of attacks such as noise, cryptographic, and protocol attacks, ensuring that watermark data cannot be removed or excluded by unauthorized distributors [6]. For further security, the watermark can be placed in many locations in the image so that if one is lost or erased, the other remains [8]. The watermark should be embedded and extracted securely to ensure that the objective of watermarking is not compromised. Insecure watermarking technologies make copyright safeguarding, data authorization, fingerprinting, and monitoring of electronic data difficult. As a result, security is prioritized in digital image watermarking systems. Various encryption methods may be deployed to determine security, with the degree of security determined by the key. To secure the integration of watermark privacy and secrecy, several methods have been explored, such as encryption methods based on chaos, discrete cosine transform (DCT), and logistic maps [7]. Since the attacker will be deterred from looking for the insertion in an embedding space and long key position, the complexity of the watermark

may also be crucial to security. As a result, it is feasible to increase the size of the keys split into small pieces of cover picture to strengthen the algorithm security [9]. Of equal importance is the total time required to embed and extract a watermark [9]. However, considering cost as the primary motivation for studying complexity should be kept to a minimum. The speed of embedding and detection, and the quantity of embedders and detectors, are the two most important aspects of computational cost [9]. To have a good watermarking system, a healthy balance of toughness and cost must be maintained [6].

Watermarking techniques broadly classified as spatial domain and frequency domain techniques have been extensively explored. Spatial domain watermarking schemes achieve watermarking by altering the pixel value in the spatial domain. This approach is preferable in terms of implementation and complexity and is therefore often used in both research and practice [7]. For instance [10] presented a watermarking scheme that deployed LSB Substitution and Hill Cipher to enhance its security. They embedded the scheme in the spatial domain to improve its imperceptibility and interleaved it specifically within the block of the cover image that had the maximum value. The scheme was simulated on image data and evaluated for its concealment abilities based on both subjective and objective image quality assessment metrics. The results showed very promising performances relative to state-of-the-art techniques and robustness against popular attacks such as Gaussian filter and median filter attacks. The authors of [11] introduced a novel spatial-based scheme for colored image watermarking. Motivated by the established literature premises that spatial domain approaches generally produce fragile watermarking schemes, the authors extended the approach by introducing scalable diffusion of watermark information across a pixel region, similar to the transform domain approach to watermarking. This ensured that the images' high quality remained uncompromised and the technique remained resilient against attacks. Additionally, it guaranteed that any alteration in the color component was effectively adjusted to, ensuring that color variation or alterations were not visually observable. The scheme was then simulated and evaluated. The experimental results showed that the scheme was resilient against attacks and showed promising performances in terms of imperceptibility. Leveraging on the merits of the spatial domain and frequency-domain watermarking approach, [12] presented a watermarking technique that deployed discrete cosine transform (DCT) in the spatial domain. They explored the use of basic color layer quantization to accomplish watermarking and blind extraction in the spatial domain via pseudo-DCT. The technique leverages the network of intra-pixel association of DC coefficients in

adjacent pixel blocks. Experimental results on image data showed that compared with state-of-the-art techniques, the scheme offered superior imperceptibility, improved resilience, and optimized real-time performance. A robust digital watermarking scheme for digital images based on the DWT-SVD algorithm was presented in [13]. The hybridized technique combined discrete wavelet transform (DWT) and singular value decomposition (SVD) and applied the watermark over the unique values of the cover image sub-bands. The simulation results showed that the technique was capable of significantly improving imperceptibility while maintaining perceptual quality. The MSE, PSNR, and SSIM values obtained revealed that DWT-SVD was remarkably robust when subjected to various image signal processing attacks. While spatial domain watermarking schemes have been embraced due to their simplicity and real-time applicability, their key flaw, as established in the literature, is that they are optimized only for images that are free of noise. They are also susceptible to cropping attacks because of the simplicity of their design. Consequently, attention is shifting to frequency domain watermarking schemes, which address these notable limitations of spatial domain watermarking schemes.

Transform domain techniques offer increased security, imperceptibility, and resilience against a multitude of signal processing assaults and are often deployed on the basis of schemes such as DCT, discrete wavelet transforms, discrete Fourier transform (DFT), and matrix decomposition [12]. A watermarking technique was developed in [14] based on block-based discrete cosine transform (DCT) coefficient change. The DCT parameters of two blocks were computed and adjusted based on the watermark bit within a predetermined range. The DCT coefficient and median of the AC coefficients organized by a zigzag sequence determined the degree of DCT coefficient alterations. Experiments showed that the technique was extremely resistant to various single and combined attacks. They noted that the solution is more efficient for electronic copyright safeguarding photos than some state-of-the-art methods. The discrete shearlet transform (DST) was presented in [15] as a novel embedding technique for blind picture watermarking. The unique DST blind watermark detection system used a non-additive mechanism based on statistical decision theory. PDF is calculated using the DST coefficients, which are modeled as a Laplacian distribution. The likelihood ratio and decision threshold were compared to reduce missed detection due to a fixed false alarm probability. Thirty typical grayscale photos were used, each with different attributes, to evaluate the proposed technique when employed against diverse assaults. The payload, robustness, and imperceptibility of the system were evaluated. The technique outperforms discrete wavelet

