JCEC
THE JOURNAL OF ENGINEERING AND EXACT SCIENCES

OPEN ACCESS

The Journal of Engineering and Exact Sciences – jCEC, Vol. 09 N. 10 (2023)
journal homepage: https://periodicos.ufv.br/jcec
eISSN: 2527-1075
ISSN: 2446-9416

A secure and robust color image watermarking method using SVD and GAT in the multiresolution DCHWT domain

Article Info:
Article history: Received 2023-08-23 / Accepted 2023-11-05 / Available online 2023-11-09
doi: 10.18540/jcecvl9iss10pp17317-01e

Boubakeur Latreche
ORCID: https://orcid.org/0009-0007-9367-3368
Telecommunications and smart systems Laboratory, Faculty of Science and Technology, University of Djelfa, Djelfa 17000, Algeria.
E-mail: b.latreche@univ-djelfa.dz
Hilal Naimi
ORCID: https://orcid.org/0009-0004-7571-9420
Laboratory of Modeling Simulation and Optimization of Systems Complexes, Faculty of Science and Technology, University of Djelfa, Djelfa 17000, Algeria.
E-mail: h.naimi@univ-djelfa.dz
Slami Saadi
ORCID: https://orcid.org/0000-0001-8091-5232
Faculty of Exact Sciences and Informatics, University of Djelfa, Djelfa 17000, Algeria.
E-mail: saadisdz@gmail.com

Abstract
This paper introduces an innovative and robust watermarking technique for safeguarding the copyright of color digital images. The method operates within the domain of SVD-based multiresolution discrete cosine harmonic wavelet transforms. In this approach, the pre-processing phase employs successive generalized Arnold transforms to encrypt the RGB watermark layers, significantly enhancing the security of the watermarking algorithm. Subsequently, the blue layer of the host image undergoes R-level 2D-DCHWT processing. The encrypted watermark is embedded by altering the singular values of the host image's approximation coefficients. Additionally, a reliable extraction algorithm is devised to recover the watermark from potentially compromised watermarked images without requiring access to the original image. Through extensive experiments and comparisons with other relevant watermarking algorithms, the findings demonstrate that this scheme effectively embeds a color digital image watermark into the host image. This not only ensures high levels of invisibility but also establishes robustness, making it well-suited for the protection of digital image copyrights.
Keywords: RGB. Color image watermarking. DCHWT. SVD. GAT.

Nomenclature

2-D: Two Dimensional
AC: Alternating Current
DC: Direct Current
DCHWC: Discrete Cosine Harmonic Wavelet Coefficients
DCHWT: Discrete Cosine Harmonic Wavelet Transform
DCT: Discrete Cosine Transform
DFHWT: Discrete Fourier Harmonic Wavelet Transform
DFT: Discrete Fourier Transform
DWT: Discrete Wavelet Transform
FFT: Fast Fourier Transform

FT: Fourier Transform
GAT: Generalized Arnold Transform
HH: Hight-Hight
HL: Hight-Low
HVS: Hue, Saturation, Value
HWC: Harmonic Wavelet Coefficients
HWT: Harmonic Wavelet Transform
IDCT: Inverse Discrete Cosine Transform
IFFT: Inverse Fast Fourier Transform
IGAT: Inverse Generalized Arnold Transform
LH: Low-Hight
LL: Low-Low
LU: Lower–Upper
MRFO: Manta Ray Foraging Optimization
MSE: Minimum Squar Error
NC: Normalize Correlation
PSNR: Peak Signal-to-Noise Ratio
PSO: Practical Swarm Optimization
RGB: Red Green Blue
SB: Sub Band
SIDWT: Shift Invariant Discrete Wavelet Transform
SSIM: Structural Similarity Index Measure
SVD: Singular Value Decomposition
WT: Wavelet Transform

1. Introduction

Modern communications technology advancements have created new opportunities for human interaction and provided people with the ease of multimedia technologies (Vaidya *et al*., 2023). The use of images has become widespread, impacting our daily lives, professions, and social media interactions (Kour *et al*., 2016). In our daily lives, images enhance digital communication and storytelling, while social media platforms have made image sharing a central feature for communication and personal expression. Professionally, images play vital roles in healthcare, journalism, marketing, engineering, and creative fields, serving various purposes from driving engagement to aiding diagnosis and innovation (Alqahtani *et al*., 2023).

Overall, the ability of contemporary communication technologies to host and share images has revolutionized the way we communicate, innovate, and engage in the digital era. However, progress frequently has a dual aspect. While individuals reap the benefits of technological advancements, a continuous influx of various forms of infringement and piracy techniques proliferates endlessly (Ray & Roy, 2020).

Certain images might include personal or private information, which may include confidential business information and sensitive government data. When unauthorized individuals gain illicit access to, steal, or tamper with such data, it can lead to major repercussions, result in substantial economic losses, and potentially pose a threat to national security (An & Liu, 2019). Addressing the prevention of such security incidents and ensuring security in the transmission of digital images represents an important research focus (Al-Ghaili *et al*., 2023).

Currently, encryption and watermarking represent the most commonly employed techniques for safeguarding digital image data (Eltoukhy *et al*., 2023; Lin & Xu, 2021). Image encryption refers to a security method that utilizes cryptographic algorithms to transform the content of a digital image into an encrypted or scrambled state, rendering it unreadable without the corresponding decryption key (Sanjay Patsariya & Manish Dixit, 2022). Its primary purpose is to safeguard sensitive or confidential visual information, restricting access to only those with the necessary authorization to decode and view the original image (Elkandoz *et al*., 2022). Certain prevalent limitations and

weaknesses related to encryption suggest that encrypted images can indeed be susceptible to a range of attacks, resulting in the partial loss of image components and hindering the accurate recovery of the original image (Abduljabbar *et al*., 2022).

Image watermarking is a method employed to insert hidden information (text, signature, etc.) or markers (images, logos, etc.) into digital images. (Keivani *et al*., 2020). These watermarks are typically imperceptible to the human eye. Watermarking serves various purposes, including safeguarding copyrights, authentication, and tamper detection. allowing for the monitoring and validation of its origin and integrity (Wang *et al*., 2023). The main concept of the digital watermarking technique was initially introduced to safeguard copyrighted multimedia data (Mohanty, 1999). It addresses the limitations of classical cryptography by leveraging the human visual system's redundancy to embed copyright data (Zhang *et al*., 2023), thereby increasing its resilience against a variety of potential attacks. Typically, watermarking exhibits distinct characteristics, including security, imperceptibility, robustness, and low complexity (Soualmi *et al*., 2023).

Image watermarking techniques for embedding and extracting watermarks in digital images are categorized, taking various factors into account, such as watermark visibility (visible or invisible) (Qi *et al*., 2019; Supiyandi *et al*., 2018), embedding domain (spatial or frequency) (Su *et al*., 2022; Taha *et al*., 2020), and security requirements (fragile or robust) (Abadi & Moallem, 2022; Lin *et al*., 2021). Watermarking systems need to adhere to particular standards in order to ensure and demonstrate the suitability of a robust watermarking approach, such as imperceptibility robustness and security.

Nowadays, the majority of watermarking methods are designed for static grayscale images, despite the extensive use of color images in our daily lives, professions, and social media interactions. For this reason and to improve the above requirements, researchers are focusing their attention on color image watermarking and have suggested numerous watermarking techniques (Ahmadi *et al*., 2021; Ernawan, 2019; Hosny *et al*., 2021; Rahardi *et al*., 2022).

In their publication, (Wang *et al*., 2016) presented a method of blind watermarking color digital images. This technique incorporates Discrete Wavelet Transform (DWT) and LU decomposition. The host image undergoes a DWT decomposition, and the process of embedding an encrypted watermark image takes place within the LH and HL sub-bands during the LU decomposition. In the paper of (Moosazadeh, 2017) a digital color image watermarking approach was presented. This approach operates in the YCoCg-R color space and utilizes the relationships between DCT coefficients. During the embedding process, the selection of target blocks is determined based on the complexity of the cover image blocks, and the adaptive choice of embedding strengths is guided by the energy values of these cover image blocks.

A method for robust and securely embedding watermarks into color images within the spatial domain was introduced in a study by (Su & Chen, 2018), In this technique, the choice is made to embed the watermark in the blue channel, and this embedding is performed in various regions by altering pixel values based on the distribution of the direct current (DC) coefficient and generation principle. In a different study by (Pandey *et al*., 2019) , An image watermarking algorithm that is not blind was proposed. This algorithm utilized the Arnold transform within the YCbCr color model, specifically applying it to the Y channel of the host image. The watermark's singular values were inserted using a variable scaling factor, and, to enhance security, the number of Arnold transform iterations was employed as a private key to scramble the watermark image before embedding.

