IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 2, April, 2025, pp. 617-633
Journal homepage: http://iieta.org/journals/ts

WH-SVD-Cb: A Robust Blind Watermarking Scheme Using Wavelet Transform and Hessenberg SVD with Arnold Chaotic Map in the Cb Channel

Farid Ayeche[1], Adel Alti[2,3*], Bilal Benmessahel[1]

[1] LMETR Laboratory, E1764200 Optics and Precision Mechanics Institute, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria
[2] LRSD, Computer Science Department, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria
[3] Department of Management Information Systems, College of Business & Economics Qassim University, Buraidah 51452, KSA

Corresponding Author Email: a.alti@qu.edu.sa

https://doi.org/10.18280/ts.420203

Received: 16 August 2024
Revised: 12 December 2024
Accepted: 21 March 2025
Available online: 30 April 2025

Keywords:
color images, DWT, HSV, watermarking, imperceptibility, robustness, WH-SVD-Cb

ABSTRACT

With the significant growth of malicious attacks, safeguarding personal data has become a critical and pressing concern. Images transmitted over unsecured networks are particularly vulnerable to tampering and unauthorized distribution. To address these challenges, networks must be fortified with robust strategies capable of preventing new attacks. These strategies should prioritize enhanced performance while maintaining content fidelity. The article presents a blind approach for color image watermarking that leverages the YCbCr color space's key properties. Both the image and the watermark were converted from RGB to YCbCr. Afterward, the watermark is encrypted using the Arnold Chaotic Map (ACM) to strengthen privacy and embedded into the Cb component using the WH-SVD-Cb watermarking schema. Image authenticity is validated through blind watermark extraction. The method's robustness and imperceptibility are analyzed through empirical evaluations. The findings indicate that embedding of watermark in the Cb component achieves notable robustness with NC values closing 1 and imperceptibility exceeding 52 dB, all within a processing time of 0.224 seconds. A demonstration code for the proposed watermarking scheme is available: https://www.mathworks.com/matlabcentral/fileexchange/177859-digital-color-image-watermarking-using-dwt-svd-hd-acm.

1. INTRODUCTION

The fast evolution of connected systems and the widespread use of Internet, coupled with significant advances in multimedia devices such as smartphones and cameras, have facilitated the transmission of various types of multimedia content. However, these advancements are compounded due to the ease of modifying digital content, making robust methods for authentication and recovery essential to maintaining trust and reliability in digital systems [1, 2].

Image watermarking has become a prominent technique for ensuring image authentication and security, providing a method to embed verification data directly within a cover image [3, 4]. In this approach, the evaluation of watermarking technique is based on two key criteria: imperceptibility and robustness [5, 6]. Two kinds of watermarking according to embedding domain: spatial techniques and transform techniques. In the first domain, the watermark is seamlessly incrusted into the transformed coefficients, whereas in the second domain, it is inserted into the pixel's values, employing widely methods such as DCT insertion and statistical-based approaches. Additionally, methods for extracting watermark can be classified into three types: (1) blind, no need for the host image during extraction. (2) semi-blind, needs the first watermark to retrieve the incrusted watermark and (3) non-blind, allows the direct recovery of watermark [7-9].

Cryptography methods have also made substantial progress in addressing various security challenges. However, these methods pose a significant obstacle to prevent unauthorized duplication and cannot fully guarantee authenticity or ownership protection. By strategically embedding encrypted data into optimal locations using watermarking techniques, a robust hybrid approach can be achieved to defend against external attacks.

Numerous crypto-watermarking techniques have been introduced in previous studies [10-35]. While these methods protect image content effectively, they often come with high computational demands and resource requirements. The proposed schema aims to address these challenges by combining cryptography and watermarking to safeguard image content while reducing execution time and maintaining high imperceptibility. Unlike some existing methods [13, 18, 26], which focus primarily on grayscale or limited aspects of color image watermarking, relatively few approaches target color images which are often inserted in the blue component of the RGB model. An alternative watermark embedding approach uses the Y channel of the YCbCr model, granting that the watermark remains imperceptible while providing

adequate robustness [27]. This method lacks a comprehensive strategy to balance robustness, imperceptibility, and execution efficiency. A unique feature of the proposed approach is the deliberate insertion of confidential information embedded into the Cb component. The Cb channel, representing chrominance information, is less perceptible to the human eye than the luminance channel (Y), enabling watermark embedding with strong robustness while preserving the image visual quality. The focus on the Cb channel, combined with the integration of two decompositions (SVD and HD) highlights their critical role in balancing between robustness, imperceptibility and computational time.

This study intends to advance the field of watermarking technique by leveraging the potential of the Cb channel in the YCbCr color space to strengthen privacy and security using a scheme known as WH-SVD-Cb. It combines transformation and encryption techniques, including Discrete Wavelet Transformation (DWT), HD and SVD with enhanced visual detail preservation to overcome the limitations of existing frameworks. A visual preservation mechanism that customizes the watermark embedding process for the Cb component. This approach improves the quality of watermarked images, reduces processing time for embedding watermarks in color images and ensuring protection against different forms of attacks. To secure the watermarked color images, an encryption algorithm based on Arnold's chaotic map is utilized. The key contributions and innovations of this paper include:

(1) New Kernel Functions: WH-SVD-Cb introduces two new kernel functions for embedding and extracting a watermark, serving as standard kernels for image watermarking in both color and grayscale domains.

(2) Improved Secret Data Embedding: WH-SVD-Cb enhances imperceptibility by incrusting the secret data in the Cb component of the YCbCr space using transformation and encryption techniques. The integration of HD, SVD, and Arnold's Chaotic Map within the DWT domain boosts robustness and security. This study delves into the YCbCr color space, introducing watermark into Cb component to achieve the desired outcomes.

(3) Comprehensive Evaluation: A thorough qualitative and quantitative analysis of WH-SVD-Cb scheme is conducted across different images s images of varying sizes. WH-SVD-Cb scheme is evaluated against several recent watermarking techniques, emphasizing its advantages in imperceptibility, robustness, and execution time.

Section 2 reviews current watermarking techniques, emphasizing their advantages, drawbacks and applications across different domains. Section 3 details the main content of fundamental methods and provides the necessary theoretical background for understanding the proposed techniques. Section 4 presents WH-SVD-Cb scheme including its enhanced visual human preservation. Section 5 compares the performance of WH-SVD-Cb against other methods. Section 6 recaps the paper and offers insights into possible directions for future research endeavors.

2. RELATED WORKS

Several research studies in image security focus on watermarking and cryptography methods. This section provides an overview of pertinent and recent works.

Liu et al. [10] encrusted the scrambled data in the transform field to achieve good visual quality. They identified the Regions of Interest (ROI) within the image blocks, with both embedding and extraction methods using transformation techniques. The study demonstrated good imperceptibility and security, producing promising outcomes to standard threats.

Vaidya et al. [11] developed a blind and robust approach to address the security concerns. Their approach combined the RSA algorithm and logistic scrambling algorithm to incrust hidden data in the low-frequency sub-host band. This embedding strategy makes the proposed system to be highly resistant to various attacks while preserving the image quality, although it may involve high computational complexity due to the extensive tasks required for embedding and extraction.

Ernawan et al. [12] proposed using multiple decompositions to safeguard copyright and embed grayscale watermark in color images. A private key is generated for the grayscale watermark to enhance security. The proposed approach exhibits good imperceptibility and offers significant resilience to attacks in image processing.

Liu et al. [13] considered the watermarking performance as an optimization problem, using a fractal coding method combined with an improved Discrete Cosine Transform (DCT) approach. Initially, they used fractal encoding to secure the host image and then used the DCT method. The approach was tested against different attacks and showed perfect robustness, though it required significant resources and time.

Savakar and Ghuli [14] mixed blind and unblind methods. Initially, blind watermarks are used, followed by non-blind watermarks as outer watermarks. Research results indicated that the suggested method provides significant resilience to different types of attacks. However, due to the non-blind embedding, it is less practical compared to other methods.

Su et al. [15] employed Discrete Fourier Transform (DFT) for incrusting watermark. The watermark is embedded in Direct Current (DC) coefficients. The simulations results showed satisfactory robustness. However, the embedding technique is semi-blind, which reduces its practicality.

Kumar et al. [16] combined various transformation techniques approach (e.g., DWT, DCT and SVD) to enhance the robustness with advanced attacks. They also applied hierarchical trees and Arnold transformation to enhance robustness. While the proposed approach gained useful performance such as robustness and imperceptibility, it suffered from high execution time.

In the study by Fares et al. [17], a new approach for color image authentication is suggested, embedding the watermark using a new substitution scheme to ensure content security. A strong watermarking based on Fourier transform is applied to incrust hidden data in the middle-frequency band. However, this approach struggled to find an ideal balance among robustness, imperceptibility, and execution time, and it did not consider important color space representations like YCbCr.

Anand and Singh [18] addressed the authentication issue in medical image watermarking by proposing a multi-watermark embedding technique. The goal was to minimize channel noise distortion for delicate data. While the watermark is encrypted and hidden, the proposed system is more vulnerable to JPEG compression and histogram equalization attacks.

In the study by Mishra et al. [19], a machine-learning approach is introduced to watermark compressed JPEG images in order to enhance the resistance and discreteness, it faced challenges with high execution time. The results indicated that the method was well-suited for real-time applications. However, the approach not applied to the YCbCr color space.

Ambadekar et al. [20] proposed a digital image watermarking by incrusting an encoded watermark into the original image to maintain good imperceptibility. This process o part of watermark encryption in the transformation domain, utilizing DWT for embedding and extraction. The technique showed resilience to noise, geometric, and compression attacks.

Singh et al. [21] formulated watermarking performance as a multi-objective optimization problem, employing Genetic Algorithm (GA) and Artificial Bee Colony (ABC) techniques. approach shows promising outcomes in authentication, robustness and copyright protection. However, it faces limitations in terms of imperceptibility. Boujerfaoui et al. [22] highlighted the evolution of watermarking techniques, particularly their integration with deep learning for intelligent image watermarking.

Image watermarking has evolved to address key issues such as robustness, reversibility, and the potential for quantum applications. Methods leveraging frequency coefficient variance offer durability against compression [23], while reversible techniques like modified LSB matching with pixel difference prioritize lossless image recovery for sensitive use cases [24]. The introduction of digital-to-quantum watermarking introduces quantum mechanics for enhanced security, bridging traditional methods with future advancements [25].

Lakrissi et al. [26] introduced an innovative method in RGB space that utilizes DWT, SVD, and HVS. The approach embeds watermarks into regions of the image identified by HVS as less perceptible, ensuring imperceptibility while maintaining robustness against various attacks. Blind watermarking approaches utilizing hybrid orientation and region complexity focus on balancing visual quality and security while ensuring robustness [28].

For medical images, Ansari et al. [29] introduced a strong approach based on Wavelet Transform (IWT) and ABC optimization to improve the balance between resilience and accuracy. Techniques based on Hessenberg matrix and SVD coefficients combined with DWT domain, enable watermark watermarking that balances robustness and imperceptibility [30]. Blind watermarking methods using the Hessenberg matrix for color images show strong resistance to common image processing [31].