and contourlets in terms of windowing flexibility and sensitivity to directional and anisotropic characteristics. A wavelet-based threshold classification technique was developed in [16] for digital image watermarking. The technique separates the original image into several sections that are chosen to embed the watermark. The DWT coefficient was then categorized using lower frequency sub-bands. Additional tests were run, and the results showed that the system was robust and imperceptible.

While the performances of state-of-the-art single transform watermarking techniques have been remarkable, they not be able to satisfy all the fundamental design objectives of a watermarking system. Hybrid transform domain approaches that synergize the strengths of different techniques have been proposed to improve the overall performance of watermarking systems in terms of robustness, security, imperceptibility, scalability, flexibility, and adaptability. For instance, a fractal encoding method was developed in [17] based on the DCT digital watermarking algorithm. This approach integrates the fractal encoding and DCT methods to improve the previous DCT method, allowing the encryptions to be doubled. Fractal encoding was used to encode the image in the manner of the first encryption. The encoded parameters were then employed within the DCT method to accomplish the second encryption. The simulation findings obtained showed that the technique's performance in terms of robustness and PSNR was superior to that of ordinary DCT.

A method suggested in [18] hybridized DWT with DCT to achieve a high-quality digital watermark. This was based on the idea that the use of suitable transforms in conjunction with the DWT had the potential to increase the performance of the watermarking system. Digital watermarking was accomplished by embedding the hidden picture on DWT sub-bands of the image and then conducting DCT on the chosen DWT sub-bands. Compared to the current watermarking strategy, the proposed approach increased watermarking clarity and attained imperceptibility and resilience. The PSNR and MSE values of the results were used to examine them. When compared to other commonly used approaches, the estimated PSNR and MSE values showed that watermarking has no impact on image quality.

While state-of-the-art single and dual watermarking schemes, which are based on algorithms such as stationary wavelet transform (SWT), discrete cosine transform (DCT), singular value decomposition (SVD), and so on, have shown remarkable promises in their performances, the underlying weaknesses of individual methods continue to accentuate limitations in terms of resilience against a wide spectrum of attacks, imperceptibility, security, adaptability to complex emerging attacks, and so on. Thus, this study presents a

resilient and undetectable implementation of the SWT-SVD-DCT system. This study contributes to knowledge by proposing a novel digital image watermarking scheme that uses three different watermarks, each of which is embedded in a different frequency band of the host image. This makes the watermarked image more robust to attacks, as it would be more difficult to remove all three watermarks without significantly degrading the quality of the image. The techniques used in this study help protect copyrights of digital images and prevent the unauthorized use of digital images.

This study is organized into four sections. Section 2 presents a detailed representation of the methodology used in this study. Section 3 presents the experimental results and discussion using tables and figures, and section 5 concludes the study.

2. Methodology

Given the multifaceted nature of digital copyright infringements and the need to provide effective solutions and significantly improve the performance of existing techniques, we present a triple transform domain watermarking scheme based on stationary wavelet transform (SWT), discrete cosine transform (DCT), and singular value decomposition (SVD). SWT, DCT, and SVD offer complementary attributes, making them suitable for hybridization into a robust and adaptable watermarking approach. The hybridized scheme harnesses the strength of each of these domains and compensates for their limitations. In the following subsection, we present the component methods.

2.1. Stationary Wavelet Transform (SWT)

Stationary wavelet transform (SWT), also referred to as undecimated wavelet, extends discrete wavelet transform (DWT) and addresses DWT's so called 'translation invariance' by eliminating downsampling and upsampling at every transformation level. Each level of the output generated by SWT has the same number of samples as the input. When the SWT transform is applied to an image, the image is divided into four sub-bands of high and low bands LL, LH, HL, and HH. SWT was the preferred wavelet transformation in this study because, unlike other wavelet transforms, it does not require any downsampling stages and instead uses a null placement process with the same length as the original sequence. Filters are updated at each level by padding them with zeros [19].