A Schur decomposition and Affine transformation-based blind watermarking method for color digital images is presented in a reference by (Liu *et al*., 2020). In this technique, watermark bits are scrambled through the Affine transmission and then inserting them by assessing the diagonal eigenvalues derived from the upper triangular matrix produced by Schur decomposition. In a separate study by (Ahmadi *et al*., 2021), introduced a blind dual-color digital image watermarking approach. In this method, the watermark is inserted Within the color space's blue channel, leveraging the HVS and Singular Value Decomposition (SVD) within the DWT domain. This embedding process is optimized using Particle Swarm Optimization (PSO) to achieve a balance between

imperceptibility and robustness. Additionally, the capacity is increased twofold by embedding two watermark bits into each selected block in the SVD domain. Furthermore, a fragile watermark is inserted into all RGB channels of the color space using a novel technique that manipulates the diagonal singular values.

In a recent publication by (Abadi & Moallem, 2022). they introduce a novel hybrid technique for robust color image watermarking. This method involves the careful selection of the most suitable color component from the host image and the identification of the most effective wavelet sub-band. After transforming the chosen color component of the host image into the wavelet domain, the process incorporates preliminary steps with the Discrete Cosine Transform (DCT). Subsequently, the watermark is inserted into the optimal range using a confidential key. In another study (Dwivedi *et al*., 2023). they present an optimized image watermarking approach that leverages MRFO (a specific optimization method), RDWT (Redundant Discrete Wavelet Transform), RSVD (Randomized Singular Value Decomposition), and Henon mapping encryption within the YCbCr color space. MRFO is applied to determine the optimized factor that balances imperceptibility, robustness, and capacity. The watermark is embedded within the luminance component of the host image, as it contains critical information.

In this research paper, a new and robust watermarking technique is introduced for protecting the copyright of color digital images in the context of SVD-based multiresolution discrete cosine harmonic wavelet transforms. This method incorporates several key steps to enhance the security and reliability of the watermarking process. To begin, Arnold transforms are sequentially applied in the preprocessing stage to encrypt the RGB watermark layers, significantly bolstering the security of the watermarking algorithm. Subsequently, a two-dimensional discrete cosine harmonic wavelet transform (2D-DCHWT) is performed at the R-level on the blue layer image. The encrypted watermark is then embedded by modifying the singular values of the approximation coefficients of the host image. Additionally, a robust extraction algorithm is devised to recover the watermark from watermarked images that may have been subjected to attacks, all without the need for the original image. After conducting extensive experiments and comparing the proposed algorithm with other relevant watermarking methods, it is evident that our approach successfully embeds a watermark into color digital images. This process not only ensures a high level of invisibility but also offers robustness, making it well-suited for the protection of digital image copyrights.

The rest of this paper is organized as follows: In Section 2, we present an introduction to the fundamental theories used in this study, including concepts like the generalized Arnold transform, HWT, DCHWT and SVD. In Section 3, the paper introduces the watermarking algorithm. Section 4 then presents the experimental results and findings that demonstrate the effectiveness of our approach. Finally, in Section 5, we provide the conclusions derived from our research.

2. Methodology

2.1 Generalized Arnold transform

The Arnold map, often referred to as the Arnold transform or Arnold cat map, is a mathematical transformation used for image scrambling (Pandey *et al*., 2019). It was proposed by V.I. Arnold in his research on ergodic theory in the 1960s (Arnold & Avez, 1968). It's a reversible and chaotic transformation that shuffles the pixels of an image in a way that appears random, but it can be completely reversed when needed (Sanjay Patsariya & Manish Dixit, 2022). Here's how the classical Arnold map is typically applied for image scrambling:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(1) \quad (1)$$

where (x_i, y_i) is the location of the pixel before the transformation and (x_{i+1}, y_{i+1}) is the location of the transformed pixel. In this context, when we mention $(x \; mod \; 1)$, it signifies the fractional component of a real number x. The Lyapunov exponent of the Arnold map exceeds 1, indicating that the map exhibits chaotic behavior. However, despite its chaotic nature, the original

(classical) Arnold map given by Equation 1 isn't directly employed for digital image encryption (Zhu *et al*., 2014). This is due to the fact that the security of the Arnold map primarily hinges on its initial value. To address this weakness, an alternative map, known as the generalized Arnold map, is introduced in the following manner:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \quad (2)$$

Here, a and b are real, non-negative numbers referred to as control parameters. N represents the dimensions, either the height or width, of the square image being processed. In summary, when a and b are both greater than 1, it can be inferred that the largest Lyapunov exponent of map in Equation 2 surpasses that of map in Equation 1. This suggests that GAT exhibits a higher degree of chaos and, consequently, is expected to excel in the task of data shuffling (Zhu *et al*., 2014). The aim of the Generalized Arnold Transform (GAT) is to mess up the original image's pixel positions.

The formula for the inverse transformation of the Generalized Arnold Transform (GAT) can be expressed in Equation 3 as follows:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \quad (3)$$

To create an encrypted image from a given image, since the transformation is an iterative process, Equation 2 is applied t times. However, to reduce the computational complexity during the decryption process, we employ Equation 3 for iterations on the encrypted image instead of conducting $T - t$ iterations using Equation 2, where T represents the transform's period. a, b and t parameters can be used as secret keys.

2.2 Harmonic wavelet transform

The Wavelet Transform (WT) is a versatile tool used in various applications due to its energy compaction and multiresolution properties. It efficiently represents data by compacting energy into a few key coefficients (Newland, 1998), making it ideal for tasks like data compression and watermarking. The WT can analyze signals at multiple resolutions. It offers precise time localization but limited frequency accuracy for high-frequency components and provides accurate frequency detail but less precise time localization for low-frequency components, making it suitable for nonstationary signal analysis (Liu & Chen, 2019).

The wavelet transform in the Fourier domain, denoted as $\mathbb{W}_{x,F}(a,b)$, calculates the relationship or correlation between the signal $x(t)$ that is under analysis and a wavelet function $\psi(t)$ and is given by:

$$\mathbb{W}_{x,F}(a,b) = \frac{1}{a^{1/2}} \int_{-\infty}^{+\infty} x(t)\psi^*(\frac{t-b}{a})dt \quad (4)$$

Here, the symbol * represents the operation of complex conjugation, $\psi(t)$ is the mother wavelet and a and b are scaling and shifting parameters, respectively. All basis functions are derived through the application of Equation 5:

$$\psi_{a,b}(t) = \frac{1}{a^{1/2}}\psi(\frac{t-b}{a}) \quad (5)$$

In the frequency domain, the wavelet transform $\mathbb{W}_{x,F}(a,b)$ can be implemented by applying Parseval's theorem as follows (Narasimhan *et al*., 2009):

$$\mathbb{W}_{x,F}(a,b) = \frac{a^{1/2}}{2\pi} \int_{-\infty}^{+\infty} X(\omega)\Psi^*(a\omega)e^{j\omega b}d\omega \quad (6)$$

Hence, the wavelet transform at a specific scale a can be obtained by taking a windowed version of the spectrum $X(\omega)$ using $\Psi^*(a\omega)$ and then performing an inverse Fourier transform on the resulting product.

$$\mathbb{W}_{x,F}(a,b) = |a|^{1/2}\mathcal{F}^{-1}[X(\omega)\Psi^*(a\omega)] \quad (7)$$

Here, $X(\omega)$ and $\Psi(a\omega)$ represent the Fourier transforms of the signal and the mother wavelet, respectively. Particularly, $\Psi(\omega)$ is uncomplicated when using the Harmonic Wavelet Transform (HWT) as proposed by authors in. It is zero across all frequencies except for being constant within a small frequency range (Newland, 1993).

$$\Psi(\omega) = \begin{cases} 1, \text{for } \omega_0 - \omega_c < \omega < \omega_0 + \omega_c, \\ 0, \text{otherwise.} \end{cases} \quad (8)$$

The mother wavelet $\psi(t)$ in the time domain that corresponds to this is as follows:

$$\psi(t) = \frac{\omega_c}{\pi}\frac{\sin(\omega_c t)}{(\omega_c t)} e^{j\omega_0 t} \quad (9)$$

$$\psi(t) = \frac{\omega_c}{\pi}\,\mathrm{sinc}\,(\omega_c t) e^{j\omega_0 t} \quad (10)$$

Therefore, the mother wavelet, represented by a (sinc function), can be described as a modulated version of a scaling function of Shannon. The daughter wavelets are obtained from $\psi(t)$ through the application of scaling (ω_c) and shifting (ω_0) parameters, which determine the octave bands' width and central frequency. Similar to other wavelets, harmonic wavelets have the capability to constitute an orthonormal basis for multiresolution analysis, as explained by (Shreyamsha Kumar, 2013). These waveforms have strong localization properties and exhibit narrow support intervals in the frequency domain, yet they exhibit a gradual decrease in amplitude over time. If the goal is to improve time localization, a different spectral weighing function, such as a Gaussian, may be necessary, but this could lead to non-orthogonal wavelets due to potential frequency domain overlap. Ultimately, the properties of the wavelet are determined by the selection of the spectral weighing function, as this function represents the Fourier transform of the wavelet (Narasimhan *et al*., 2009).