The RDWT-based blind watermarking alters the watermark embedding process by considering the inherent properties of the image, striking a balance between visual image quality and resilience [32]. Another image watermarking approach emphasizes a wavelet method combined with genetic optimization algorithm, focusing on robustness and imperceptibility [33].

More recently, the trend has shifted towards multi-level security watermarking, which introduces various encryption and watermarking techniques for enhanced security [34, 35].

Table 1 highlights the main features of existing approaches cited in the studies [10-35], focusing on the type of watermark, embedding domain, and main limitations. To address these limitations, the development of color image crypto-watermarking frameworks (WH-SVD-Cb) brings further improvements in robustness and visual quality.

WH-SVD-Cb advanced the block watermarking strategy to minimize computational cost by employing a blind extraction process. Unlike existing methods, this approach embeds the watermark in the Cb component to enhance robustness and optimize performance. To enhance resilience against various attack scenarios, Hessenberg is utilized as a matrix transformation, while the SVD technique is integrated into the system's core to reinforce robustness against external attacks. In addition, Arnold's Chaotic Map is applied to encrypt the color-watermarked images, improving the system's resilience against external threats. The preservation of visual quality in the WH-SVD-Cb and the intelligent data embedding mapping of the WH-SVD-Cb are detailed in the next sections.

Table 1. Comparison of various watermarking approaches

Methods	Embedding Domain	Type of Watermark	Majors' Drawbacks
Liu et al. [10]	Spatial	Blind	Susceptible to attacks like cropping and rotation.
Liu et al. [13]			Susceptible to attacks like cropping and rotation.
Boujerfaoui et al. [22]			Vulnerable to specific types of chaotic attack models.
Ansari et al. [33]			Computationally intensive.
El-Shafai et al. [34]			Computationally intensive.
Soualmi et al. [35]			Highly sensitive with non-malicious modifications.
Kumar et al. [16]		Semi-blind	High computational overhead due to SPIHT.
Savakar and Ghuli [14]		Non-blind	High complexity, limited scalability.
Ernawan et al. [12]	Frequency	Blind	Vulnerable to image distortions in some scenarios.
Su et al. [15]			Vulnerable to lossy compression and noise.
Singh et al. [21]			Reduced robustness in high-contrast regions.
Sajeer et al. [27]			High computational cost for optimization.
Ansari et al. [29]			Vulnerable to attacks due to the use of RONI.
Su et al. [31]			Limited robustness to geometric distortions.
Nazir et al. [32]			Risk of false positives.
Vaidya et al. [11]			Computationally intensive due to multiple transforms.
Wang et al. [28]		Semi-blind	Limited adaptability for diverse images.
Liu et al. [30]			Susceptible to noise addition.
Proposed Approach		**Blind**	**A reasonable agreement among the watermarking requirements with a restricted embedding capacity.**

3. BACKGROUND

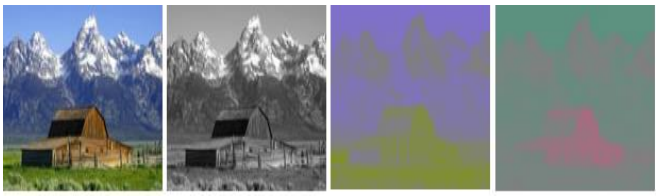
This section presents and discusses the key techniques used in developing the proposed approach.

3.1 Human Visual System (HSV)

In this scheme, we used both color host images and watermarks. The RGB model is the most widely used in a

computer and multimedia applications. This is because it directly relates to the red, green, and blue elements recognized by the human eye via three different types of vision cells. These vision cells can work together when stimulated by light to form the perception of color [26]. However, in the RGB space, there is a high degree of correlation between the components, leading to redundancy, which complicates the watermarking process. This redundancy makes it difficult to achieve an invisible watermark that remains resistant to changes.

In contrast, the YCbCr color space, which aligns with HVS, is often preferred for watermarking. In this color model, Y represents the brightness element, whereas the components Cb and Cr contain the color information. The YCbCr space is particularly effective for embedding information in channels that are less perceptible to the human eye. This makes it an optimal choice for watermarking, as it allows for hiding data that the human eye cannot easily detect. Figure 1 illustrates the three components (Y, Cb, and Cr) along with a corresponding color image in RGB.



(a) (b) (c) (d)

Figure 1. The color image in RGB is shown in (a), its corresponding components Y, Cb and Cr in (b), (c), (d)

The transformations between the two spaces RGB and YCbCr are defined by the following equations [28]:

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.5000 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.000 & 1.403 \\ 1 & -0.344 & -0.714 \\ 1 & 1.773 & 0.00 \end{bmatrix} + \begin{bmatrix} Y \\ C_b - 128 \\ C_r - 128 \end{bmatrix} \quad (2)$$

3.2 ACM

To improve security and verify legitimate ownership during the embedding and extraction processes, an encryption phase using ACM was integrated. In the proposed approach, each of three channels Y, Cb, and Cr has its encryption. The ACM, first introduced by Vladimir Arnold in 1960, is a technique where a square image is encrypted [29] by rearranging and distorting its pixels. Indeed, ACM is achieved through an iterative process in which the image is scrambled, and each iteration produces a new encrypted version of the image. This process aims to prevent unauthorized access to the watermark, even after a successful extraction.

The ACM and its inverse (ACM^{-1}) for an image I of size $N \times N$, are defined by the Eq. (1) and Eq. (2).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N \quad (3)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \right) \ mod\ N \quad (4)$$

3.3 DWT

Wavelet transformations are a widely used family of mathematical transformation tools that have found applications in various fields, particularly in engineering sciences due to their ability to decompose images in both spatial and frequency domain [24, 25].

DWT offers a good resistance to various watermarking attacks [30]. Through the application of DWT, the host image is decomposed into four unique frequency bands: Low-High (LH), High-Low (HL), High-High (HH), and Low-Low (LL). Post-transformation, the LL sub-band retains the bulk of the image's essential data. The LL sub-band is commonly chosen for watermark embedding because it preserves the host image's quality while offering greater resilience against attacks such as filtering or compression [31]. The DWT and its corresponding inverse transformation (DWT-1) of an image I are specified in Eq. (5) and Eq. (6).

$$DWT = \frac{2}{\sqrt{H \times W}} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} f(x,y) \times \phi_{j_0,x,y}(x,y) \quad (5)$$

$$DWT^{-1} = \frac{2}{\sqrt{H \times W}} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} f(x,y) \times \psi^{-1}_{j,x,y}(x,y) \quad (6)$$

3.4 Hessenberg Decomposition (HD)

HD is a mathematical process in linear algebra used to simplify triangular form called Hessenberg matrix [31, 32]. Named after the mathematician Karl Hessenberg, this technique is particularly useful in numerical analysis and computational applications, such as solving eigenvalue problems or improving computational efficiency in matrix-related algorithms. We categorize matrices into two distinct types: (1) Upper Hessenberg Matrix is a square matrix where every element beneath the first sub-diagonal is zero, and (2) Lower Hessenberg Matrix is a square matrix where every element above the first sub-diagonal is zero.

The decomposition expresses a given square matrix X as:

$$P\ H\ P^t = HD(X) \quad (7)$$

where, P is an orthogonal matrix, and H is an upper Hessenberg matrix, where the elements $H_{i,j}$ are zero for all $i > j + 1$.

In practice, we can calculate HD by the Householder matrix Q defined by Eq. (8):

$$Q = \frac{(I_n - 2\mu\mu^T)}{\mu^T\mu} \quad (8)$$

where, μ represents a nonzero vector in R^n and I^n represents identity matrix. In the overall procedure, there are $n - 2$ steps and therefore HD is calculated as:

$$P = (Q_1 Q_2 \dots Q_{n-2})^T\ X (Q_1 Q_2 \dots Q_{n-2}) \quad (9)$$

$$X = P\ H\ P^T X = P\ H\ P^T \quad (10)$$

$$HD = P^T\ X\ P \quad (11)$$

By using Hessenberg matrices, the robustness can be improved because the HD technique ensures a more accurate image [30, 31].

3.5 Singular Value Decomposition (SVD)

SVD is a mathematical method grounded in the principles of linear algebra. It transforms a set of correlated data into an uncorrelated one, revealing the key relationships within the original data [27-29]. SVD, a widely used method in image processing, is essential for analyzing image data, as images consist of non-negative scalar data that can have strong correlations between their elements.

SVD decomposes a symmetric matrix A into U, S, and V matrixes. This decomposition separates the singular values into a diagonal matrix. The resulting left, middle and rights singular matrices are U, S and V respectively. The SVD is defined in Eq. (12):

$$USV^T = SVD(Y) \tag{12}$$

where,

$$UU^T = I_n \tag{13}$$

$$VV^T = I_n \tag{14}$$

The orthonormal columns of U represent the eigenvectors of YY^T while V contains the eigenvalues of Y^TY as orthonormal columns. A can be formulated using Eq. (15):

$$Y = \sum_{i=1}^{r} \sigma_i \mu_i v_i \tag{15}$$

where, μ_i, μ_i are the i^{th} eigenvector of U and V. σ_i is the i^{th}singular value.

4. PROPOSED SCHEMA: WH-SVD-CB

In this section, we present our approach for applying principals of human visual perception using the YCbCr model. Given that the YCbCr model is less sensitive to changes, our primary objective is to exploit its key features by embedding the watermark in the Cb channel, thus improving the watermark's resilience and perceptual transparency. The method suggested consists of embedding and extraction stages. The cover image employs transformation methods like DWT, HD, and SVD, whereas the watermark is protected through the ACM technique. To regulate the visibility/invisibility of the embedded watermark, we adjust a factor (α) within the range of [0,1].

The WH-SVD-based watermarking schema based on WH-SVD, embeds the watermark in the Cb component using DWT, HD, and SVD in the Cb color space. Our approach to watermark embedding and extraction ensures high abstraction levels, simplifying the integration of various transformation techniques.