2.2. Discrete Cosine Transform (DCT)

DCT manipulates the frequency components of an image to convert it into a transform domain. Only real values are used in DCT, which is the sum of cosine functions. The data decorrelation and energy compaction qualities of DCT make it an orthogonal

transformation. It is used to compress JPEG images. The following equation determines the discrete cosine transform (DCT) [20]:

$$C(a, b) = \alpha(a)\alpha(b) \sum_{p=0}^{M-1} \sum_{q=0}^{M-1} f(y, z) \cos \left[\frac{\pi(2y+1)a}{2M} \right] \cos \left[\frac{\pi(2z+1)b}{2M} \right] \quad (1)$$

For $a, b = 0, 1, 2, \dots, M-1$ and $\alpha(a)$ and $\alpha(b)$ are defined in equation 4.

$$\alpha(m) = \begin{cases} \frac{1}{\sqrt{m}} & \text{for } a = 0 \\ \sqrt{\frac{2}{M}} & \text{for } a \neq 0 \end{cases} \quad (2)$$

The inverse transform is defined as

$$f(y, z) = \sum_{p=0}^{M-1} \sum_{q=0}^{M-1} \alpha(a)\alpha(b)C(a, b) \cos \left[\frac{\pi(2y+1)a}{2M} \right] \cos \left[\frac{\pi(2z+1)b}{2M} \right] \quad (3)$$

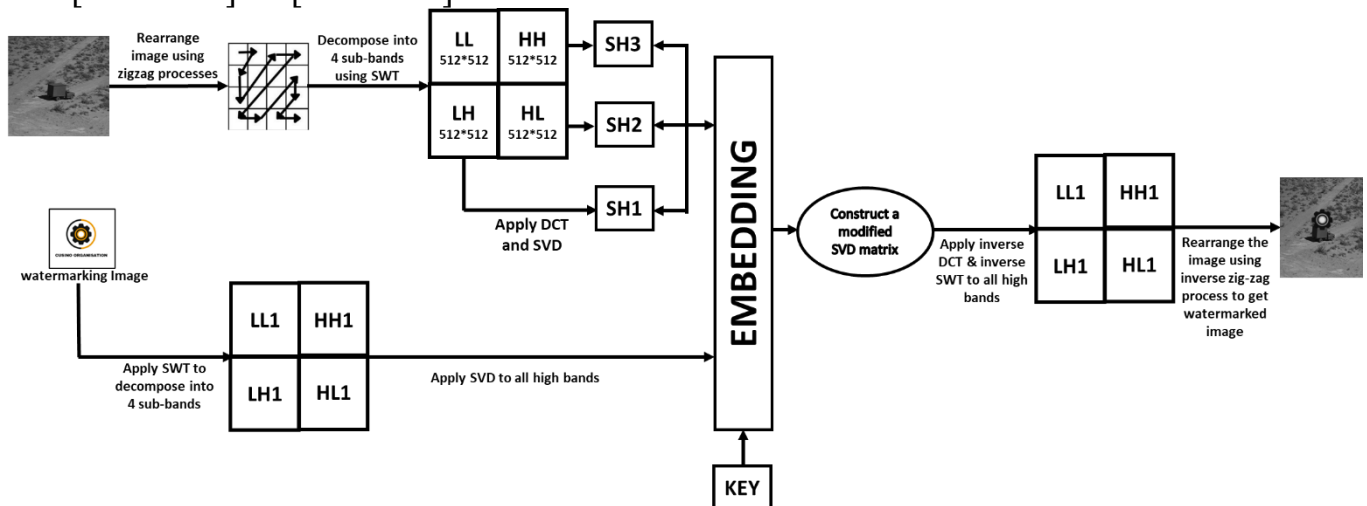


Fig. 1 Framework of the triple embedding algorithm

The triple watermarking algorithm is presented in Algorithm 1.

Algorithm 1 SWT–DCT–SVD watermarking algorithm

Input: Original Image

Output: Watermarked image

1. Input the original image HI;
2. Apply zigzag transformation to reposition the host picture HI to produce the rearranged image RI;
3. Decompose RI into four sub-bands: LL, HL, LH, and HH using SWT;
4. Select all the high bands of LL, HL, LH, and HH, and then apply DCT and SVD to all to obtain SH1, SH2, and SH3;
5. Using a single-level SWT, divide the watermark image into four sub-bands: LL1, HL1, LH1, and HH1;
6. Using the equation $S_{wi} = S_i + S_w$ where $i = 1, 2, 3$, modify SH1, SH2, and SH3;
7. Construct LL, LH11, HL11, and HH11 using the modified SVD matrix;
8. Apply inverse DCT to all high bands of LL11, LH11, HL11, and HH11;

2.3. Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) represents a matrix decomposition module deployed to break a matrix into three simpler forms to provide explicit details of its attributes. Given an original image I, the SVD, when applied, decomposes it into three finer matrices X, Y, and Z with the following mathematical relation:

$$A = X\Sigma Z_o^T \quad (4)$$

where A is the original image matrix, X and Z are orthogonal matrices, signifying the left and right singular vectors, respectively, Σ (Sigma) is a diagonal matrix made up of the singular values and Z_o^T is the transpose of orthogonal matrix Z [19].