In the harmonic wavelet transform (HWT), signal decomposition takes place in the frequency domain by organizing Fourier transform (FT) coefficients based on their conjugate symmetry property. The inverse Fourier transform of these grouped coefficients yields decimated signals referred to as harmonic wavelet coefficients (HWCs). The HWT offers inherent capabilities for both decimation and interpolation operations, eliminating the need for band-limiting or image-rejection filters (Dhyani *et al*., 2016), and it can be efficiently implemented using the FFT and IFFT. This reduces computational complexity compared to convolution. These advantages make HWT attractive for image watermarking. However, during HWC computation, Fourier coefficients exhibit leakage due to the abrupt discontinuity of finite data length and the rectangular window used in DFT computation (McFee, 2023). This leakage scatters energy to other scales in HWT, indirectly affecting neighboring scales during processing (Tan & Jiang, 2018). To fully leverage HWT's benefits, reducing this leakage is essential. The solution is to use a discrete cosine transform (DCT) instead of a DFT for HWT computation in image watermarking, aiming to minimize the leakage effect.

2.3 Discrete Cosine Harmonic wavelet transform

To fully leverage the advantages of the HWT, reducing leakage effects is crucial. Using the Discrete Cosine Transform (DCT) instead of the Discrete Fourier Transform (DFT) is a significant step. The DCT extends data symmetrically, leading to a smoother transition between DCT periods and reducing the root cause of leakage – discontinuity (Roopa & Narasimhan, 2014). This reduction in leakage results in a decrease in spectral magnitude bias, making low-level spectral peaks near high-level ones more detectable. Compared to the DFT, the DCT offers superior frequency resolution due to data extension (Latreche *et al*., 2019), allowing it to resolve closely spaced spectral peaks effectively. This results in reduced bias in both spectral magnitude and frequency, enhancing detectability. However, the trade-off is that higher frequency resolution may come with increased variance as more spectral details are captured.

For real symmetric signals, $x_s(t)$ is the signal that is under analysis and $\psi_s(t)$ is the wavelet function. The wavelet transform $\mathbb{W}_{x,C}(a,b)$ in the cosine domain (instead of the Fourier domain) can be written as:

$$\mathbb{W}_{x,C}(a,b) = \frac{a^{1/2}}{2\pi} \int_{-\infty}^{+\infty} X_s(\omega)\Psi_s(a\omega)\cos(\omega b)d\omega \quad (11)$$

Here, $X_s(\omega)$ and $\Psi_s(a\omega)$ represent the cosine transforms of the signal $x_s(t)$ and the wavelet function $\psi_s(t)$, respectively. Expressing the wavelet transform by the inverse cosine transform can be done as follows:

$$\mathbb{W}_{x,C}(a,b) = |a|^{1/2}\mathrm{C}^{-1}[X_s(\omega)\Psi_s(a\omega)] \quad (12)$$

the cosine harmonic wavelet function $\Psi_s(\omega)$ is uncomplicated and remains at zero across the entire frequency spectrum, except for a small frequency band where it maintains a constant value.

$$\Psi_s(\omega) = \begin{cases} 1, \omega_0 - \omega_c < \omega < \omega_0 + \omega_c, -\omega_0 - \omega_c < \omega < -\omega_0 + \omega_c, \\ 0, \text{otherwise.} \end{cases} \quad (13)$$

In the time domain, the corresponding wavelet $\psi_s(t)$ emerges as:

$$\psi_s(t) = \frac{\omega_c}{\pi}\frac{\sin(\omega_c t)}{(\omega_c t)}\cos(\omega_0 t) \quad (14)$$

$$\psi_s(t) = \frac{\omega_c}{\pi}\cos(\omega_0 t)\ \mathrm{sinc}(\omega_c t) \quad (15)$$

Therefore, the mother wavelet is a $sinc$ function modulated by cosine. In this case, breaking down the signal in the frequency domain is straightforward, but it faces challenges with time precision because the $sinc$ function decays slowly. While using spectral weighting other than a rectangular shape enhances time localization, it sacrifices the orthogonality of the wavelet set. The specific choice of spectral weighting dictates the nature of the wavelet since it essentially represents the cosine transform of the wavelet itself (Narasimhan *et al*., 2009). The discrete cosine transform (DCT) (Latreche, 2023) allows for the practical implementation of the previously mentioned cosine transformation, as it generates symmetric signals $x_s(t)$ and the wavelet function $\psi_s(t)$ by itself.

In the Discrete Cosine Harmonic Wavelet Transform (DCHWT), signal decomposition involves organizing DCT coefficients in a manner akin to DFT coefficients, with the exception of needing conjugate operations since DCT coefficients are real. The symmetric placement of coefficients isn't necessary due to the inherent properties of DCT (Kiranmayi & Udayashankara, 2020). Performing the inverse DCT (IDCT) on these groups yields discrete cosine harmonic wavelet coefficients (DCHWCs).

Further processing involves taking the DCT of these sub bands (comprising DCHWCs), followed by repositioning the resulting sub band DCT coefficients to reconstruct the original DCT spectrum at the initial sampling rate. Similar to the Fourier-based Harmonic Wavelet Transform (HWT), the DCHWT offers advantages, including built-in decimation and interpolation, eliminating the need for band-limiting or image-rejection filters, and facilitating fast algorithms based on the DCT.

Additionally (Dhyani *et al*., 2016), the DCHWT is computationally simpler than the Fourier-based HWT (DFHWT) as it only requires real operations, making it even more computationally efficient than convolution (Shreyamsha Kumar, 2013).

In the case of a 2D signal, the DCHWT doesn't encounter this issue (Figure 1(a)). This is because the DCT is a real-valued transformation, and the generation of real signals doesn't necessitate the use of complex conjugate symmetry. In the context of image processing, the DCT coefficients of the columns are organized and, when subjected to the inverse DCT, produce DCHWT coefficients for those columns. Similarly, DCT coefficients along the rows at each scale are grouped, and the inverse DCT of these groups results in a 2D DCHWT (as shown in Figure 1(b). This process can be repeated for additional scales, starting with the LL (low-low) block as the input. Since there

are no approximations made, there are no errors introduced when reconstructing the image using all of the coefficients.

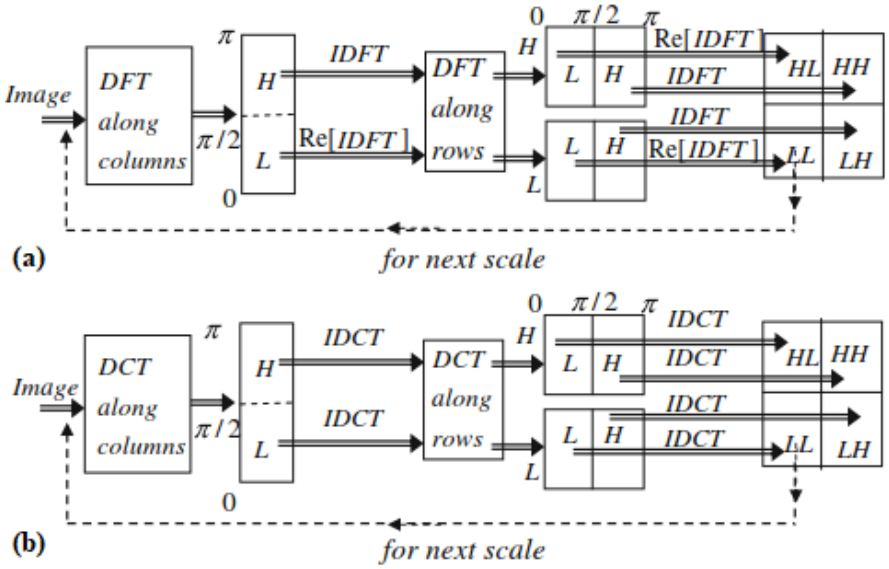


Figure 1 – (a) 2D-DFHWT; (b) 2D-DCHWT.