4.1 Watermark embedding function

The watermark embedding function relies on Arnold's chaotic map in conjunction with DWT, HD, and SVD as illustrated in Figure 2. The watermark is first encoded using Arnold's method to enhance its security. After encryption, the image carried out a combination of DWT, HD, and SVD transformations at multiple levels. Since SVD captures information about the image's intensities, these transformations contribute to strengthening the watermarking process, ensuring data authenticity and reinforcing the watermark's robustness. The visibility and invisibility of the embedded information are controlled by the factor (α). The embedding process is structured as follows:

(1) Divide the source image I into four sub-components: $LL, LH, HL,$ and HH:

$$DWT(I) = [LL; LH; HL; HH] \tag{16}$$

(2) Perform HD on the LL component:

$$HD(LL) = P * H * P^T \tag{17}$$

(3) Apply SVD to the matrix H:

$$SVD(H) = HU * HS * HV^T \tag{18}$$

(4) Encrypt watermark image W using Arnold chaotic map:

$$W^* = Arnold(W) \tag{19}$$

(5) Apply SVD to encrypted watermark W^*:

$$SVD(W^*) = U_{W^*} * S_{W^*} * V_{W^*}^T \tag{20}$$

(6) Compute an incrusted singular value HS_W^*:

$$HS_{W^*} = H + \alpha S_{W^*} \tag{21}$$

(7) Apply the inverse SVD o watermarked sub-band H^*:

$$H^* = HU * HS_{W^*} * HV^T \tag{22}$$

(8) Create a novel sub-band LL^* using HD^{-1}:

$$LL^* = P * H^* * P^T \tag{23}$$

(9) Produce the final watermarked image I_W in the YCbCr color space by performing DWT^{-1}:

$$I_W = iDWT(LL^*; LH, HL; HH) \tag{24}$$

4.2 The watermark extracting function

This function extracts a watermark W^* from the received watermarked image I_w as shown in Figure 3, following the procedure outlined below:

(1) Decompose a watermarked image I_w into four sub-bands LL_W, LH_W, HL_W, HH_W:

$$DWT(I_w) = [LL_W; LH_W; HL_W; HH_W] \tag{25}$$

(2) Perform HD on LL_W:

$$HD(LL_W) = P_W * H_W * P_W^T \tag{26}$$

(3) Apply SVD to H_W:

$$SVD(H_W) = H_W U * H_W S_W * H_W V^T \tag{27}$$

(4) Compute the extracted singular values S_{W^*}:

$$S_{W^*} = (H_W S_W - H S_W)/\alpha \quad (28)$$

(5) Apply the inverse SVD on the watermark:

$$W_1^* = U_{W^*} * S_{W^*} * V_{W^*}^T \quad (29)$$

(6) Apply the inverse Arnold transformation:

$$W_2^* = iArnold(W_1^*) \quad (30)$$

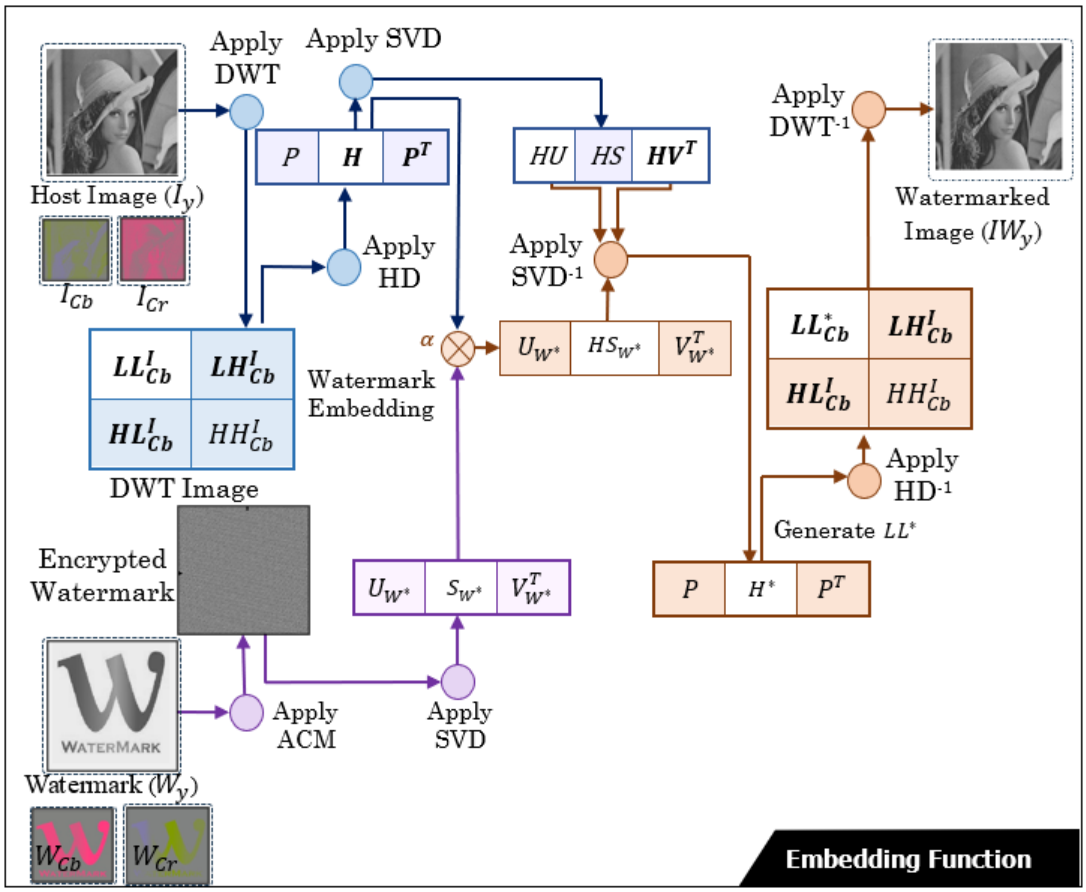


Figure 2. Watermarking embedding function

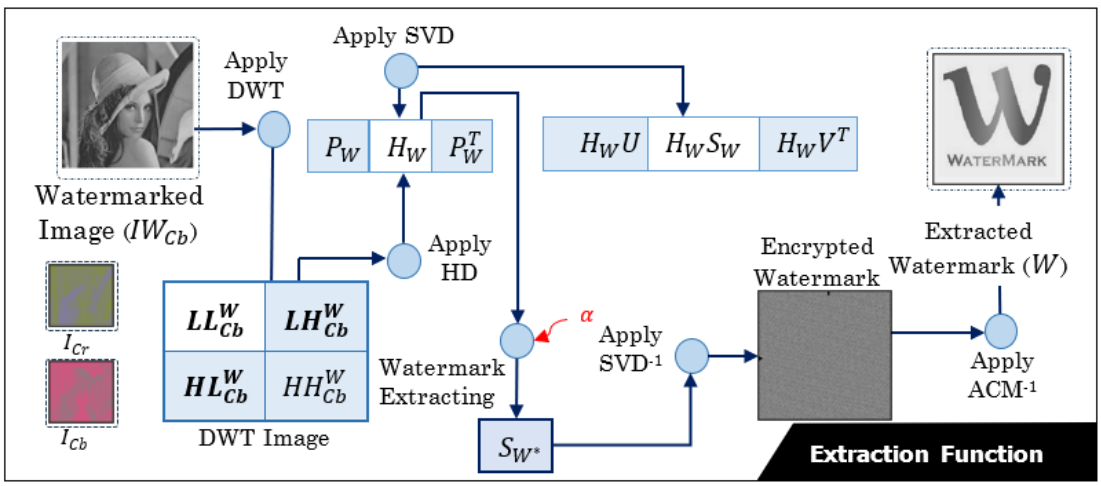


Figure 3. Watermarking extracting function

4.3 Watermark embedding and extraction

The watermark is embedded in the Cb of the YCbCr-transformed host image. Both watermarking and encryption are applied for color image protection, aiming to reinforce imperceptibility and improve security. The blind aspect of the suggested approach is validated by emphasizing that the watermark is not needed during the extraction phase. This is achieved by utilizing only the watermarked Cb channel to enable accurate extraction directly from the watermarked image. Once the image is obtained from the sender, the watermark is retrieved and restored. The processes for embedding and retrieving the watermark are presented in Figure 4 and Figure 5, respectively, and can be explained as

follows:

WH-SVD-Cb Embedding Process

Inputs: Original image *(I),* Watermark image *(W).*

Outputs: Watermarked image *(IW).*

1. Convert I from the RGB to its YCbCr components: I_Y, I_{Cb} *and* I_{Cr}.
2. Convert the RGB watermark W to its YCbCr components:W_Y, W_{Cb} and W_{Cr}.
3. Embed the watermark component W_{Cb} into I_{Cb} to get the watermarked component IW_{Cb} by the ***watermark embedding function*** and the scaling factor α as follows:

$$[\, I_{W_{Cb}}] = \text{Watermark\_Embedding}(I_Y, W_{Cb}, \alpha) \quad (31)$$

4. Combine I_Y, IW_{Cb} and I_{Cr} to get IW.

WH-SVD-Cb Extraction Process

Inputs: *Watermarked image (IW).*

Outputs: *Extracted watermark (W^*).*

1. Convert IW from RGB to its YCbCr components: IW_Y, IW_{Cb} *and* IW_{Cr}.
2. Extract W^*_{Cb} from the received watermarked component IW_{Cb} by the ***watermark extraction function*** and the scaling factor α as follows:

$$[\, W^*_Y\,] = \text{Watermark\_Extraction}(IW_Y, \alpha) \quad (32)$$

3. Combine W_Y, W_{Cr} and W^*_{Cb} to get W^*.

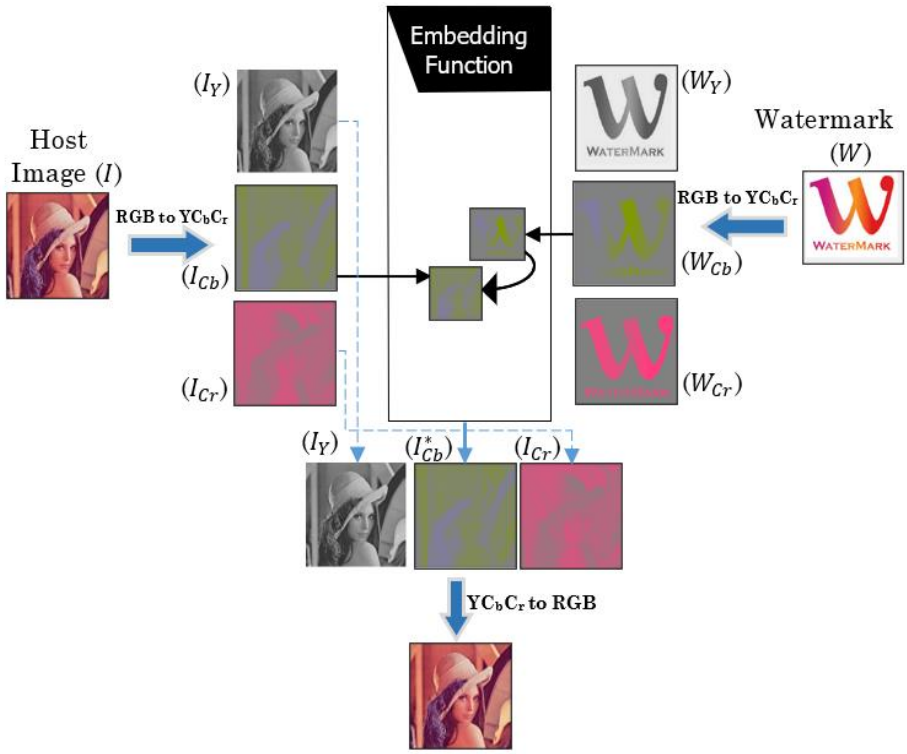


Figure 4. Watermarking embedding stage

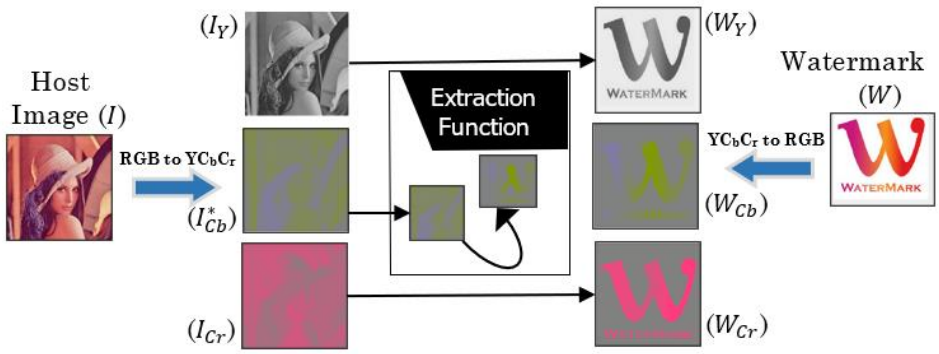


Figure 5. Watermarking extracting stage

5. EXPERIMENTAL EVALUATION

This research evaluates the performance of WH-SVD-Cb schemes in a dataset of 512 × 512 color images, and watermarks of different sizes (64 × 64, 128 × 128, 256 × 256) is used. Figure 6 illustrates samples of the color images, while Figure 7 visualizes the watermarks used in the experiment. The experimental setup consists of a computer featuring an Intel® i5-8600 processor (3.10 GHz) with 32 GB of memory, operating MATLAB R2020a on a Windows 11 platform.

Figure 8 shows the Lean host image and Airplane watermarked images

To demonstrate the advantages of WH-SVD-Cb scheme, its effectiveness is benchmarked against various contemporary methods explored in the literature. Section 5.1 examines the fidelity of the watermarked image compared to the source image using PSNR and SSIM metrics. Section 5.2 compares the robustness using NC and Section 5.3 compares the embedding and extraction execution cost. Rigorous measures were implemented to assess its performance across various scenarios. First, metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) were utilized to assess the effectiveness of watermarked and recovered watermarks. A comparative analysis was also conducted in terms of the Normalized Coefficient (NC) values over a range of α in [0.02, 0.2].

5.1 Imperceptibility evaluation and comparison

Imperceptibility plays a crucial role in watermarking, as poor imperceptibility can lead to disastrous consequences. This suggests that the sent image and its watermarked one must appear indistinguishable to the human eye. To measure the visual fidelity of the watermarked images, two standard metrics are used, the first metric is called PSNR, while the second metric is SSIM.

The PSNR value is computed as follows:

$$PSNR(X,Y) = 10 \times log_{10}\left(\frac{Max^2}{MSE}\right) dB \quad (33)$$

where, Max refers to the highest possible pixel in the image, which is usually 255 for an 8-bit color image. MSE quantifies the average of the squared differences between corresponding pixel values in the source image (X) and the watermarked image (Y), as shown below:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I_W(i,j))^2 \quad (34)$$

where, I and I_W refer to the source and watermarked images, respectively, while M and N represent the image dimensions, specifically the number of rows and columns in I and I_W. Higher PSNR values indicate better imperceptibility and high visual quality, with infinite value of PSNR representing a perfect similarity between two images [29].

Conversely, SSIM serves as a measurement for structural similarity index. The calculation of this metric is done using the equation below:

$$SSIM = \frac{(2\mu_I\mu_o + C_1)(2\sigma_{IO} + C_2)}{(\mu_I^2 + \mu_o^2 + C_1)(\sigma_I^2 + \sigma_O^2 + C_2)} \quad (35)$$

where, μ_1 and μ_o represent the mean intensity values (average brightness) of images I and O, respectively, σ_I and σ_O denote the standard deviations of images I and O, representing contrast, σ_{IO} signifies the covariance between I and O, reflecting how much the images vary together, $C_1$and C_2 are minor constants included to prevent any division errors.

Table 2 illustrates the PSNR scores for the WH-SVD-Cb scheme, using Lenna as a host image and three different sizes of airplane watermark images (256 × 256, 128 × 128, 64 × 64), with α varying between 0.005 and 0.2. The results show that WH-SVD-Cb scheme achieves high PSNR, reaching 52.11dB.

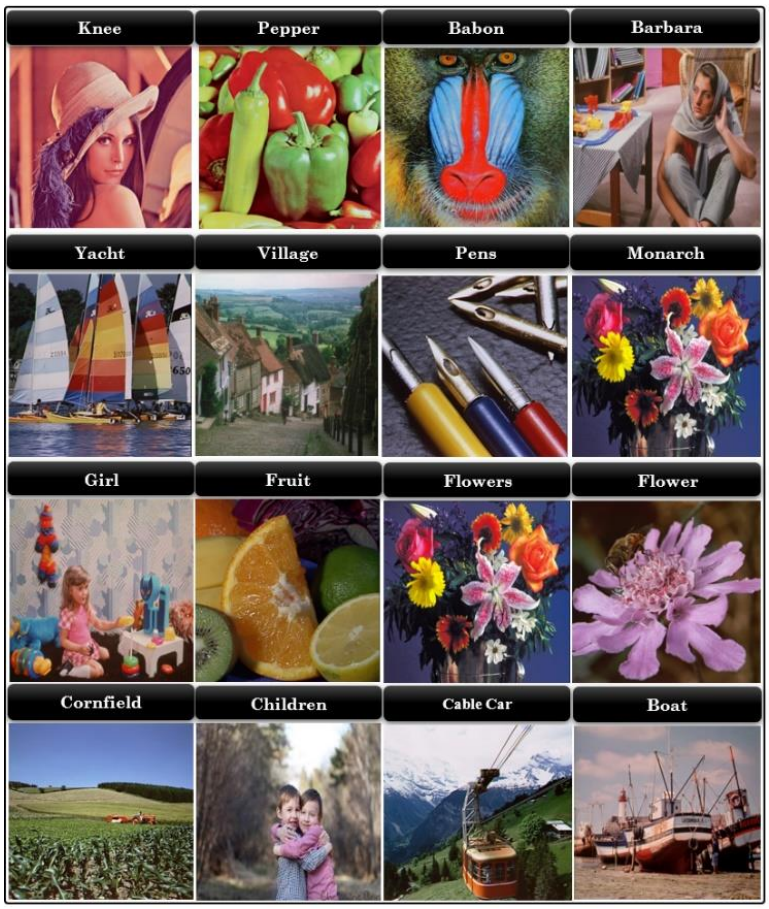


Figure 6. Sample host images used in the experiments [36]

(1) (2) (3) (4)

Figure 7. Sample of color watermarks [36]

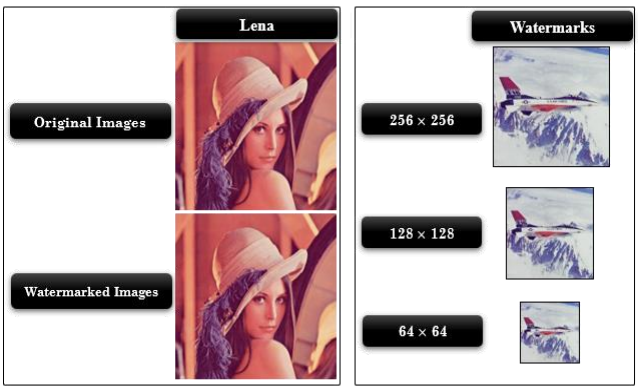


Figure 8. Lean host image and Airplane watermarked Images

Table 2. PSNR evaluation of the WH-SVD-Cb scheme on various watermarked images

Factor (α)	Watermark Size		
	64 × 64	128 × 128	256 × 256
0.005	52.11	52.11	52.11
0.02	52.11	45.62	44.71
0.04	45.61	44.71	37.58
0.06	45.61	40.34	34.44
0.08	44.70	37.56	32.07
0.1	40.69	36.20	30.10
0.12	40.35	34.43	28.52
0.14	39.37	33.18	27.20
0.16	37.55	32.08	26.04
0.18	36.93	30.96	25.02
0.2	36.20	30.11	24.11

Table 3. SSIM evaluation of the WH-SVD-Cb scheme on various watermarked images

Factor (α)	Watermark Size		
	64 × 64	128 × 128	256 × 256
0.005	0.9998	0.9998	0.9998
0.02	0.9998	0.9994	0.9992
0.04	0.9994	0.9992	0.9961
0.06	0.9994	0.9980	0.9921
0.08	0.9992	0.9961	0.9863
0.1	0.9981	0.9946	0.9784
0.12	0.9980	0.9921	0.9691
0.14	0.9974	0.9894	0.9584
0.16	0.9961	0.9863	0.9461
0.18	0.9956	0.9822	0.9324
0.2	0.9946	0.9785	0.9174

Table 4. PSNR and SSIM comparisons of WH-SVD-Cb schema under different sizes of watermarks

Host Image	64 × 64		128 × 128		256 × 256	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lenna	**52.11**	**0.999**	52.11	0.999	45.62	0.999
Pepper	**52.16**	**0.999**	52.16	0.999	45.57	0.999
Baboon	**52.12**	**0.999**	52.12	0.999	45.69	0.998
Barbara	**52.14**	**0.999**	52.14	0.999	45.61	0.997
Yacht	**52.13**	**0.998**	52.13	0.998	45.68	0.996
Village	**52.13**	**0.998**	52.13	0.998	45.61	0.995
Pens	**52.11**	**0.998**	52.11	0.998	45.64	0.995
Monarch	**52.18**	**0.999**	52.18	0.999	45.59	0.998
Girl	**52.12**	**0.998**	52.12	0.998	45.63	0.996
Fruits	**52.12**	**0.999**	52.12	0.999	45.58	0.997
Flowers	**52.16**	**0.999**	52.16	0.999	45.65	0.997
Flower	**52.10**	**0.999**	52.10	0.999	45.56	0.997
Cornfield	**52.12**	**0.999**	52.12	0.999	45.82	0.999
Children's	**52.32**	**0.997**	52.32	0.997	45.79	0.992
Cablecar	**52.14**	**0.998**	52.14	0.998	45.58	0.994
Boat	**52.29**	**0.998**	52.29	0.998	45.62	0.992

Table 5. Comparison of watermarked image quality across different methods

Methods	PSNR (dB)	SSIM
Wang et al. [28]	43.67	0.9771
Ansari et al. [29]	44.02	-
Liu et al. [30]	45.12	09989
Su et al. [31]	50.73	0.9426
Nazir et al. [32]	**52.71**	0.9912
Ansari et al. [33]	**70.73**	0.9923
El-Shafai and Hemdan [34]	**51.75**	0.9923
WH-SVD-Cb	**52.11**	**0.9990**

Table 3 displays the SSIM scores for the WH-SVD-Cb method implemented with watermarks of varying sizes: 256 × 256, 128 × 128, and 64 × 64 with α varying between 0.005 and 0.2. The results show that the WH-SVD-Cb scheme consistently attains high SSIM scores, with values close to 1.