2.4. Hybrid SWT–DCT–SVD Design

The hybrid domain technique presented in this study involves the stepwise deployment of SWT, DCT, and SVD to achieve transform domain watermarking. Figure 1 presents the framework and components of the triple watermarking system.

9. Apply the inverse SWT (iSWT);
10. Using the inverse zigzag technique, move the image back to its original location to create the watermarked image WI.

First, the original image was made to undergo zig-zag transformation to re-arrange it into a 2-D matrix. Figure 2 represents the zig-zag process graphically. Thereafter, the SWT transform was applied to re-arrange the image matrix, decomposing it into four sub-bands. The re-arranged image's high bands were subjected to DCT and SVD. A similar SWT decomposition was applied to the high bands of the watermark image, followed by SVD and DCT. To obtain a watermarked image, the singular matrix of the watermark image was implanted into the singular matrix of the host image using a key.

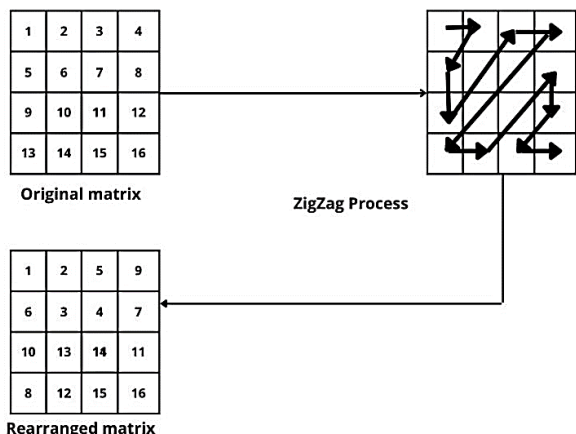


Fig. 2 Zig-zag process

Figure 3 presents a flow diagram of the watermarking process.

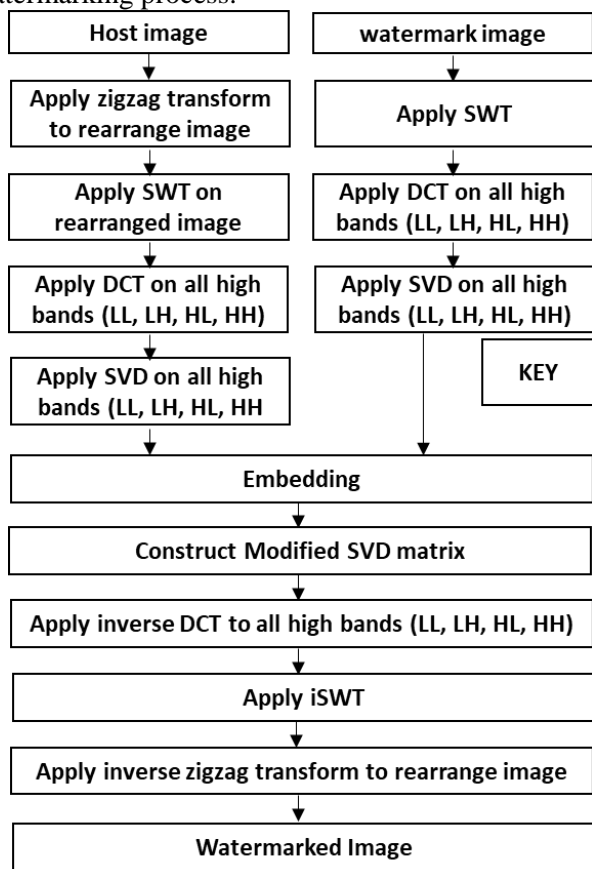


Fig. 3 SWT-DCT-SVD watermark embedding process

2.5. Extraction Phase

The extraction phase is the inverse of the embedding phase. The process is depicted in Algorithm 2.

Algorithm 2 SWT-DCT-SVD extraction algorithm

- Input:** Watermarked image
Output: Host Image
1. Input the watermarked image WI;
 2. Apply zigzag transformation to rearrange the watermarked image WI to produce the rearranged image RI*;
 3. Apply SWT to decompose RI* into four sub-bands: LL*, HL*, LH*, and HH*;
 4. Apply DCT to all high bands of the rearranged image;
 5. Apply SVD to all high bands of the rearranged image;

6. Compute the singular value for all high bands and modify each by using the equation $S_w = S_{wi} + S_i$ where $i = 1,2,3$;
7. Construct modified SVD matrix LL1*, HL1*, LH1*, and HH1*;
8. Apply inverse DCT (iDCT) to all high bands;
9. Apply inverse SWT (iSWT) to all sub-bands to obtain the watermark image.

Figure 4 presents a flow diagram of the triple extraction process.