2.4 Singular Value Decomposition

Singular Value Decomposition (SVD) is a fundamental concept in linear algebra and matrix factorization. It's used for various applications in mathematics, statistics and image processing (Su *et al*., 2022). SVD decomposes a matrix (image) into three other matrices, allowing us to analyze its properties and extract important information. The SVD of an image matrix A with $N \times N$ of size can be described as (Dwivedi *et al*., 2023):

$$A = USV^T = \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,N} \\ u_{2,1} & u_{2,2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ u_{N,1} & u_{N,2} & \cdots & u_{N,N} \end{bmatrix} \times \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_N \end{bmatrix} \times \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,N} \\ v_{2,1} & v_{2,2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ v_{N,1} & v_{N,2} & \cdots & v_{N,N} \end{bmatrix} \quad (16)$$

$$A = \sum_{i=1}^{r} \lambda_i u_i v_i^T \quad (17)$$

U and V represent $N \times N$ orthogonal matrices, S is an $N \times N$ diagonal matrix, and T indicates matrix transposition. The column vectors of U and V are denoted as u_i and v_i, respectively. The diagonal elements of S, labeled as λ_i, are referred to as the singular values of A and adhere to $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = \cdots = \lambda_N = 0$.

SVD is a key component in image transformation, particularly in the field of digital watermarking technology (Wang *et al*., 2022; Yasmeen & Uddin, 2021). The singular values of an image describe its data distribution characteristics and exhibit remarkable stability; even minor changes in singular values do not impact the image's visual quality (Eltoukhy *et al*., 2023). Furthermore, SVD imposes no constraints on the size of the image matrix.

3. Proposed Algorithm

In this section, we present an innovative and secure technique for watermarking color images, which has been specifically designed based on DCHWT, SVD, and GAT. Within the framework of the proposed algorithm, the pivotal phases are watermark embedding and watermark extraction. The embedding process hides the watermark within the color host image, while the extraction process extracts the hidden watermark information. Importantly, this extraction is achieved without necessitating access to the original information.

3.1 Watermark embedding procedure

Consider the original Red (R) Green (G) Blue (B) color host image denoted as (H) with a size of $M \times M$ and the RGB color watermark image as (W) with a size of $N \times N$. The process of embedding the digital watermark can be outlined in the following steps:

Step 1: To begin, we partition an $M \times M$ host image into separate R, G, and B layers, denoted as H_R, $H_G$and H_B, respectively. Similarly, we segment an $N \times N$ watermark, resulting in three distinct layers: W_R, W_G and W_B. Subsequently, in order to enhance the security of the proposed algorithm, we apply a generalized Arnold transform (GAT) successively to the three watermark layers, utilizing three distinct keys (K_R, $K_G$and K_B). This process generates three distinct chaotic watermark layers, denoted as W_R^C, $W_G^C$and W_B^C.

Step 2: Concerning the blue layer of the host image H_B with dimensions $M \times M$, the decomposition is performed up to R-levels using 2D-DCHWT, and it can be described as follows:

- Calculate the 2D Discrete Cosine Transform (DCT) of the provided layer H_B,
- Calculate R, when $R = \log_2 \frac{M}{N}$,
- Group the generated 2D-DCT coefficients, considering an example with $R = 3$, G_1, G_2, G_3 and G_4 are of size $\frac{M}{2^3}$ (64×64), G_5, G_6 and G_7 are of size $\frac{M}{2^2}$ (128×128), G_8, G_9 and G_{10} are of size $\frac{M}{2^1}$ (256×256).
- Apply the 2D Inverse Discrete Cosine Transform (IDCT) of the G_i groups $(i = 1{:}\,10)$. G_1, G_2, G_3 and G_4 gives the approximation A_3, horizontal H_3, vertical V_3 and diagonal D_3 coefficients at the third level, respectively. G_5, G_6 and G_7 gives the horizontal H_2, vertical V_2 and diagonal D_2 coefficients at the second level, respectively. G_8, G_9 and G_{10} gives the horizontal H_1, vertical V_1 and diagonal D_1 coefficients at the first level, respectively.

Step 3: The SVD is performed on the approximation A_3 coefficients at the third level to give us three matrices: U_{A_3}, S_{A_3} and $V_{A_3}^T$. Similarly, the SVD is performed for the encrypted blue layer of the watermark W_B^C to result in $U_{W_B^C}$, $S_{W_B^C}$ and $V_{W_B^C}^T$.

Step 4: To calculate the embedded singular value, denoted as S_W, we perform an addition of the S_{A_3} and $S_{W_B^C}$ matrices while using an optimal scaling factor α $(S_W = S_{A_3} + \alpha * S_{W_B^C})$.

Step 5: The inverse SVD is performed on (U_{A_3}, S_W and $V_{A_3}^T$) to produce the new embedded approximation coefficients denoted as A_3^W.

Step 6: We produce the watermarked blue layer, denoted as H_B^W, by performing the reverse R-level 2D-DCHWT on A_3^W, H_{i}, V_{i} and D_{i} for $(i = 1{:}\,3)$.

Step 7: finally, it gets the final watermarked image H^W by merging three layers: $R(H_R)$, $G(H_G)$ and $B(H_B^W)$, preserving the embedded watermark information and ensuring the integrity of the image data.

3.2 Watermark extracting procedure

Watermark extraction is the process of retrieving the embedded digital watermark from an image, often for the purpose of verification, authentication, or copyright protection. The procedure for extracting the digital watermark can be summarized with the following steps:

Step 1: We divide the $M \times M$ watermarked image H^W into separate R, G, and B layers, denoted as H_R^W, H_G^W and H_B^W, respectively.

Step 2: Regarding the blue layer of the watermarked image H_B^W with dimensions $M \times M$, the decomposition is carried out up to R-levels using 2D-DCHWT, resulting in A_3^W, H_i^W, V_i^W and D_i^W for $(i = 1{:}\,3)$, taking into account an example where $R = 3$.

Step 3: The SVD is performed on the approximation A_3^W coefficients at the third level to give us three matrices: $U_{A_3}^W$, $S_{A_3}^W$ and $(U_{A_3}^W)^T$.

Step 4: To determine the extracted singular matrix of the encrypted blue layer of the watermark, denoted as $S^{E}_{W^{C}_{B}}$, we perform a subtraction of the $S^{W}_{A_3}$ from S_E matrices and then divide the result by the optimal scaling factor α $(S^{E}_{W^{C}_{B}} = (S_E - S^{W}_{A_3})/\alpha)$.

Step 5: The inverse SVD is performed on ($U_{W^{C}_{B}}$, $S^{E}_{W^{C}_{B}}$ and $V^{T}_{W^{C}_{B}}$) to produce the extracted encrypted blue layer of the watermark ($W^{E,C}_{B}$).

Step 6: We apply the inverse generalized Arnold transform (IGAT) successively to the three encrypted watermark layers W^{C}_{R}, $W^{C}_{G}$and $W^{E,C}_{B}$, using three distinct keys (K_R, K_G and K_B). This operation produces three distinct extracted watermark layers W^{E}_{R}, W^{E}_{G} and W^{E}_{B}.

Step 7: Finally, it gets the final extracted watermark image W^{E} by merging three layers: $R(W^{E}_{R})$, $G(W^{E}_{G})$ and $B(W^{E}_{B})$.