Table 4 shows the obtained results for PSNR and SSIM metrics after applying the WH-SVD-Cb watermarking algorithm to various host images using the Airplane as a watermark image. The distinction between the cover and watermarked one is imperceptible upon visual inspection with the human eye. WH-SVD-Cb shows enhanced performance, achieving an average PSNR of around 52 dB, and SSIM scores close to 0.999. These values indicate that the WH-SVD-Cb achieves high imperceptibility, maintaining high-quality and visually indistinguishable watermarked images.

Table 5 provides a comparison of the imperceptibility of the WH-SVD-Cb scheme with several recent techniques from the literature [28-34]. According to Table 5, the schemes by Wang et al. [28], Ansari et al. [29], Liu et al. [30] and Su and Chen [31] show acceptable PSNR values of 43.67 dB, 44.02 dB, 45.12 dB and 50.73 dB, respectively less than 51 dB due to the embedding technique. The schemes by Nazir et al. [32] achieved average SSIM values of around 0.9912, indicating good image structure preservation but falling short of the WH-SVD-Cb. In the study by El-Shafai and Hemdan [34] performs better, with average PSNR values of 70.73 dB, but not reach the high-quality structure preservation of the WH-SVD-Cb. The performance of the WH-SVD-Cb, especially across images with varying textures and complexities, suggests that the method is significantly maintaining the image quality while embedding the watermark.

The proposed method, WH-SVD-Cb, shows consistent improvements in PSNR across all images with a PSNR of 52.11 dB with a high image structure preservation of 0.999, highlighting its effectiveness in refining the watermarking process. Consequently, the watermarked image retains a high level of quality, making it suitable for practical applications. The performance of the WH-SVD-Cb, especially across images with varying textures and complexities, suggests that the method is highly robust in preserving the structural quality of watermarked images, with average SSIM values of 0.999.

We can conclude that WH-SVD-Cb demonstrates the highest PSNR values, slightly improving upon its predecessors' methods [28-31].

5.2 Robustness evaluation and comparison

Once imperceptibility is achieved, it is vital to ensure the watermark's resistance against image degradation. In these experiments, the watermarked images undergo various attacks, comprising regular and irregular attacks (see Table 6) attacks to assess the scheme's performance under diverse conditions. Regular attacks evaluate the proposed method by altering the watermarked image at a precisely controlled rate between 10% and 80% with 10% steps. In contrast, the irregular attack involves real-life scenarios of images, consisting of multiple types of attacks. Table 6 shows that irregular attacks include cropping, compression, normal, histogram equalization, and rescaling.

In filter-based attacks, techniques including the median filter, Gaussian filter, and average filter are applied to assess the impact of various filtering approaches. Noise attacks mimic typical image degradations by adding degradations like Gaussian noise at varying intensities to evaluate the system's resilience to interference.

Compression attacks use both JPEG and JPEG2000 techniques, with a compression ratio of 50 for JPEG and a compression ratio of 12 for JPEG2000, mimicking scenarios where watermarked images undergo lossy compression during storage or transmission.

Rescaling attacks test adaptability to size changes by applying image reduction and enlargement with scaling factors of 0.25 and 4, respectively. Motion blur is simulated using parameters Theta = 4 and Len = 7 to reflect dynamic environment conditions. Sharpening attacks, with a threshold of 0.8, evaluate the watermark's integrity under image enhancement processes, while rotation attacks at 2 degrees simulate the impact of angular transformations.

This comprehensive evaluation, which includes a wide range of specified attacks, provides a comprehensive evaluation of the proposed technique's efficiency and its security contexts. The Normalized Coefficient (NC) is a metric used to assess the robustness of a watermarking system by measuring the similarity between the original watermark W and the extracted one W^*. The formula for NC is as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{i,j*}W_{i,j}^{*}\right)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{i,j}\right)}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{i,j}^{*}\right)}} \quad (36)$$

where, W is the original watermark image and W^* is the extracted watermark image. M and N represent the width and height of W and W^*. A system is considered robust if the NC values are nearly equal to 1.

The researcher has applied various attack to assess robustness in terms of NC. The evaluation of the WH-SVD-Cb is presented in Table 7 for attacked watermarks for sizes 64×64, 128×128 and 256×256. For the 128×128 watermark, the proposed method showed strong resistance across all attacks, achieving high NC values near 1.

Table 6. Applied attacks on watermarked images

Types of Attack	List of Attacks
Filter	Median filter (3×3)
	Gaussian filter (3×3)
	Average filter (3×3)
Noise	Gaussian noise (0.001)
	Salt & Peppers noise (0.001)
	Speckle noise (0.001)
Compression	JPEG compression (QF = 50)
	JPEG2000 compression (CR = 12)
HE	Histogram Equalization
Motion blur	Motion blur (Theta = 4, Len = 7)
Sharpening	Sharpening (0.8)
Rescaling	Rescaling (0.25)
	Rescaling (4)
Rotation	Rotation (+10°)
	Rotation (-10°)

Table 7. NC evaluation of the WH-SVD-Cb scheme against various common attacks

Applied Attacks	Watermark Size		
	64 × 64	128 × 128	256 × 256
Median Filter 3×3	0.9999	0.9999	0.9999
Gaussian Filter	0.9999	0.9999	0.9999
Average Filter 3×3	0.9999	0.9999	0.9999
Gaussian Noise (0.001)	0.9999	0.9999	0.9999
Salt & Peppers	0.9999	0.9999	0.9999
Speckle Noise (0.001)	0.9999	0.9999	0.9999
JPEG Compression (50)	0.9999	0.9999	0.9999
JPEG Compression (12)	0.9999	0.9999	0.9999
Histogram Equalizer	0.9999	0.9999	0.9999
Motion Blur (4-7)	0.9999	0.9999	0.9999
Sharpening (0.8)	0.9999	0.9999	0.9999
Rescaling (0.25)	0.9999	0.9999	0.9999
Rescaling (4)	0.9999	0.9999	0.9999
Rotation (+10°)	0.9999	0.9999	0.9999
Rotation (-10°)	0.9999	0.9999	0.9999

Figure 9 also provides examples of the watermark's visual clarity after following JPEG compression attack at rate of 50 and 12, along with 10° rotation attack, and Gaussian noise using the airplane image as a test case. As visualized in Figure 9, the WH-SVD-Cb scheme achieves high NC values close to 1, reflecting its robustness. Moreover, it delivers good SSIM values and acceptable PSNR levels. These results can be explained by the encryption process integrated in the proposed method, which includes Arnold chaotic map and the strategic embedding of bits within the Cb component.

Table 8 presents the evaluation of the PSNR, SSIM, and NC metrics for the WH-SVD-Cb method during both the embedding and extraction stages, with different scaling factors (α). The results demonstrate the fidelity of the watermarked images using the WH-SVD-Cb method to maintain. Specifically, embedding within the chaotic domain of the Arnold map ensures optimal fidelity, as demonstrated by the values presented in Table 8.

As the scaling factor increases within the range of 0.01 to 1, PSNR values show a gradual decrease, whereas SSIM values

remain nearly constant throughout this range. A notable strength of this method is the stability of NC values across varying scaling factors during the embedding and extraction stages.

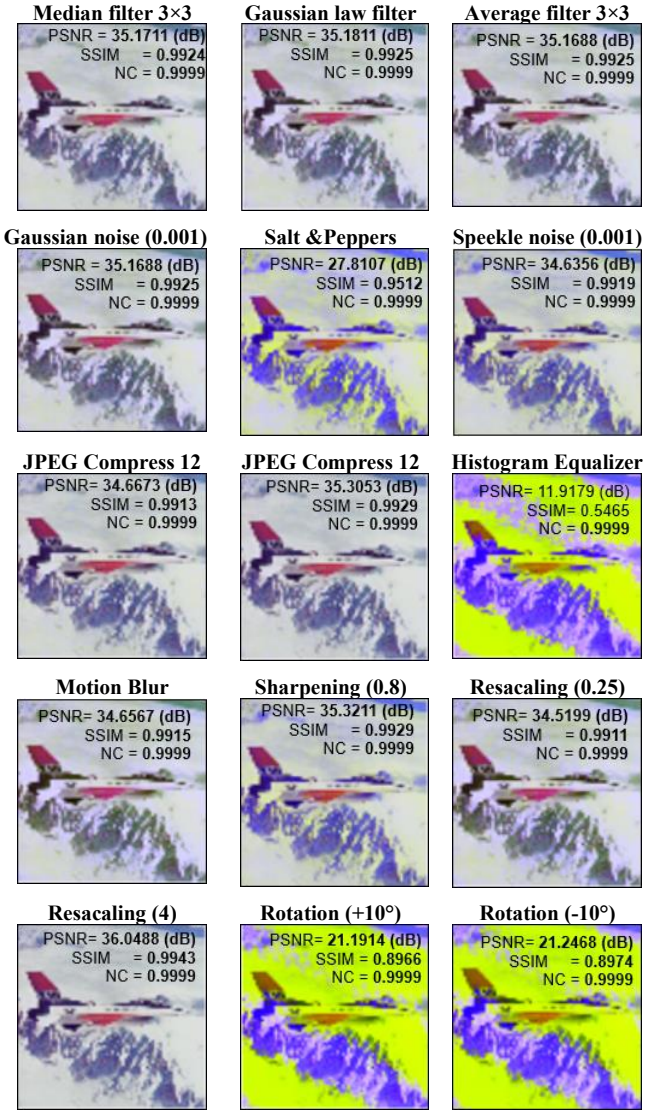


Figure 9. Robustness evaluation against different attacks

In addition, Table 8 highlights the resistance of the suggested approach, which leverages the Cb channel for embedding through transformation and encryption techniques. The findings reveal that the proposed scheme effectively resists tampering, as indicated by NC values consistently approaching 1. However, it is observed that for large-size images, higher values of the factor α can influence imperceptibility.

Figures 10 and 11 show the relationships between the scaling factor and the PSNR and SSIM, respectively. These metrics provided clear and objective indicators of image quality and demonstrated the effectiveness of the extraction process. The PSNR lowers as the scaling factor rises, within the interval of 0.005 to 0.02. In contrast, SSIM remains almost constant within the same range. Based on these observations, initial values for t are recommended as t1=0.01, for both PSNR and SSIM.

For the resistance against intended alterations such as compression (JPEG QF = 90 and H.264 QP = 16), noising (Gaussian 1% and S&P 1%), rotation (10°), and filtering (average and median 3×3), Figure 12 demonstrates the enhanced effectiveness of the suggested method regarding NC values in relation to all evaluated attacks.