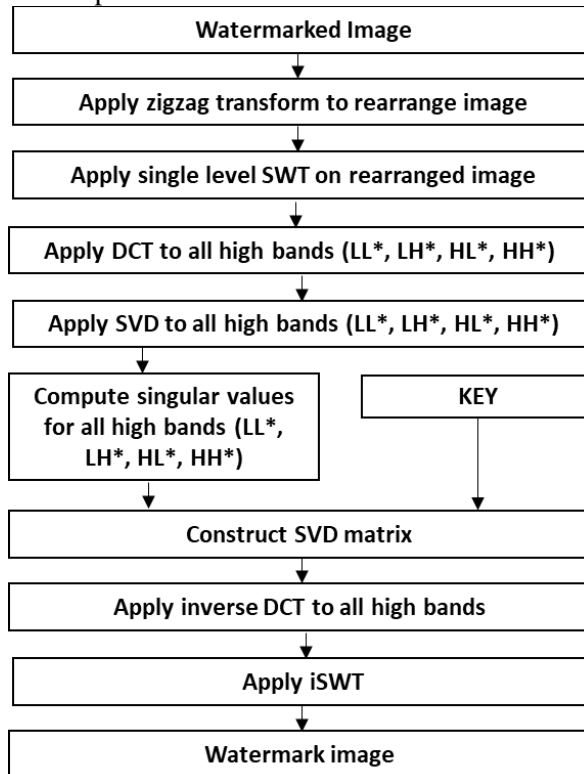


Fig. 4 SWT-DCT-SVD watermark extraction process

3. Experimental Results and Discussion

We experimented with the SWT-DCT-SVD watermarking algorithm on three (3) different 512x512, 8-bit depth 64x64 grayscale images downloaded from the USC-SIPI picture database. The watermarking scheme was simulated using Python programming language and Jupyter Lab as the IDE tool. Figure 5 presents the original images.



Fig. 5 Original images: (a) ship, (b) airplane, (c) truck

Two (2) watermark images presented in Figure 6 were equally used for the experimental procedure.

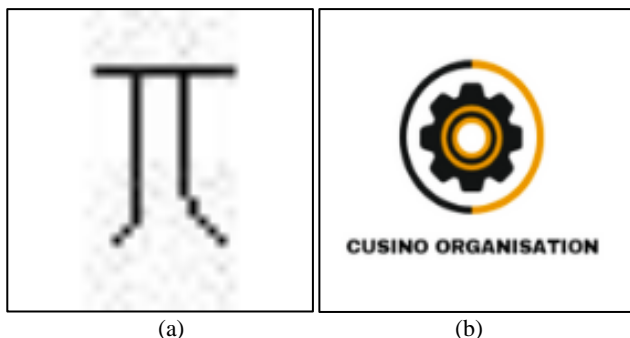


Fig. 6 Watermark images: (a) Pie, (b) Cusino organization logo

The original images and watermark images were used for the overall analysis of the triple watermarking scheme, which included mean square error (MSE), peak signal-to-noise ratio (PSNR) for imperceptibility analysis, normalized correlation coefficient (NCC) and bit error ratio (BER) for robustness analysis.

3.1. Imperceptibility Analysis

Imperceptibility analysis was carried out on the images that had been watermarked using the SWT-DCT-SVD watermarking scheme to establish that the quality of the original images had not been significantly distorted by the watermark. This is typically determined by computing the PSNR and MSE values of the original and watermarked images.

The mean square error is given by equation 5.

$$MSE = \frac{1}{PxQ} \sum_{p=1}^P \sum_{q=1}^Q [1(p, q) - 1_w(p, q)]^2 \quad (5)$$

In equation 5, (p, q) is the original image and $1_w(p, q)$ is the watermarked image of size PxQ , respectively.

The formula used for calculating the PSNR is given in equation 6:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (6)$$

Figure 7 shows the original images side by side with their watermarked images and their MSE and PSNR results.

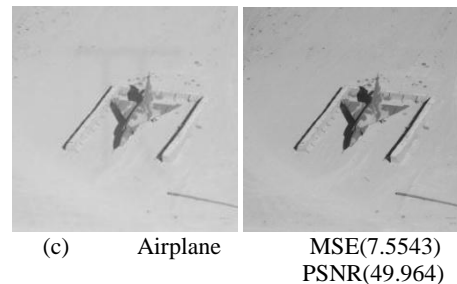
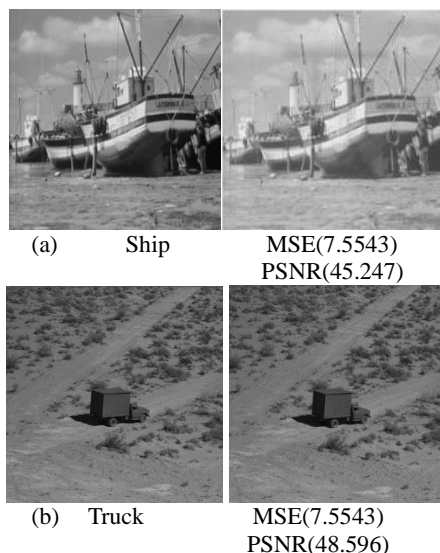


Fig. 7 Original images side by side with their watermarked images and their MSE and PSNR results: (a) Ship side by side with its watermarked version and its MSE and PSNR score, (b) Truck side by side with its watermarked version and its MSE and PSNR score, (c) Airplane side by side with its watermarked version and its MSE and PSNR score

The results showed that the MSE for the three images ranged on average at approximately 7.5, suggesting that the visual quality of the original images was not significantly altered; thus, they are less perceptible.