3.3 Adaptive scaling factor

The scaling factor, denoted as α, is used to adjust the magnitude of the inserted/extracted singular value to achieve the desired watermark strength. The choice of α depends on various factors, including the robustness of the algorithm and the imperceptibility of the watermark in the host image. We want to ensure that the watermark remains imperceptible to the human eye while our method exhibits robustness against potential attacks (Ernawan *et al*., 2023). Increasing α can enhance the visibility of the watermark, but it might also increase the method's susceptibility to attacks. Conversely, decreasing α can reduce the watermark's visibility, potentially making the method more resilient against different types of attacks (Ariatmanto *et al*., 2022). The key is to select α in a way that strikes a balance between robustness and imperceptibility. To assess the imperceptibility of the watermarked image, we employ two metrics: the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM). The PSNR metric gauges the disparity in signal noise between the original host image and the watermarked one. A higher PSNR value indicates more effective watermarking.

$$PSNR(H, H^{W}) = 20\ \log_{10}\left(\frac{Max_I}{MSE(H, H^{W})}\right) \tag{18}$$

Where Max_I refers to the highest attainable pixel value within the image. In the case where each pixel is encoded with 8 bits per sample, this value is equal to 255. MSE can be calculated using Equation 19.

$$MSE(H, H^{W}) = \frac{1}{m^2}\sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{3}(H(i,j,k) - H^{W}(i,j,k))^2 \tag{19}$$

On the other hand, the SSIM metric evaluates the structural resemblance between the two images. SSIM can be computed using Equation 20.

$$SSIM(H, H^{W}) = \frac{2\mu_H\mu_{H^W} + v_1}{\mu_H^2 + \mu_{H^W}^2 + v_1} \times \frac{2\sigma_{HH^W} + v_2}{\sigma_H^2 + \sigma_{H^W}^2 + v_2} \tag{20}$$

With $\mu_H, \mu_{H^W}\sigma_H^2$ and $\sigma_{H^W}^2$, represent means and variances values for both the host image (H) and the watermarked image (H^{W}), respectively. while σ_{HH^W} represents the covariance value between host and watermarked images. v_1, v_2 are constant values less than one ($v_1, v_2 \ll 1$). SSIM ranges from 0 to 1. When the SSIM value equals 1, it signifies that the watermarked image exhibits a flawless similarity to the host image (Wang *et al*., 2004). To evaluate the robustness of our proposed method against different attacks, we employ the normalized correlation (NC) between the watermark W and the extracted watermark W^{E}. The NC metric quantifies the level of correlation between these two elements and can be computed as in Equation 21.

$$NC(W, W^{E}) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{3} W(i,j,k) \times W^{E}(i,j,k)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{3}[W(i,j,k)]^2}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{3}[W^{E}(i,j,k)]^2}} \tag{21}$$

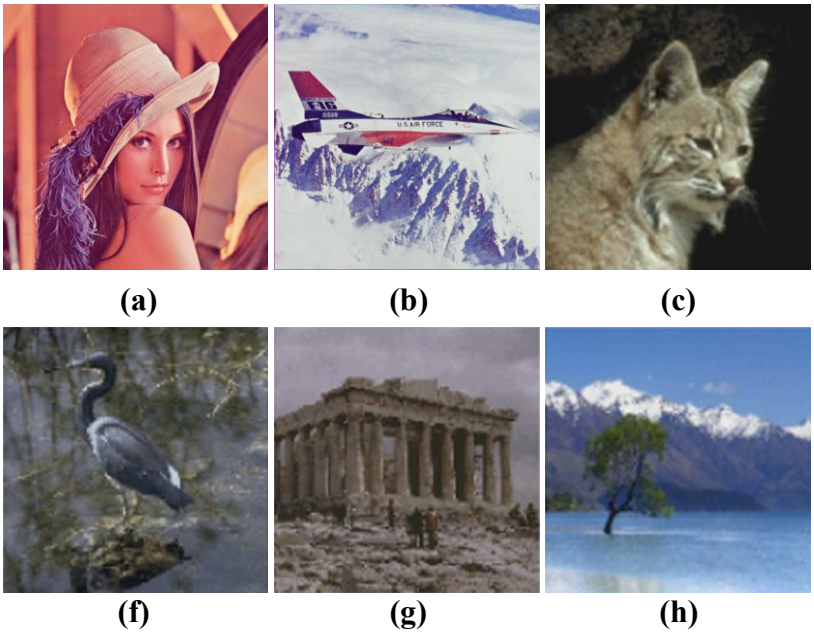
A high NC value, close to 1, is desirable because it indicates a strong correlation between the original and extracted watermarks. This suggests that the watermark extraction process is highly accurate and robust against various attacks. In this work, we use an optimum scaling factor α that maximizes an objective function, achieving the right trade-off between robustness and imperceptibility. The objective function (F) is a weighted combination of the imperceptibility $(PSNR/SSIM)$ and robustness (NC) components, with the scaling factor α:

$$F = \underset{\alpha}{\text{Max}} \sum_{i=1}^{k} \left(PSNR(H, H_i^W)\right) + \left(SSIM(H, H_i^W)\right) + 2 \times \left(NC(W, W_i^E)\right) \quad (22)$$

In this situation, we represent the watermarked image and the extracted watermark image obtained from the ith attack as H_i^{W} and W_i^{E}, respectively.

4. Results and Discussions

To evaluate the proposed algorithm, a series of extensive experiments is conducted in this section. Thorough analyses are performed, and comparisons with other state-of-the-art algorithms (results from (Wang *et al*., 2023)) are executed. The experimental computer configuration included a system with an NVIDIA GeForce GT 555M CUDA 2GB graphics card from ASUSTek Computer Inc., and an Intel® Core™ i5-2430M CPU running at 2.40 GHz, also from ASUSTek Computer Inc. The system was equipped with 8.0 gigabytes of DDR3 RAM memory. The software used for the experiment was Matlab 2018b, running on a 64-bit Windows 10 machine. The proposed approach undergoes comprehensive testing and analysis, utilizing six color images with dimensions of 512×512 as host images, as illustrated in Figure 2. Additionally, three color images with a size of 128×128 were used as watermarks, displayed in Figure 3. These images were chosen from the databases (Dataset, 2002; Dataset, 1997).



(a) (b) (c)

(f) (g) (h)

Figure 2 – Host images: (a) Lena, (b) Avion, (c) Bobcat, (d) Bluheron, (e) Athens, and (f) Sea.

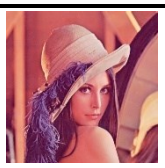
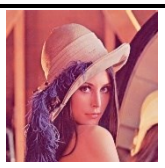
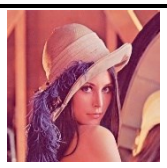
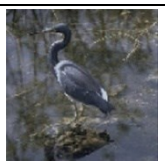
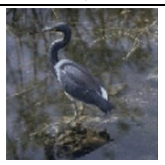
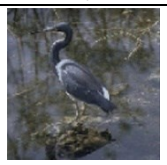
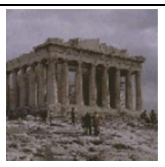
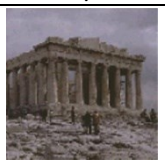
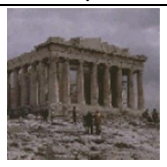
(a) (b) (c)

Figure 3 – Watermark images: (a) Peugeot, (b) Number, and (c) Leopard.

4.1 Imperceptibility performance analysis

In this section, we conduct extensive simulation experiments to evaluate the watermark's imperceptibility. These experiments involve individual evaluation of our proposed algorithm and comparative evaluations with other advanced algorithms (Chen *et al*., 2021; Goléa *et al*., 2010; Wang *et al*., 2023; Yuan *et al*., 2020a; Yuan *et al*., 2020b). We utilize the host image and watermark depicted in Figures 2 and 3 to validate the watermark's invisibility. To illustrate the imperceptibility of the watermark, we initially embedded three watermarks into six host images. The experimental results and corresponding visual representations are presented in Table 1.

Table 1 – Imperceptibility performance using different parameters.

Hosts \ Watermarks	Peugeot	Number	Leopard
Lena			
PSNR/SSIM	44.3830/0.9992	42.4034/0.9988	45.2965/0.9993
Avion			
PSNR/SSIM	44.2744/0.9880	42.3712/0.9823	45.2865/0.9900
Bobcat			
PSNR/SSIM	44.4350/0.9939	42.4347/0.9900	45.3176/0.9954
Bluheron			
PSNR/SSIM	44.4458/0.9910	42.4108/0.9856	45.3148/0.9929
Athens			
PSNR/SSIM	44.3789/0.9912	42.3986/0.9866	45.3571/0.9928
Sea			
PSNR/SSIM	44.4005/0.9981	42.3763/0.9972	45.3649/0.9982

Upon analyzing the data in Table 1, it's evident that our proposed algorithm yields PSNR values higher than 42 dB (for the Peugeot watermark) and higher than 44 dB (for the Number and Leopard watermarks), and SSIM values exceeding 0.99 in the majority of cases (14/18 = 78%) and higher than 0.98 in the rest (04/18 = 22%). This range of PSNR (between 37 dB and 48 dB) indicates strong watermark imperceptibility and high-quality watermarked images. When observing the visual representations in Table 1, it becomes clear that the watermark is virtually indiscernible to

the human eye after embedding. In essence, the proposed watermark algorithm demonstrates exceptional invisibility.

Furthermore, to establish the superior imperceptibility of our proposed algorithm, we embedded the watermark Peugeot in Lena and Avion host images, the watermark Number in Bobcat and Bluheron host images and the Leopard watermark in Athens and Sea host images using various algorithms (exactly as done in (Wang *et al*., 2023)).