Table 8. Comparative analysis for robustness under different scaling factors and NC values

Factor (α)	Attacks	PSNR	SSIM	NC
0.01	No Attack	52.1168	0.9998	0.9999
	Median filter	41.3663	0.9976	0.9999
	Gaussian filter	41.4009	0.9976	0.9999
	Sharpening	42.9382	0.9984	0.9999
	JPEG compression	36.6596	0.9965	0.9999
	JPEG2000 compression	42.8022	0.9983	0.9999
	Average filter	41.3532	0.9976	0.9999
0.05	No Attack	45.6132	0.9993	0.9999
	Median filter	40.2655	0.9971	0.9999
	Gaussian filter	40.2788	0.9972	0.9999
	Sharpening	41.4103	0.9979	0.9999
	JPEG compression	36.8801	0.9960	0.9999
	JPEG2000 compression	41.1834	0.9978	0.9999
	Average filter	40.2411	0.9971	0.9999
0.1	No Attack	40.6940	0.9980	0.9999
	Median filter	38.1950	0.9958	0.9999
	Gaussian filter	38.2103	0.9959	0.9999
	Sharpening	38.8320	0.9966	0.9999
	JPEG compression	37.2641	0.9957	0.9999
	JPEG2000 compression	38.6623	0.9964	0.9999
	Average filter	38.1863	0.9959	0.9999
0.5	No Attack	28.1964	0.9667	0.9999
	Median filter	28.0161	0.9643	0.9999
	Gaussian filter	28.0161	0.9645	0.9999
	Sharpening	28.0616	0.9654	0.9999
	JPEG compression	27.9043	0.9631	0.9999
	JPEG2000 compression	28.0127	0.9674	0.9999
	Average filter	28.0135	0.9654	0.9999
1	No Attack	22.1800	0.8752	0.9999
	Median filter	22.1368	0.8727	0.9999
	Gaussian filter	22.1364	0.8729	0.9999
	Sharpening	22.1424	0.8745	0.9999
	JPEG compression	22.0994	0.8715	0.9999
	JPEG2000 compression	22.1225	0.8729	0.9999
	Average filter	22.1356	0.8729	0.9999

A comparative analysis of four schemes (YCb, Y [37], YCbCr [38], Cb) was performed under identical conditions using the Lena image. The evaluation focused on NC values, evaluated with three watermark images of sizes 256×256, 128×128, and 64×64. The summarized results in Table 9 indicate that the Cb scheme consistently achieves NC values close to 1 across all image sizes, remaining within the computational range of [0.05, 0.2]. These findings highlight the Cb scheme not only outperforms the other schemes but also exhibits exceptional robustness for all three watermark image sizes.

Table 10 displays the NC comparison between WH-SVD-Cb and recent watermarking techniques [28-34]. We notice that WH-SVD-Cb approach gives good robustness through the obtained scores NC and the watermarking is established in the Cb channel using DWT, HD, and SVD. This means that WH-SVD-Cb effectively preserves high robustness and perfect scores with color images. Figure 13 shows the NC values after

applying many attacks to Lenna host image. For the watermark of size 64 × 64, results show that the WH-SVD-Cb schema outperforms all the other schemas.

5.2.1 Evaluation of robustness to JPEG compression attacks

The proposed method's robustness was assessed under varying Quality Factors (QFs) during JPEG compression, ranging from 90 to 10 in increments of 10. A lower QF means stronger image compression. Remarkably, even at a QF of 10, our proposed method achieved excellent results, with all NCs close to 1. This consistency was observed for watermarks of three different sizes: 64×64, 128×128 and 256×256. Compared to other schemes such as Y [37], YCbCr [38], and YCb, the proposed scheme clearly outperforms the others. Detailed results can be found in Figure 13(a).

Figure 13(b) provides comprehensive experiments that extended to JPEG2000 compression with the ratios varied from 4 to 36. Higher CR values mean stronger image compression. Remarkably, even at a CR of 36, the lowest NCs for the three watermarks are close to 1. This consistency was observed across watermarks of three different sizes: 64×64, 128×128 and 256×256. Compared to other schemes, including Y [37], YCbCr [38] and YCb, the proposed scheme outperforms the others.

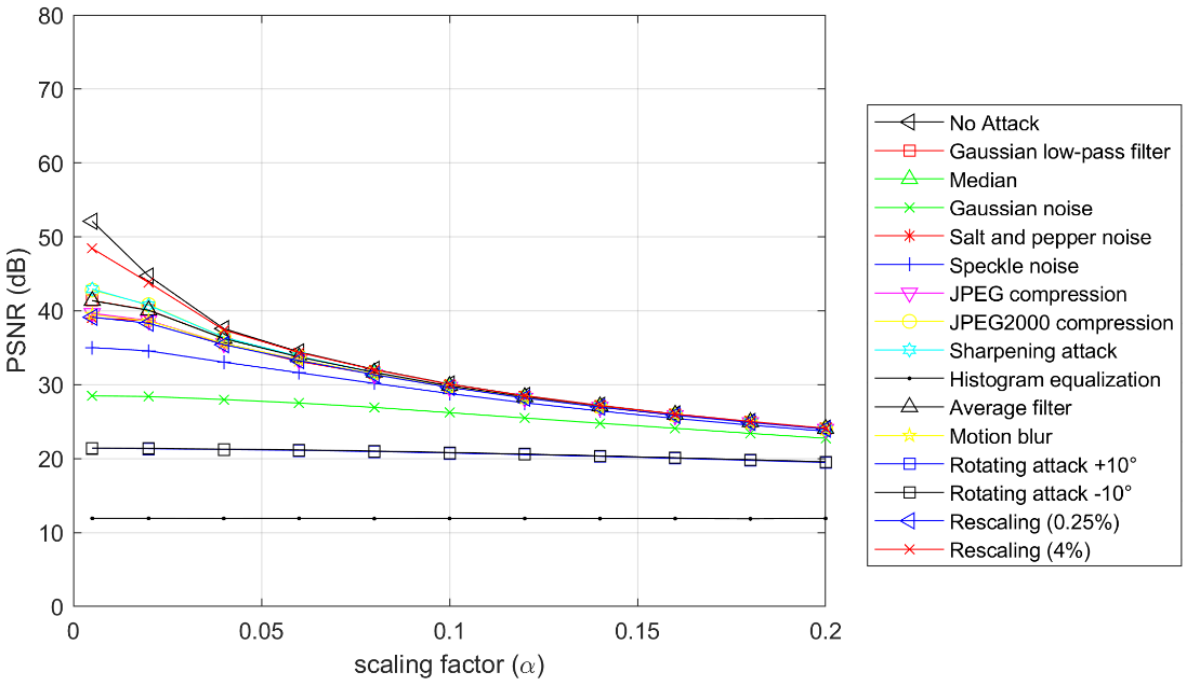


Figure 10. Comparative analysis for imperceptibility in terms of PSNR under different scaling factors

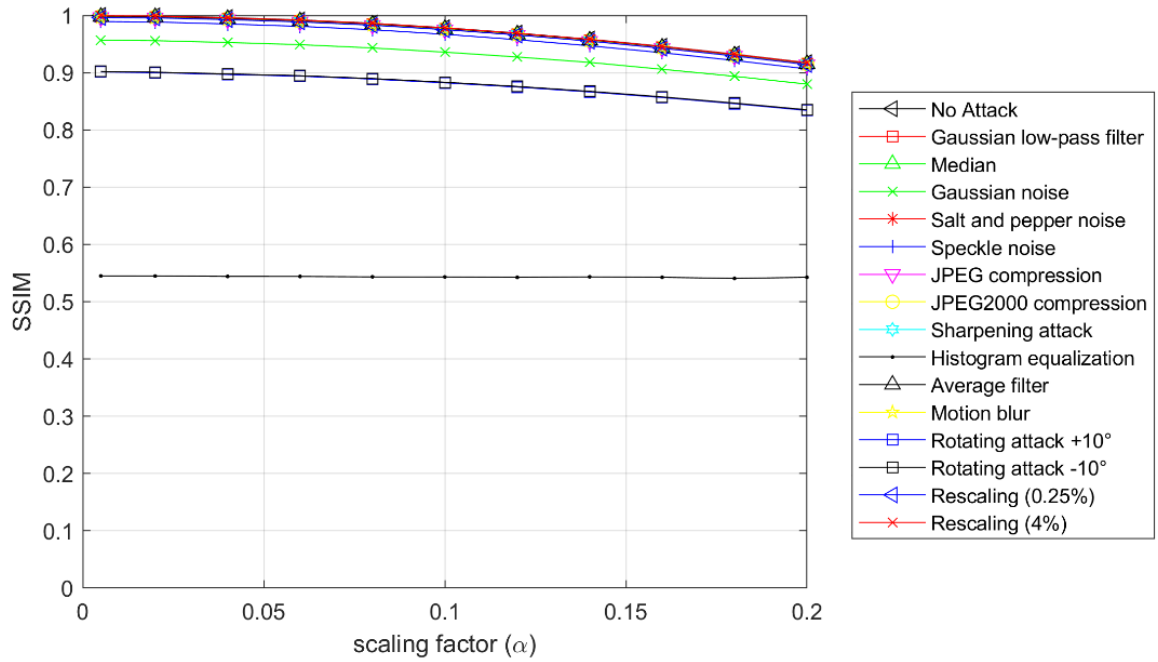


Figure 11. Comparative analysis for imperceptibility in terms of SSIM under different scaling factors

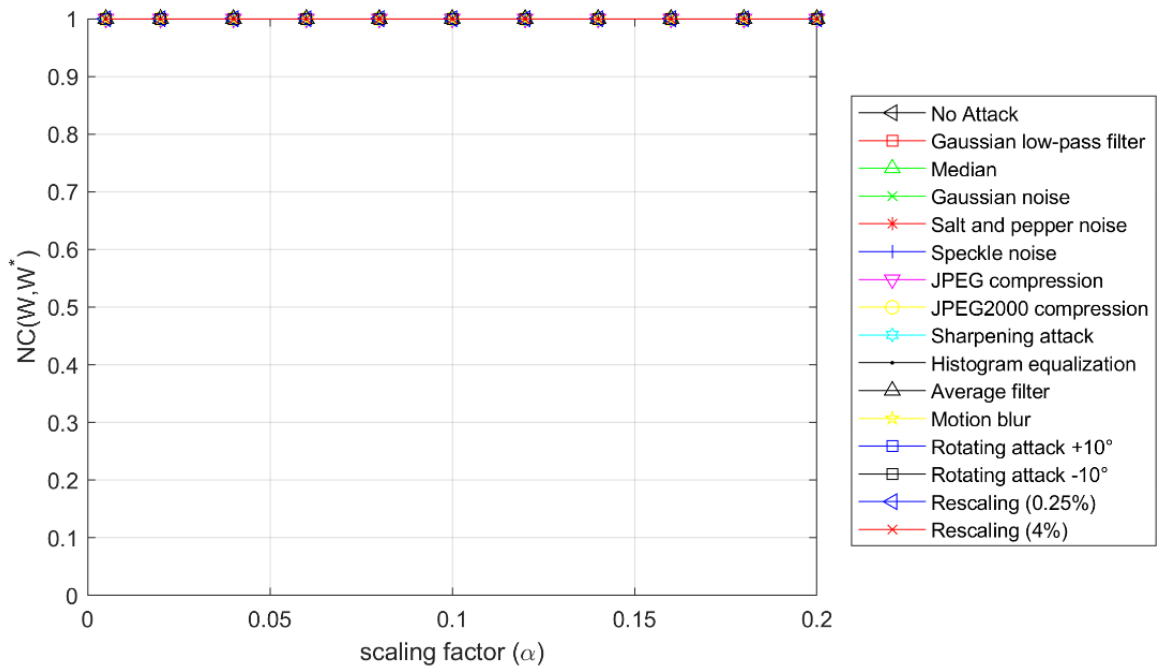


Figure 12. Comparative analysis for robustness in terms of NC under different scaling factors