The PSNR for the three images ranged between 45 and 49, indicating that the watermark is less noticeable to human observers; thus, the scheme can be said to be less perceptible.

3.2. Robustness Analysis

Robustness analysis was performed to determine that the watermark was immune to degradation and other signal processing attacks. We used two generally accepted metrics, namely, the normalized correlation coefficient (NCC) and bit error ratio (BER), to establish this. The formula used in measuring NCC is given in equation 7, and the formula used in computing BER is stated in equation 8.

$$NCC = \frac{\sum_x \sum_y w(x, y) w_{i,j}^i}{\sum_x \sum_y |w(x, y)|^2} \quad (7)$$

$$BER(o, w) = \frac{\sum_{x=1}^M \sum_{y=1}^M \otimes o * (x, y)}{M^2} \quad (8)$$

Table 1 shows the NCC and BER scores of the SWT-DCT-SVD scheme on the images.

Images	NCC	BER
Truck	0.9987	0.0081
Airplane	0.9889	0.0075
Ship	0.9989	0.0075

The result showed that the NCC for the three images ranged on average from approximately 0.98 to 0.99, a very high ratio that is a pointer to the quality and fidelity of the scheme. It is also indicative that the watermarked image retains the properties and structure of the original image. The SWT-DCT-SVD watermarking scheme may therefore be adjudged robust having carried out watermarking with minimal distortion

The BER for the three images ranged on average

between 0.75 and 0.81, a low ratio indicating the SWT-DCT-SVD's resilience against attacks such as compression and noise and ability to retrieve the watermark, even in the presence of various attacks or distortions.

A digital image watermarking method using SWT-DCT-SVD was designed and simulated using publicly available image data. The experimental evaluation of the technique, using metrics such as PSNR, MSE, NCC, and BER, demonstrated a significant level of resilience against various attacks, robustness, and imperceptibility, despite the noisy nature of the images used. It is also noted that, while the literature that used exact list image data for simulation is sparse, we assessed that the SWT-DCT-SVD watermarking scheme performed comparatively well against similar schemes such as [13], [20]-[22].

4. Conclusion

This study's contribution to the frontiers of information security is highlighted in the innovative combination of three transform domains: stationary wavelet transform (SWT), discrete cosine transform (DCT), and singular value decomposition (SVD). Each of these domains is embedded in a different frequency band of the host image. This makes the watermarked image more robust to attacks because it would be more difficult to remove all three watermarks without significantly degrading the quality of the image. The integration of these three domains is a unique approach that leverages their complementary strengths to enhance watermarking performance. By incorporating the robustness of DCT and SVD into the watermarking process, the proposed scheme can withstand various signal processing attacks. The high values of normalized cross correlation (NCC) and low bit error ratio (BER) are indicative of the scheme resilience against common attacks, such as compression and noise, ensuring watermark retrieval even in the presence of distortions. The study was also able to successfully balance imperceptibility and robustness, as indicated by its PSNR and MER performance.

While it is established in the literature that SWT, DCT, and SVD are complementary algorithms, their hybridization nevertheless increased the computational cost. Therefore, it is suggested that future studies consider the integration of optimization schemes to reduce this concern.