In Tables 2 and 3, both the PSNR and SSIM values achieved by our proposed algorithm surpass those of other pertinent algorithms. The proposed algorithm demonstrates high consistency in watermark extraction across all host images, with an NC score of 1.0000 for each image as shown in Table 4. This suggests strong performance in terms of watermark imperceptibility.

Table 2 – The PSNR measurements from different algorithms.

Host image	PSNR					
	(Yuan *et al*., 2020b)	(Goléa *et al*., 2010)	(Chen *et al*., 2022)	(Yuan *et al*., 2020a)	(Wang *et al*., 2023)	Proposed
Lena	36.3689	39.4358	40.8077	37.5851	41.2072	**44.3830**
Avion	36.3257	38.3922	39.7498	37.1426	40.0748	**44.2744**
Bobcat	36.8073	35.3946	41.0736	37.5833	40.6817	**42.4347**
Bluheron	36.4803	38.6405	**42.3514**	37.9887	41.5963	**42.4108**
Athens	36.4098	40.5937	41.3934	37.6780	40.9303	**45.3571**
Sea	35.8883	36.4876	41.5901	37.6285	41.2384	**45.3649**
Average	36.3501	38.1574	41.1610	37.6010	40.9579	**44.0375**

Table 3 – The SSIM measurements from different algorithms.

Host image	SSIM					
	(Yuan *et al*., 2020b)	(Goléa *et al*., 2010)	(Chen *et al*., 2022)	(Yuan *et al*., 2020a)	(Wang *et al*., 2023)	Proposed
Lena	0.9616	0.9414	0.9803	0.9350	0.9712	**0.9992**
Avion	0.9562	0.9458	0.9807	0.9245	0.9684	**0.9880**
Bobcat	0.9661	0.9190	0.9820	0.9399	0.9735	**0.9900**
Bluheron	0.9673	0.9549	0.9835	0.9460	0.9755	**0.9856**
Athens	0.9678	0.9763	0.9823	0.9468	0.9745	**0.9928**
Sea	0.9532	0.9495	0.9809	0.9287	0.9669	**0.9982**
Average	0.9620	0.9478	0.9816	0.9368	0.9717	**0.9923**

Table 4 – The NC measurements from different algorithms.

Host image	SSIM					
	(Yuan *et al*., 2020b)	(Goléa *et al*., 2010)	(Chen *et al*., 2022)	(Yuan *et al*., 2020a)	(Wang *et al*., 2023)	Proposed
Lena	**1.0000**	0.9937	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Avion	**1.0000**	0.9949	**1.0000**	**1.0000**	**1.0000**	**0.9999**
Bobcat	**1.0000**	0.8178	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Bluheron	**1.0000**	0.9926	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Athens	**1.0000**	0.9973	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Sea	**1.0000**	0.9954	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Average	**1.0000**	0.9653	**1.0000**	**1.0000**	**1.0000**	**1.0000**

4.2 Robustness performance analysis

Robustness evaluation in image watermarking is a critical aspect of assessing the performance and reliability of a watermarking algorithm. It involves testing the algorithm's ability to maintain the integrity and detectability of the embedded watermark when the watermarked image undergoes various attacks, transformations, or modifications.

In this section, we perform comprehensive simulation experiments to assess the robustness of our proposed method. These experiments encompass individual assessments of our algorithm and comparative evaluations with other advanced algorithms (Chen *et al*., 2021; Goléa *et al*., 2010; Wang *et al*., 2023; Yuan *et al*., 2020a; Yuan *et al*., 2020b).

We employ the Lena, Avion and Sea images from Figure 2 as host images and the images in Figure 3 as watermarks, respectively. Subsequently, we embed these watermarks and perform extraction following a sequence of a wide range of attacks and distortions that an image may encounter, including but not limited to compression, noise, cropping, scaling, rotation, filtering, and geometric transformations. The particular types of attacks are detailed in Table 5.

Table 5 – Various attacks used in the experiment.

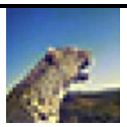
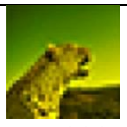
Attack index	Attack	Parameters
A1	JPEG compression	QF = 90
A2	JPEG compression	QF = 30
A3	JPEG 2000 compression	CR = (5:1)
A4	JPEG 2000 compression	CR = (10:1)
A5	Gaussian noise	Var = 0.001
A6	Gaussian noise	Var = 0.003
A7	Salt and peppers noise	0.2 %
A8	Salt and peppers noise	1 %
A9	Median filtering	3 × 3
A10	Median filtering	2 × 2
A11	Cropping	25 %
A12	Cropping	50 %
A13	Zoom-in	(4:1)
A14	Zoom-out	(1:2)
A15	Rotation	15°
A16	Rotation	30°
A17	Translation	(10, 20, 0)
A18	Translation	(-40, -20, 0)

Table 6 contains imperceptibility performance measurements for different watermark-host image combinations (Peugeot-Lena, Number-Avion, Leopard-Sea) under various attacks (A1, A3, A5, ... A17) applied to the watermarked image.

The table provides the NC measurements for each watermark and the extracted watermark image combination under specific attack conditions. It is clearly seen that the analysis reveals that most cases fall into the "high imperceptibility" category, with NC values exceeding 0.99 and equaling 1 in some cases, indicating strong watermark imperceptibility. Nonetheless, there are some cases where moderate imperceptibility is observed, specifically when subjected to cropping by 25%, a 15° rotation, and translation with parameters (10, 20, 0). In these instances, the NC values fall within the range of 0.72 to 0.85.

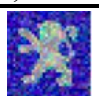
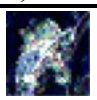
These lower values suggest that these particular attacks have a mild impact on the visibility of the watermark. It's important to note that the extracted watermarks, as presented in Table 6, generally maintain exceptional visual quality and faithfully replicate the original watermark. The only exception is that they may appear slightly brighter due to the cropping by 25%, the 15° rotation, and the translation with parameters (10, 20, 0) attacks.

Table 6 – Imperceptibility performance using different parameters.

Watermarks / Attacks	Peugeot in Lena	Number in Avion	Leopard in Sea
A1			
NC	0.9979	0.9963	0.9959
A3			
NC	0.9995	0.9998	0.9996
A5			
NC	0.9988	0.9991	0.9923
A7			
NC	0.9993	0.9993	0.9951
A9			
NC	0.9908	0.9981	0.9984
A11			
NC	0.9627	0.8196	0.7444
A13			
NC	1.0000	1.0000	1.0000
A15			
NC	0.7280	0.8428	0.7962
A17			
NC	0.7349	0.8196	0.7444

Furthermore, we include other advanced algorithms for comparative purposes. These algorithms are evaluated using different combinations of watermarks and host images (Peugeot-Lena and Number-Avion) under various post-embedding attacks (A2, A4, A6, ... A18). We then compare the experimental outcomes with those achieved by our proposed algorithm. The specific simulation results can be found in Tables 7 and 8.

Table 7 – Robustness performance using various methods against different attacks (using Lena host image and Peugeot watermark image).

Attack index	Extracted watermark					
	(Yuan *et al.*, 2020b)	(Goléa *et al.*, 2010)	(Chen *et al.*, 2022)	(Yuan *et al.*, 2020a)	(Wang *et al.*, 2023)	Proposed
A2						
NC	0.7763	0.6531	0.5064	0.9404	0.8577	**0.9808**
A4						
NC	0.8835	0.8071	0.7698	0.9561	0.9383	**0.9995**
A6						
NC	0.8720	0.5903	0.7473	0.8298	0.7623	**0.9935**
A8						
NC	0.9245	0.7050	0.9724	0.8963	0.9478	**0.9912**
A10						
NC	0.8302	0.6517	0.7425	0.8847	0.8439	**0.9983**
A12						
NC	0.8722	0.4455	0.8478	0.8456	0.8398	**0.9632**
A14						
NC	0.9222	0.5698	0.7525	0.8252	0.9833	**0.9968**
A16						
NC	0.8840	0.7630	0.6431	0.8113	**0.9062**	0.7251
A18						
NC	0.9822	**0.9697**	0.8529	0.8589	0.9404	0.7251

JPEG and JPEG 2000, which are widely-used standard image compression methods, were employed in the evaluation. The outcomes of the proposed method, with NC values ranging from 0.9808 to 0.9998, demonstrate the robustness of our algorithm against image compression. As shown in Tables 7 and 8, it is clearly seen that the extracted watermarks remain identifiable and maintain good visual quality even after image compression.

The experimental outcomes of various algorithms were assessed under two common noise attacks, Gaussian and Salt and Pepper. The NC values observed, falling within the range of 0.9872 to 0.9965, provide strong evidence that our proposed algorithm exhibits higher resistance to these types of noise compared to all other algorithms, which showed NC values ranging from 0.5903 to 0.9724.