Table 9. Evaluation of robustness across different scaling factors utilizing various embedding channels

α	256 × 256				128×128				64 × 64			
	YCbCr	YCb	Y	Cb	YCbCr	YCb	Y	α	YCbCr	YCb	Y	Cb
0.005	0.3889	0.9452	0.9452	0.9999	-	0.1298	0.1298	0.9999	-	0.1300	0.1300	0.9999
0.02	0.9938	0.9997	0.9997	0.9999	0.9782	0.9957	0.9957	0.9999	0.3523	0.9346	0.9346	0.9999
0.04	0.9969	0.9999	0.9999	0.9999	0.9938	0.9997	0.9997	0.9999	0.9789	0.9951	0.9951	0.9999
0.06	0.9999	0.9999	0.9999	0.9999	0.9983	0.9999	0.9999	0.9999	0.9970	0.9986	0.9986	0.9999
0.08	0.9998	0.9999	0.9999	0.9999	0.9968	0.9999	0.9999	0.9999	0.9938	0.9996	0.9996	0.9999
0.1	0.9999	0.9999	0.9999	0.9999	0.9990	0.9999	0.9999	0.9999	0.9963	0.9998	0.9998	0.9999
0.12	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9982	0.9998	0.9998	0.9999
0.14	0.9999	0.9999	0.9999	0.9999	0.9996	0.9999	0.9999	0.9999	0.9981	0.9999	0.9999	0.9999
0.16	0.9999	0.9999	0.9999	0.9999	0.9998	0.9999	0.9999	0.9999	0.9966	0.9999	0.9999	0.9999
0.18	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9995	0.9999	0.9999	0.9999
0.2	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9989	0.9999	0.9999	0.9999

5.2.2 Evaluation of robustness to Gaussian and median filter attacks

Figures 13(c) and 13(d) illustrate the robustness of the system against Gaussian and median filters, where parameters such as window size and standard deviation were systematically adjusted. According to these figures, the WH-SVD-Cb consistently improves over previous methods due to its enhanced block mapping technique. This consistency was observed across watermarks of three different sizes: 64×64, 128×128 and 256×256. Compared to other schemes such as Y [37], YCbCr [38], and YCb, the suggested method clearly outperforms the other schemes.

Table 10. NC comparison of the attacked watermarks

Attacks	[28]	[29]	[30]	[31]	[32]	[33]	[34]	WH-SVD-Cb
Salt & pepper noise (v=0.001)	0.995	0.890	0.998	-	0.9996	0.893	-	0.9999
Gaussian noise (v=0.005)	0.995	0.890	0.998	-	0.9996	0.879	0.994	0.9999
Rotation 2°	0.982	-	-	0.983	0.9999	0.934	0.998	0.9999
Rotation 5°	-	-	0.978	-	1	-	-	0.9999
JPEG compression QF=50	-	-	0.984	-	1	0.920	0.980	0.9999
Scaling (zoom out=0.25, zoom-in=4)	0.995	0.957	0.999	0.957	1	-	-	0.9999
Speckle noise (var=0.001)	0.898	0.913	0.988	0.913	1	0.925	-	0.9999
Gaussian filter 3×3	0.994	-	0.994	-	1	0.975	-	0.9999
Median filter 3×3	0.991	0.986	0.992	0.966	1	0.960	-	0.9999
Average filter 3×3	0.989	0.907	0.989	0.907	1	0.873	-	0.9999
Sharpening	-	-	0.975		1	0.970	-	0.9999
Histogram Equalization	0.947	0.997	0.948	0.997	1	0.864	-	0.9999

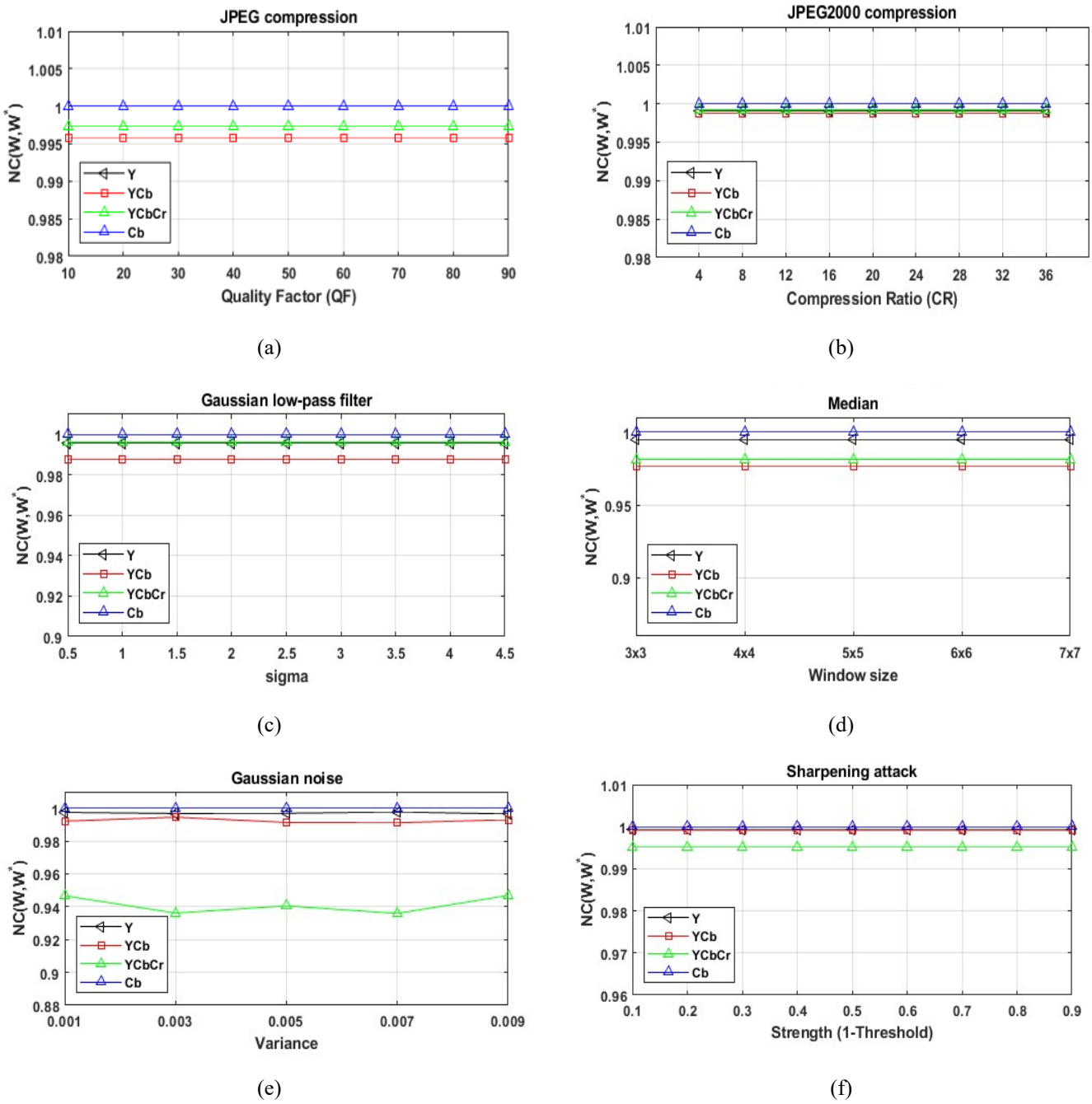


Figure 13. NC comparison of the attacked images: (a) JPEG Compression, (b) JPEG2000 Compression, (c) Gaussian Filter, (d) Median Filter, (e) Gaussian Noise, and (f) Sharpening

5.2.3 Evaluation of robustness to Gaussian noise and sharpening attacks

Gaussian noise and sharpening attacks were explored in Figures 13(e) and 13(f), with varying variance and threshold settings. The results indicated that NCs for both Gaussian noise and sharpening were effectively equal to 1. Compared to other schemes such as Y [37], YCbCr [38], and YCb, the proposed method clearly outperforms the others.

5.3 Complexity evaluation and comparison

Table 11 evaluates the algorithm complexity of the WH-SVD-Cb. The complexity of each key step in the WH-SVD-Cb scheme is described as follows:

• DWT: The complexity of the DWT is $O(NlogN)$), where N represents the image size. This step is often computationally demanding due to the multi-level transformations involved.

• HD: The computational cost of HD is generally $O(N)$, as it involves analyzing and decomposing the histogram, assuming each pixel is processed.

• SVD (Singular Value Decomposition): The computational cost of SVD is $O(N^3)$. However, optimizations using methods like Lanczos or randomized SVD can reduce this computational time.

• Arnold Map: The Arnold Map, used for scrambling image pixels, typically has a complexity of $O(N)$ since each pixel is transformed based on predefined rules.

The total complexity is resulted in a worst-case complexity of $O(N^3)$.

The computation time of the WH-SVD-Cb is determined by assessing the time required for method execution. Factors such as hardware and software environments, algorithmic complexity, image size may impact execution time.

Table 11. Complexity cost of the proposed method

Watermarking Method	Complexity
DWT	$O(NlogN)$
HD	$O(N)$
SVD	$O(N^3)$
Arnold Map	$O(N)$
WH-SVD-Cb	$O(N^3)$

Table 12. Comparison of watermark embedding computation time under different image sizes (in seconds)

Watermarking Method	64 × 64	128 × 128	256 × 256
DWT	0.0255	0.0251	0.0232
HD	0.0006	0.0024	0.0106
SVD	0.0016	0.0068	0.0231
Arnold Map	0.0673	0.0952	0.2675
Total	0.0953	0.1297	0.3245

Table 13. Comparison of watermark embedding computation time in seconds

Watermarking Method	Watermark Embedding (s)	Watermark Extraction (s)	Total (s)
Su and Chen [31]	0.5663	0.3205	0.8868
Nazir et al. [32]	0.3958	0.4721	0.8668
Ansari et al. [33]	0.2863	-	0.3234
El-Shafai and Hemdan [34]	1.2530	0.9470	1.4476
WH-SVD-Cb	0.1832	0.0442	0.2274

Table 12 compares the computation time for watermark embedding across different image sizes. image size. According to Table 12, the computational time increases proportionally with image size and is further influenced by image size and the application of transformation and encryption techniques.