References

- [1] HUSSEIN E. and BELAL M A. Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey. *International Journal of Engineering Research & Technology*, 2012, 1(7): 12-23.
- [2] ASANI E O, BIETY-NWANJU G, ADENIYI A E, et al. Development of an Image Encryption Algorithm using Latin Square Matrix and Logistics Map. *International Journal of Advanced Computer Science and Applications*, 2023, 14(9): 869-877. <http://dx.doi.org/10.14569/IJACSA.2023.0140991>
- [3] ASANI E O, OMOTOSHO A, DANQUAH P A. et al. A Maximum Entropy Classification Scheme for Phishing Detection using Parsimonous Features. *TELKOMNIKA Telecommunication Computing Electronics and Control*, 2021, 19(5): 1707-1714. <http://doi.org/10.12928/TELKOMNIKA.v19i5.15981>
- [4] RAWAT R, OKI O A, SANKARAN K S, et al. A New Solution for Cyber Security in Big Data Using Machine Learning Approach. In *Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies*, 166, Springer, Singapore, 2023: 495-505.
- [5] ADESINA, AJAGBE S A, ODULE T J, and AGBELE K K. Development of an Improved School Information Management System. *FUW Trends in Science & Technology Journal*, 2022, 7(1): 120-132.
- [6] BEGUM M, and UDDIN M S. Digital Image Watermarking Techniques: A Review. *Information*, 2020, 11(2): 110-119.
- [7] TAHERA L A, and HEMACHANDRAN K. Digital Image Watermarking Techniques and its Applications. *International Journal of Engineering Research & Technology*, 2013, 2(3): 23-43.
- [8] PAYAL K, and NAVJOT K. A Review on Digital Image Watermarking. *International Journal of Engineering Research & Technology*, 2015, 4(12): 14-29.
- [9] HAI T, and LI C. Robust Image Watermarking Theories and Techniques: A Review. *Journal of Applied Research and Technology*, 2014, 12(1): 18-29.
- [10] KUMAR S, and SINGH B K. Entropy based spatial domain image watermarking and its performance analysis. *Multimedia Tools and Applications*, 2021, 80: 9315-9331. <https://doi.org/10.1007/s11042-020-09943-x>
- [11] ABRAHAM J, and PAUL V. An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University - Computer and Information Sciences*, 2019, 31(1): 125-133. <https://doi.org/10.1016/j.jksuci.2016.12.004>
- [12] YUAN Z, SU Q, LIU D, ZHANG X, and YAO T. Fast and robust image watermarking method in the spatial domain. *IET Image Processing*, 2020, 14(15): 3829-3838. <https://doi.org/10.1049/iet-ipr.2019.1740>
- [13] POONAM and ARORA S M. A DWT-SVD based Robust Digital Watermarking for Digital Images. *Procedia Computer Science*, 2018, 132: 1441-1448. <https://doi.org/10.1016/j.procs.2018.05.076>.
- [14] ABDULLATIF M, ZEKI A M, CHEBIL J, and GUNAWAN T S. Properties of digital image watermarking. *Proceedings of the 2013 IEEE 9th International Colloquium on Signal Processing and its Applications*, Kuala Lumpur, Malaysia, 2013: 235-240. <https://doi.org/10.1109/CSPA.2013.6530048>.
- [15] AHMADERAGHI B, KURUGOLLU F, DEL RINCON J M, and BOURIDANE A. Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. *IEEE Transactions on Computational Imaging*, 2018, 4(1): 46-59.
- [16] CHEN Z, CHEN Y, HU W, and QIAN D. Wavelet Domain Digital Watermarking Algorithm Based on Threshold Classification. In: TAN Y, SHI Y, BUARQUE F,

et al. (Eds) *Advances in Swarm and Computational Intelligence*. ICSI 2015. *Lecture Notes in Computer Science*, 9142: 129-136. Springer, Cham. https://doi.org/10.1007/978-3-319-20469-7_15.

[17] LIU S, PAN Z, and SONG H. Digital image watermarking method based on DCT and fractal encoding. *IET Image Processing*, 2017, 11(10): 815-821.

[18] JOSEPH H, and RAJAN B K. Image Security Enhancement using DCT & DWT Watermarking Technique. *Proceedings of the International Conference on Communication and Signal Processing*, Chennai, India, 2020, pp. 0940-0945, <https://doi.org/10.1109/ICCSP48568.2020.9182052>.

[19] AMIRI A, and MIRZAKUCHAKI S. A digital watermarking method based on NSCT transform and hybrid evolutionary algorithms with neural networks. *SN Applied Sciences*, 2020, 2: 1669. <https://doi.org/10.1007/s42452-020-03452-0>

[20] DONG H, HE M, and QIU M. Optimized Gray-Scale Image Watermarking Algorithm Based on DWT-DCT-SVD and Chaotic Firefly Algorithm. *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 310-313, 2015.

[21] JOSEPH A, and ANUSUDHA K. Robust watermarking based on DWT SVD. *International Journal of Signal & Image Processing*, 2013, 1(1) <https://doi.org/10.48550/arXiv.1309.2423>

[22] KANSAL M, SINGH G, and KRANTHI B V. DWT, DCT and SVD based Digital Image Watermarking. *Proceedings of the International Conference on Computing Sciences*, pp. 77-81, 2012

参考文献:

[1] HUSSEIN E. 和 BELAL M A. 应用于数字媒体的数字水印技术、应用和攻击：调查。国际工程研究与技术学报, 2012, 1(7): 12-23。

[2] ASANI E O, BIETY-NWANJU G, ADENIYI A E 等。使用拉丁方矩阵和物流图开发图像加密算法。国际高级计算机科学与应用杂志, 2023, 14(9): 869-877。 <http://dx.doi.org/10.14569/IJACSA.2023.0140991>