Table 8 – Robustness performance using various methods against different attacks (using Avion host image and Number watermark image).

Attack index	Extracted watermark					
	(Yuan *et al.*, 2020b)	(Goléa *et al.*, 2010)	(Chen *et al.*, 2022)	(Yuan *et al.*, 2020a)	(Wang *et al.*, 2023)	Proposed
A2						
NC	0.6870	0.7797	0.7934	0.9369	0.7541	**0.9881**
A4						
NC	0.7967	0.7191	0.7857	0.8821	0.8405	**0.9998**
A6						
NC	0.7792	0.6938	0.7333	0.7498	0.6478	**0.9965**
A8						
NC	0.8625	0.8135	0.9598	0.8740	0.9251	**0.9872**
A10						
NC	0.7221	0.6234	0.6580	0.7914	0.7009	**0.9992**
A12						
NC	0.8067	0.5211	**0.9633**	0.9615	0.9625	0.8200
A14						
NC	0.8668	0.5651	0.7109	0.7351	0.7999	**0.9989**
A16						
NC	0.7804	0.7714	0.6514	**0.8406**	0.8224	0.8274
A18						
NC	0.8927	0.8436	0.9855	**0.9894**	0.9873	0.8196

Furthermore, it's worth highlighting that our proposed algorithm exhibits notable robustness against median filtering attacks using various window sizes, specifically 2x2 and 3x3. The NC values are 0.9983 and 0.9992 for 2x2 windows and 0.9908 and 0.9981 for 3x3 windows for both image combinations, Peugeot-Lena and Number-Avion, respectively. In these cases, the watermark retains its high visual quality and faithfully mirrors the original watermark, underscoring the resilience of our proposed method against these diverse attacks.

When assessing the robustness of a watermarking algorithm, it's important to consider its performance under various geometric attacks in addition to attacks involving compression, noise, and filtering. Geometric attacks, such as cropping, scaling, rotation, and translation, are crucial aspects to evaluate. Tables 7 and 8 present the results of these geometric attacks for our proposed algorithm and advanced algorithms.

The experimental outcomes indicate that our algorithm excels in extracting watermarks with better identification and higher NC values, providing clear advantages over most other algorithms. The only exceptions are cases where the extracted watermarks may appear slightly brighter, which occurs during cropping by 50%, a 30° rotation, and translation with parameters (-40, -20, 0) attacks, resulting in NC values ranging from 0.72 to 0.83.

4. Conclusions

In this paper, we introduce an innovative and robust image watermarking technique designed for color images. This method relies on the combination of DCHWT and SVD, resulting in a substantial improvement in both robustness and invisibility. Furthermore, our approach incorporates the use of the generalized Arnold transform for successive watermark encryption, significantly enhancing the security of the watermarking process.

We assess the performance of this proposed algorithm against various types of attacks, including common image processing attacks and geometric distortions. The results reveal that the watermarked images exhibit a favorable level of visual quality, as evidenced by high PSNRs and SSIMs. Moreover, our method demonstrates its ability to successfully extract watermarks even when subjected to diverse attacks, as indicated by the high NC values. The performance analysis highlights that our proposed watermarking algorithm excels and offers distinct advantages compared to other advanced algorithms.

In our future work, we plan to extend the application of this algorithm to real-time video watermarking, making it suitable for use in fields such as telemedicine, surveillance, and security applications. Additionally, we will develop the use of enhanced algorithms to further elevate the watermarking performance.

References

Abadi, R. Y., & Moallem, P. (2022). Robust and optimum color image watermarking method based on a combination of DWT and DCT. *Optik*, 261, 169146, https://doi.org/10.1016/j.ijleo.2022.169146.

Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., ... & Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. *IEEE Access*, 10, 26257-26270, https://doi.org/10.1109/ACCESS.2022.3151174.

Ahmadi, S. B. B., Zhang, G., Rabbani, M., Boukela, L., & Jelodar, H. (2021). An intelligent and blind dual color image watermarking for authentication and copyright protection. *Applied Intelligence*, 51, 1701-1732, https://doi.org/10.1007/s10489-020-01903-0.

Al-Ghaili, A. M., Kasim, H., Hassan, Z., Al-Hada, N. M., Othman, M., Kasmani, R. M., & Shayea, I. (2023). A Review: Image Processing Techniques' Roles towards Energy-Efficient and Secure IoT. *Applied Sciences*, 13(4), 2098, https://doi.org/10.3390/app13042098.

Alqahtani, A. S., Madheswari, A. N., Mubarakali, A., & Parthasarathy, P. (2023). Secure communication and implementation of handwritten digit recognition using deep neural network. *Optical and Quantum Electronics*, 55(1), 27, https://doi.org/10.1007/s11082-022-04290-7.

An, F. P., & Liu, J. E. (2019). Image encryption algorithm based on adaptive wavelet chaos. *Journal of Sensors*, 2019, 1-12, https://doi.org/10.1155/2019/2768121.

Ariatmanto, D., & Ernawan, F. (2022). Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking. *Journal of King Saud University-Computer and Information Sciences*, 34(3), 605-614, https://doi.org/10.1016/j.jksuci.2020.02.005.

Arnold, V. I., & Avez, A. (1968). *Ergodic problems of classical mechanics*.

Chen, S., Su, Q., Wang, H., & Wang, G. (2022). A high-efficiency blind watermarking algorithm for double color image using Walsh Hadamard transform. *The Visual Computer*, 38(6), 2189-2205, https://doi.org/10.1007/s00371-021-02277-1.

Chen, Y., Jia, Z. G., Peng, Y., Peng, Y. X., & Zhang, D. (2021). A new structure-preserving quaternion QR decomposition method for color image blind watermarking. *Signal Processing*, 185, 108088, https://doi.org/10.1016/j.sigpro.2021.108088.

Dataset, C.-U. I. (2002). University of Granada, *Computer Vision Group*. In. https://ccia.ugr.es/cvg/dbimagenes/c512.php. (Last accessed: 02/02/2023).

Dataset, S. I. (1997). University of Southern California, *signal and image processing institute*. In. https://sipi.usc.edu/database/. (Last accessed: 02/02/2023).

Dhyani, S., & Singh, R. (2016). Multifocus and multispectral image fusion based on pixel features using discrete cosine harmonic wavelet transformed and morphological filter. *Signal, Image and Video Processing*, 7(6), 1125-1143,

Dwivedi, R., Awasthi, D., & Srivastava, V. K. (2023). An Optimized Dual Image Watermarking Scheme based on Redundant DWT and Randomized SVD with Henon Mapping Encryption. Circuits, *Systems, and Signal Processing*, 1-49, https://doi.org/10.1007/s00034-023-02479-z.

Elkandoz, M. T., & Alexan, W. (2022). Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications*, 81(18), 25497-25518. https://doi.org/10.1007/s11042-022-12595-8.

Eltoukhy, M. M., Khedr, A. E., Abdel-Aziz, M. M., & Hosny, K. M. (2023). Robust watermarking method for securing color medical images using Slant-SVD-QFT transforms and OTP encryption. *Alexandria Engineering Journal*, 78, 517-529, https://doi.org/10.1016/j.aej.2023.07.068.

Ernawan, F. (2019). Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection. *International Journal of Electrical and Computer Engineering*, 9(3), 1850. http://doi.org/10.11591/ijece.v9i3.pp1850-1860.

Ernawan, F., & Ariatmanto, D. (2023). A recent survey on image watermarking using scaling factor techniques for copyright protection. *Multimedia Tools and Applications*, 1-41. https://doi.org/10.1007/s11042-023-14447-5.

Goléa, N. E. H., Seghir, R., & Benzid, R. (2010, May). A bind RGB color image watermarking based on singular value decomposition. In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010 (pp. 1-5). IEEE, https://doi.org/10.1109/AICCSA.2010.5586967.

Hosny, K. M., Darwish, M. M., & Fouda, M. M. (2021). Robust color images watermarking using new fractional-order exponent moments. *IEEE Access*, 9, 47425-47435, https://doi.org/10.1109/ACCESS.2021.3068211.

Keivani, M., Sazdar, A. M., Mazloum, J., & Rahmani, A. E. (2020). Application of Empirical Wavelet Transform in Digital Image Watermarking. *Traitement du Signal*, 37(5), https://doi.org/10.18280/ts.370517.

Kiranmayi, G. R., & Udayashankara, V. (2020). Detection of epilepsy using discrete cosine harmonic wavelet transform-based features and neural network classifier. *International Journal of Biomedical Engineering and Technology*, 32(2), 109-122, https://doi.org/10.1504/IJBET.2020.105649.

Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in Cyber Security. *Defence Science Journal*, 66(6), https://doi.org/10.14429/dsj.66.10800.

Latreche, B. (2023). CT and MRI image fusion based on variance and pixel significance. *The Journal of Engineering and Exact Sciences*, 9(9), 16619-01e, https://doi.org/10.18540/jcecvl9iss9pp16619-01e.

Latreche, B., Saadi, S., Kious, M., & Benziane, A. (2019). A novel hybrid image fusion method based on integer lifting wavelet and discrete cosine transformer for visual sensor networks. *Multimedia Tools and Applications*, 78, 10865-10887, https://doi.org/10.1007/s11042-018-6676-z.

Lin, C. C., He, S. L., & Chang, C. C. (2021). Pixel-based fragile image watermarking based on absolute moment block truncation coding. *Multimedia Tools and Applications*, 80(19), 29497-29518, https://doi.org/10.1007/s11042-021-10598-5.

Lin, C., & Xu, X. (2021). An Electronic Bill Encryption Algorithm Based on Multiple Watermark Encryption. Traitement du Signal, 38(1), https://doi.org/10.18280/ts.380113.

Liu, D., Yuan, Z., & Su, Q. (2020). A blind color image watermarking scheme with variable steps based on Schur decomposition. *Multimedia Tools and Applications*, 79, 7491-7513, https://doi.org/10.1007/s11042-019-08423-1

Liu, W., & Chen, W. (2019). Recent advancements in empirical wavelet transform and its applications. *IEEE Access*, 7, 103770-103780, https://doi.org/10.1109/ACCESS.2019.2930529.

McFee, B. (2023). *Digital Signals Theory*. CRC Press, https://doi.org/10.1201/9781003264859.

Mohanty, S. P. (1999). *Watermarking of digital images*. Submitted at Indian Institute of Science Bangalore, 1-3.

Moosazadeh, M., & Ekbatanifard, G. (2017). An improved robust image watermarking method using DCT and YCoCg-R color space. *Optik*, 140, 975-988, https://doi.org/10.1016/j.ijleo.2017.05.011.

Narasimhan, S. V., Harish, M., Haripriya, A. R., & Basumallick, N. (2009). Discrete cosine harmonic wavelet transform and its application to signal compression and subband spectral estimation using modified group delay. *Signal, Image and Video Processing*, 3, 85-99, https://doi.org/10.1007/s11760-008-0062-7.

Newland, D. E. (1993). Harmonic wavelet analysis. Proceedings of the Royal Society of London. *Series A: Mathematical and Physical Sciences*, 443(1917), 203-225, https://doi.org/10.1098/rspa.1993.0140.

Newland, D. E. (1998). Time-frequency and time-scale signal analysis by harmonic wavelets. *In Signal analysis and prediction* (pp. 3-26). Boston, MA: Birkhäuser Boston, https://doi.org/10.1007/978-1-4612-1768-8_1.

Pandey, M. K., Parmar, G., Gupta, R., & Sikander, A. (2019). Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space. *Microsystem Technologies*, 25, 3071-3081, https://doi.org/10.1007/s00542-018-4162-1.

Patsariya, S., & Dixit, M. (2022). Entropy Based Secure and Robust Image Watermarking Using Lifting Wavelet Transform and Multi-Level-Multiple Image Scrambling Technique. *Traitement du Signal*, 39(5), https://doi.org/10.18280/ts.390533.

Patsariya, S., & Dixit, M. (2022). A New Block Based Non-Blind Hybrid Color Image Watermarking Approach Using Lifting Scheme and Chaotic Encryption Based on Arnold Cat Map. *Traitement du Signal*, 39(4), https://doi.org/10.18280/ts.390408.

Qi, W., Yang, G., Zhang, T., & Guo, Z. (2019). Improved reversible visible image watermarking based on HVS and ROI-selection. *Multimedia Tools and Applications*, 78, 8289-8310, https://doi.org/10.1007/s11042-018-6812-9.

Rahardi, M., Abdulloh, F. F., & Putra, W. S. (2022). A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection. *International Journal of Advanced Computer Science and Applications*, 13(7), https://dx.doi.org/10.14569/IJACSA.2022.0130785.

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.

Roopa, S., & Narasimhan, S. V. (2014). S-transform based on analytic discrete cosine transform for time–frequency analysis. *Signal processing*, 105, 207-215, https://doi.org/10.1016/j.sigpro.2014.05.035.

Shreyamsha Kumar, B. K. (2013). Multifocus and multispectral image fusion based on pixel significance using discrete cosine harmonic wavelet transform. *Signal, Image and Video Processing*, 7, 1125-1143, https://doi.org/10.1007/s11760-012-0361-x.

Soualmi, A., Benhocine, A., & Midoun, I. (2023). Artificial Bee Colony-Based Blind Watermarking Scheme for Color Images Alter Detection Using BRISK Features and DCT. *Arabian Journal for Science and Engineering*, 1-14, https://doi.org/10.1007/s13369-023-07958-8.

Su, Q., & Chen, B. (2018). Robust color image watermarking technique in the spatial domain. *Soft Computing*, 22, 91-106, https://doi.org/10.1007/s00500-017-2489-7.

Su, Q., Zhang, X., & Wang, H. (2022). A blind color image watermarking algorithm combined spatial domain and SVD. *International Journal of Intelligent Systems*, 37(8), 4747-4771, https://doi.org/10.1002/int.22738.

Supiyandi, S., Sihombing, G. L. A., Siburian, H. K., Purnomo, A., Anam, F., Emanuel, E. P. L., ... & Rahim15, R. (2018). Application of Invisible Image Watermarking. *Int. J. Eng. Technol*, 7(2), 760-762, https://doi.org/10.14419/ijet.v7i3.2.18749.

Taha, D. B., Taha, T. B., & Al Dabagh, N. B. (2020). A comparison between the performance of DWT and LWT in image watermarking. *Bulletin of Electrical Engineering and Informatics*, 9(3), 1005-1014, https://doi.org/10.11591/eei.v9i3.1754.

Tan, L., & Jiang, J. (2018). *Digital signal processing: fundamentals and applications*. Academic press.

Vaidya, S. P., & Mouli, P. C. (2023). Robust digital color image watermarking based on compressive sensing and DWT. *Multimedia Tools and Applications*, 1-15, https://doi.org/10.1007/s11042-023-15349-2.

Wang, D., Yang, F., & Zhang, H. (2016). Blind Color Image Watermarking Based on DWT and LU Decomposition. *J. Inf. Process. Syst.*, 12(4), 765-778, https://doi.org/10.3745/JIPS.03.0055.

Wang, H., Yuan, Z., Chen, S., & Su, Q. (2023). Embedding color watermark image to color host image based on 2D-DCT. *Optik*, 274, 170585, https://doi.org/10.1016/j.ijleo.2023.170585.

Wang, K., Gao, T., You, D., Wu, X., & Kan, H. (2022). A secure dual-color image watermarking scheme based 2D DWT, SVD and Chaotic map. *Multimedia Tools and Applications*, 81(5), 6159-6190, https://doi.org/10.1007/s11042-021-11725-y.

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4), 600-612, https://doi.org/10.1109/TIP.2003.819861.

Yasmeen, F., & Uddin, M. S. (2021). An efficient watermarking approach based on LL and HH edges of DWT–SVD. *SN Computer Science*, 2(2), 82, https://doi.org/10.1007/s42979-021-00478-y.

Yuan, Z., Liu, D., Zhang, X., & Su, Q. (2020). New image blind watermarking method based on two-dimensional discrete cosine transform. *Optik*, 204, 164152, https://doi.org/10.1016/j.ijleo.2019.164152.

Yuan, Z., Liu, D., Zhang, X., Wang, H., & Su, Q. (2020). DCT-based color digital image blind watermarking method with variable steps. *Multimedia Tools and Applications*, 79, 30557-30581, https://doi.org/10.1007/s11042-020-09499-w.

Zhang, M., Ding, W., Li, Y., Sun, J., & Liu, Z. (2023). Color image watermarking based on a fast structure-preserving algorithm of quaternion singular value decomposition. *Signal Processing*, 208, 108971, https://doi.org/10.1016/j.sigpro.2023.108971.

Zhu, H., Zhao, C., Zhang, X., & Yang, L. (2014). An image encryption scheme using generalized Arnold map and affine cipher. *Optik*, 125(22), 6672-6677, https://doi.org/10.1016/j.ijleo.2014.06.149.