Table 13 presents a comparison of processing times for embedding and extraction stages between the proposed WH-SVD-Cb scheme and other methods [31-34]. By embedding the watermark exclusively in the Cb channel, the WH-SVD-Cb scheme reduces execution time compared to other methods. Table 13 demonstrates that the WH-SVD-Cb technique is well-suited for real-time applications with an execution time of 0.2274 s. However, as the watermark size increases, the image embedding process for the selected blocks takes more embedding time. Despite this, the WH-SVD-Cb scheme consistently produces the shortest extraction times and maintains better image quality than the other techniques.

5.4 Lessons learned and limitations

The findings of the proposed approach demonstrated superior visual image quality and enhanced resistance compared to several other contemporary watermarking methods. The results demonstrate that the careful selection of components from an optimal representation space, such as the HSV model, can have a significant impact. Ultimately, the Cb channel of the YCbCr space was chosen for processing full-color images. We have demonstrated that the WH-SVD-Cb scheme outperforms existing watermarking methods, as evidenced by comparisons with prior studies [28-34]. In other words, selecting a good component as blue in frequency domain blind watermarking could lead to optimal performance results of WH-SVD-Cb watermarking schema.

6. CONCLUSION

This study examined the DWT coefficients of transformed images in the YCbCr color space, integrated HD and SVD transformations, and encoded with Arnold's chaotic map, in response to image quality and reliability. The present research focused on the Cb channel, DWT transformation and chaotic sequences to embed the watermark bits through a novel method referred to as WH-SVD-Cb. The WH-SVD-Cb shows significant improvements with an imperceptibility of over 52 dB. Furthermore, the method exhibited high robustness, with NC values close to 1. The technique relies on intelligent CB components for embedding texture information. Future studies focus on boosting embedding capacity and improving resilience to geometric and signal processing issues, particularly for medical color images to enable real-time protection of patient information and medical data.

ACKNOWLEDGMENT

This work was support by the Qassim University.

REFERENCES

[1] Hussan, M., Parah, S.A., Qureshi, G.J. (2024). Reversible data hiding framework with content authentication capability for e-health. Multimedia Tools and Applications, 83(12): 35335-35353. https://doi.org/10.1007/s11042-023-17019-9

[2] Xian, Y., Ma, R., Liu, P., Zhou, L. (2023). Image encryption scheme based on new 1D chaotic system and blockchain. In International Workshop on Digital Watermarking, pp. 3-17. https://doi.org/10.1007/978-981-97-2585-4_1

[3] Su, Q., Niu, Y., Zou, H., Zhao, Y., Yao, T.A. (2014). Blind double-color image watermarking algorithm based on QR decomposition. Multimedia Tools and Applications, 72: 987-1009. https://doi.org/10.1007/s11042-013-1653-z

[4] Kumar, C., Singh, A.K., Kumar, P. (2018). A recent survey on image watermarking techniques and their application in e-governance. Multimedia Tools and Applications, 77(3): 3597-3622. https://doi.org/10.1007/s11042-017-5222-8

[5] Nikolaidis, N., Pitas, I. (1998). Robust image watermarking in the spatial domain. Signal Processing, 66(3): 385-403. https://doi.org/10.1016/S0165-1684(98)00017-6

[6] Singh, L., Singh, A.K., Singh, P.K. (2020). Secure data hiding techniques: A survey. Multimedia Tools and Applications, 79(23): 15901-15921. https://doi.org/10.1007/s11042-018-6407-5

[7] Kumar, S., Singh, B.K., Yadav, M. (2020). A recent survey on multimedia and database watermarking. Multimedia Tools and Applications, 79(27): 20149-20197. https://doi.org/10.1007/s11042-020-08881-y

[8] Thakur, S., Singh, A.K., Ghrera, S.P., Dave, M. (2018). Watermarking techniques and its applications in tele-health: A technical survey. In Cryptographic and Information Security Approaches for Images and Videos by S. Ramakrishnan Chapter -17, pp. 467-511. https://doi.org/10.1201/9780429435461.

[9] Abraham, J., Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences, 31(1): 125-133. https://doi.org/10.1016/j.jksuci.2016.12.004
[10] Liu, Y., Tang, S., Liu, R., Zhang, L., Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications, 97: 95-105. https://doi.org/10.1016/j.eswa.2017.12.003
[11] Vaidya, P., PVSSR, C.M. (2017). A robust semi-blind watermarking for color images based on multiple decompositions. Multimedia Tools and Applications, 76(24): 25623-25656. https://doi.org/10.1007/s11042-017-4355-0
[12] Ernawan, F., Aminuddin, A., Bakar, S.A. (2023). A blind recovery technique with integer wavelet transforms in image watermarking. Engineering Science and Technology, an International Journal, 48: 101586. https://doi.org/10.1016/j.jestch.2023.101586
[13] Liu, S., Pan, Z., Song, H. (2017). Digital image watermarking method based on DCT and fractal encoding. IET Image Processing, 11(10): 815-821. https://doi.org/10.1049/iet-ipr.2016.0862
[14] Savakar, D.G., Ghuli, A. (2019). Robust invisible digital image watermarking using hybrid scheme. Arabian Journal for Science and Engineering, 44(4): 3995-4008. https://doi.org/10.1007/s13369-019-03751-8
[15] Su, Q., Liu, D., Yuan, Z., Wang, G., Zhang, X., Chen, B., Yao, T. (2020). New rapid and robust color image watermarking technique in spatial domain. IEEE Access, 7: 30398-30409. https://doi.org/10.1109/ACCESS.2019.2895062
[16] Kumar, C., Singh, A.K., Kumar, P. (2020) Improved wavelet-based image watermarking through SPIHT. Multimedia Tools and Applications, 79(15): 11069-11082. https://doi.org/10.1007/s11042-018-6177-0
[17] Fares, K., Amine, K., Salah, E. (2020). A robust blind color image watermarking based on Fourier transform domain. Optik, 208: 164562. https://doi.org/10.1016/j.ijleo.2020.164562
[18] Anand, A., Singh, A.K. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152: 72-80. https://doi.org/10.1016/j.comcom.2020.01.038
[19] Mishra, A., Rajpal, A., Bala, R. (2018). Bi-directional extreme learning machine for semi-blind watermarking of compressed images. Journal of Information Security and Applications, 38: 71-84. https://doi.org/10.1016/j.jisa.2017.11.008
[20] Ambadekar, S.P., Jain, J., Khanapuri, J. (2019). Digital image watermarking through encryption and DWT for copyright protection. In Recent Trends in Signal and Image Processing, pp. 187-195. https://doi.org/10.1007/978-981-10-8863-6_19
[21] Singh, P., Devi, K.J., Thakkar, H.K., Santamaría, J. (2021) Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness. Entropy, 23(12): 1650. https://doi.org/10.3390/e23121650
[22] Boujerfaoui, S., Riad, R., Douzi, H., Ros, F., Harba, R. (2022). Image watermarking between conventional and learning-based techniques: A literature review. Electronics, 12(1): 74. https://doi.org/10.3390/electronics12010074
[23] Solak, S., Abdirashid, A.M., Adjevi, A., Sahu, A.K. (2024). Robust data hiding method based on frequency coefficient variance in repetitive compression. Engineering Science and Technology, an International Journal, 56: 101756. https://doi.org/10.1016/j.jestch.2024.101756
[24] Sahu, A.K., Swain, G. (2022). High fidelity based reversible data hiding using modified LSB matching and pixel difference. Journal of King Saud University-Computer and Information Sciences, 34(4): 1395-1409. https://doi.org/10.1016/j.jksuci.2019.07.004
[25] Dhar, S., Sahu, A.K. (2024). Digital to quantum watermarking: A journey from past to present and into the future. Computer Science Review, 54: 100679. https://doi.org/10.1016/j.cosrev.2024.100679
[26] Lakrissi, Y., Saaidi, A., Essahlaoui, A. (2018). Novel dynamic color image watermarking based on DWT-SVD and the human visual system. Multimedia Tools and Applications, 77: 13531-13555. https://doi.org/10.1007/s11042-017-4974-5.
[27] Sajeer, M., Mishra, A. (2023). A robust and secured fusion based hybrid medical image watermarking approach using RDWT-DWT-MSVD with Hyperchaotic system-Fibonacci Q Matrix encryption. Multimedia Tools and Applications, 82(24): 37479-37501. https://doi.org/10.1007/s11042-023-15001-z
[28] Wang, J., Wan, W.B., Li, X.X., De Sun, J., Zhang, H.X. (2020). Color image watermarking based on orientation diversity and color complexity. Expert Systems with Applications, 140: 112868. https://doi.org/10.1016/j.eswa.2019.112868
[29] Ansari, I.A., Pant, M., Ahn, C.W. (2016). Robust and false positive free watermarking in IWT domain using SVD and ABC. Engineering Applications of Artificial Intelligence, 49: 114-125. https://doi.org/10.1016/j.engappai.2015.12.004
[30] Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7: 80849-80860. https://doi.org/10.1109/ACCESS.2019.2915596
[31] Su, Q., Chen, B. (2017). A novel blind color image watermarking using upper Hessenberg matrix. AEU-International Journal of Electronics and Communications, 78: 64-71. https://doi.org/10.1016/j.aeue.2017.05.025
[32] Nazir, H., Ullah, M.S., Qadri, S.S., Arshad, H., Husnain, M., Razzaq, A., Nawaz, S.A. (2023). Protection-enhanced watermarking scheme combined with non-linear systems. IEEE Access, 11: 33725-33740. https://doi.org/10.1109/ACCESS.2023.3263492
[33] Ansari, I.A., Pant, M., Ahn, C.W. (2016). ABC optimized secured image watermarking scheme to find out the rightful ownership. Optik, 127(14): 5711-5721. https://doi.org/10.1016/j.ijleo.2016.03.070.
[34] El-Shafai, W., Hemdan, E.E. (2023). Robust and efficient multi-level security framework for color medical images in telehealthcare services. Journal of Ambient Intelligence and Humanized Computing, 14: 3675-3690. https://doi.org/10.1007/s12652-021-03494-1
[35] Soualmi, A., Alti, A., Laouamer, L. (2022). An imperceptible watermarking scheme for medical image tamper detection. International Journal of Information Security and Privacy (IJISP), 16(1): 1-18.

https://doi.org/10.4018/IJISP.2022010102
[36] The USC-SIPI Image Database. https://sipi.usc.edu/database, accessed on 23 April 2024.
[37] Sharma, S., Sharma, H., Sharma, J.B. (2019). An adaptive color image watermarking using RDWT-SVD and artificial bee colony-based quality metric strength factor optimization. Applied Soft Computing, 84: 105696. https://doi.org/10.1016/j.asoc.2019.105696
[38] Sharma, N., Shukla, A. (2021). A hybrid technique of blind color watermarking employing RDWT and SVD. International Journal of Engineering Research & Technology (IJERT), 10(10): IJERTV10IS100078. https://doi.org/10.17577/IJERTV10IS100078