[3] ASANI E O, OMOTOSHO A, DANQUAH PA. 等。使用简洁特征的网络钓鱼检测的最大熵分类方案。电信公司电信计算电子与控制, 2021, 19(5): 1707-1714。 <http://doi.org/10.12928/TELKOMNIKA.v19i5.15981>

[4] RAWAT R, OKI O A, SANKARAN K S 等。使用机器学习方法的大数据网络安全新解决方案。在移动计算和可持续信息学方面。数据工程和通信技术讲义, 166, 施普林格, 新加坡, 2023: 495-505。

[5] ADESINA, AJAGBE SA, ODULE T J 和 AGBELE KK. 改进学校信息管理系统的开发。福沃科技趋势杂志, 2022, 7(1): 120-132。

[6] BEGUM M 和 UDDIN MS. 数字图像水印技术：综述。信息, 2020, 11(2): 110-119。

[7] TAHERA LA 和 HEMACHANDRAN K. 数字图像水印技术及其应用。国际工程研究与技术杂志, 2013, 2(3): 23-43。

[8] PAYAL K 和 NAVJOT K. 数字图像水印评论。国际工程研究与技术学报, 2015, 4(12): 14-29。

[9] HAI T 和 LI C. 鲁棒图像水印理论与技术：综述。应用研究与技术学报, 2014, 12(1): 18-29。

[10] KUMAR S, 和 SINGH B K. 基于熵的空间域图像水印及其性能分析。多媒体工具和应用, 2021, 80: 9315-9331. <https://doi.org/10.1007/s11042-020-09943-x>

[11] ABRAHAM J 和 PAUL V. 一种难以察觉的空间域彩色图像水印方案。沙特国王大学学报-计算机与信息科学, 2019, 31(1): 125-133. <https://doi.org/10.1016/j.jksuci.2016.12.004>

[12] YUAN Z, SU Q, LIU D, ZHANG X, 和 YAO T. 空间域快速鲁棒图像水印方法。IET 图像处理, 2020, 14(15): 3829-3838. <https://doi.org/10.1049/iet-ipr.2019.1740>

[13] POONAM 和 ARORA S M. 基于离散小波变换奇异值分解的数字图像鲁棒数字水印。计算机科学, 2018, 132: 1441-1448。 <https://doi.org/10.1016/j.procs.2018.05.076>。

[14] ABDULLATIF M, ZEKI A M, CHEBIL J 和 GUNAWAN T S. 数字图像水印的属性。2013 年 IEEE 第 9 届国际信号处理及其应用研讨会论文集, 马来西亚吉隆坡, 2013: 235-240, <https://doi.org/10.1109/CSPA.2013.6530048>。

[15] AHMADERAGHI B, KURUGOLLU F, DEL RINCON J M 和 BOURIDANE A. 使用统计决策理论的基于离散剪切波变换的盲图像水印检测算法。IEEE 计算成像学报, 2018, 4(1): 46-59。

[16] CHEN Z, CHEN Y, HU W, 和 QIAN D. 基于阈值分类的小波域数字水印算法。见：TAN Y, SHI Y, BUARQUE F 等。(编辑) 群体和计算智能的进展。胞浆内单精子显微注射 2015。计算机科学讲义, 9142: 129-136。施普林格、查姆。 https://doi.org/10.1007/978-3-319-20469-7_15。

[17] LIU S, PAN Z, 和 SONG H. 基于离散余弦变换和分形编码的数字图像水印方法。IET 图像处理, 2017, 11(10): 815-821。

[18] JOSEPH H 和 RAJAN B K. 使用离散余弦变换和载重吨水印技术增强图像安全性。国际通信与信号处理会议论文集, 印度钦奈, 2020, 第 0940-0945 页,

<https://doi.org/10.1109/ICCSP48568.2020.9182052>。

[19] AMIRI A, 和 MIRZAKUCHAKI S. 基于神经干细胞移植变换和神经网络混合进化算法的数字水印方法。序列号应用科学, 2020, 2 : 1669 。
<https://doi.org/10.1007/s42452-020-03452-0>

[20] DONG H, HE M, 和 QIU M. 基于离散小波变换奇异值分解和混沌萤火虫算法的优化灰度图像水印算法。网络分布式计算和知识发现国际会议论文集, 第 310-313 页, 2015.

[21] JOSEPH A 和 ANUSUDHA K. 基于离散小波奇异值分解的鲁棒水印。国际信号与图像处理杂志, 2013 , 1(1) <https://doi.org/10.48550/arXiv.1309.2423>

[22] KANSAL M, SINGH G 和 KRANTHI B V. 基于载重吨、离散余弦变换和奇异值分解的数字图像水印。国际计算科学会议论文集, 第 77-81 页, 2012