# An Optimized Color Image Watermarking Scheme based on HD and SVD in DWT Domain

**Mourad Sahir**
Department of Electronics, Faculty of Technology, LIS Laboratory, University of Setif-1, Algeria
mourad.sahir@univ-setif.dz

**Tewfik Bekkouche**
Department of Electromechanics, Faculty of Technology, ETA Laboratory, University of BBA, Algeria
toufik.bekkouche@univ-bba.dz (corresponding author)

**Fairouz Belilita**
Department of Physics, Faculty of Sciences, LIS Laboratory, University of Setif-1, Algeria
fairouz.amardjia@univ-setif.dz

**Nourredine Amardjia**
Department of Electronics, Faculty of Technology, LIS Laboratory, University of Setif-1, Algeria
amardjianour@univ-setif.dz

*Received: 4 November 2024 | Revised: 17 December 2024 and 25 January 2025 | Accepted: 10 February 2025*

 *DOI: https://doi.org/10.48084/etasr.9504*

**ABSTRACT**

**Digital watermarking is considered a trustworthy strategy for proving ownership of valuable digital files such as audio, image, and video documents. Most of the prevailing image watermarking systems embed grayscale or binary image watermarks, while only a few use color images as watermarks. In this paper, we develop a secure, imperceptible, and robust optimized semi-blind color image watermarking technique that uses color images as watermarks. It is based on Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD) in the Discrete Wavelet Transform (DWT) domain. First, the color host image and color watermark image in RGB space are converted to YCbCr space, and then the watermark data are embedded into the luminance component (Y) of the host image. In this work, the principal component of the watermark's luminance (Y) is implanted into the associated singular value of the host image with an appropriate scaling factor that optimizes the robustness-imperceptibility tradeoff. The Artificial Bee Colony (ABC) algorithm is used to find the appropriate scaling factors. To further enhance the security, the Arnold transformation is used to scramble the Y channel of the watermark before it is injected into the host image. As demonstrated by the Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) metrics, the proposed scheme exhibits high invisibility and is robust to most image processing manipulations, geometric operations, and combinational attacks. Compared to various existing color image watermarking schemes that use color images as watermarks, it shows higher imperceptibility and robustness.**

***Keywords-color image watermark; Hessenberg decomposition; singular value decomposition; discrete wavelet transform; artificial bee colony***

## I. INTRODUCTION

Due to the widespread and rapid distribution of large amounts of digital files such as audio, images and video over high-speed communication systems, there is a strong need to verify their originality and copyright ownership. This can be achieved by digital watermarking, which is a widely used technique for copyright protection of digital information [1]. Digital image watermarking refers to the embedding of hidden data recognized as a watermark or signature, into a host image, also known as a cover, using confidential keys. The signature can be recovered later to prove the ownership of the creator [2]. An appropriate watermarking technique must provide some key features. These features consist of high imperceptibility or invisibility, which means that there is no perceived change between the original and the watermarked content, high

robustness or resilience, which means that the watermark should be resistant to intentional and unintentional manipulations, and a useful capacity, which indicates the amount of information present in the watermark [3].

Depending on what elements are involved during the watermark extraction stage, digital image watermarking methods are categorized into non-blind, semi-blind, and blind schemes. A non-blind scheme requires access to the original cover, the initial watermark, and the secret keys [4]. A semi-blind scheme requires the initial watermark or some side information about it and the private keys [5, 6]. A blind scheme requires only the secret keys [7]. Generally, digital image watermarking techniques are classified into pixel-based domain and spectrum-based domain approaches. In pixel-based domain approaches, the watermark is embedded directly into the pixel locations [8]. This has many advantages such as better perceptual quality, less computation, and high embedding capacity, but less robustness. It's generally adapted for authentication applications. In a spectrum-based domain approach, a transform function is performed on the original cover image to implant the watermark within the terms, and then the inverse transform is applied to recover the implanted watermark. The most commonly used methods are based on the Discrete Cosine Transform (DCT) [9], the Discrete Fourier Transform (DFT) [10], the Discrete Wavelet Transform (DWT) [11, 12], and Singular Value Decomposition (SVD) [13]. The transform techniques provide high imperceptibility and, most importantly, are more robust than the spatial techniques. Many researchers have explored SVD-based watermarking in various domains, such as DCT, DFT, and DWT. Watermarking in a transformed domain mainly improves the robustness. In our work, we use the Hessenberg Decomposition (HD) [14] and SVD in the DWT domain. The HD allows to significantly increase the imperceptibility factor.

In recent works, color image watermarking has emerged as one of the challenging research problems. A major problem is how to construct a watermark pattern that inserts a color watermark into a color image, since most of the existing watermarking schemes use grayscale images or binary images as watermarks. Also, as mentioned earlier, imperceptibility and robustness are two essential performance characteristics in image watermarking, and finding the right balance between them is a challenging problem. One way to achieve this is to use a biologically derived algorithm such as the Artificial Bee Colony (ABC) [15]. In the present work, our main objective is to develop a new watermarking scheme that inserts a color image watermark into a host color image and that can provide a substantial imperceptibility, substantial embedding capacity, and most importantly, high robustness against a large fraction of detected attacks. The main contributions of our proposed scheme are:

- The ABC algorithm is applied based on predefined conditions, the target PSNR and robustness, to systematically determine the correct values for the scaling coefficients, as these coefficients depend on the host image. The proposed watermarking scheme provides large embedding capacity, excellent watermark imperceptibility, and enhanced resilience against common image processing manipulations, geometric, and combined attacks, outperforming current leading image watermarking techniques.
- To enhance security, an additional layer of protection is implemented. Prior to embedding, the watermark is scrambled using a chaotic reordering known as the Arnold transformation.

## II. A REVIEW OF SOME BASIC PRELIMINARIES

### A. Discrete Wavelet Transform

The DWT is a frequency-based transform that provides a time-frequency representation of a digital signal. The two-dimensional DWT (2D-DWT) decomposes an image into an ensemble of four components, which can be reassembled by its inverse procedure (2D-IDWT) to reconstruct the original image. The 2D-DWT is realized using two digital channel filters, a low pass and a high pass, and a set of down samplers [16]. The input image is decomposed by these filters into four components with distinct resolutions: a low-resolution approximation (LL), and vertical (LH), horizontal (HL), and diagonal (HH) detail components. Most of the original image information is contained in the LL component, while the vertical, horizontal, and diagonal details are embodied in the LH, HL, and HH components, respectively.

### B. Hessemberg Decomposition

HD is the factorization of a square matrix B as [17]:

$$B = QHQ^T \quad (1)$$

where Q is an orthogonal matrix and H is an upper Hessenberg matrix satisfying $h_{ij} = 0$ for $i > j+1$. HD is computed by Householder matrices. The Householder matrix P is an orthogonal matrix given by:

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

where $\mu$ is a non-zero vector in $R^n$ and $I_n$ is the $n \times n$ identity matrix. There are $n-2$ steps in the whole process when B is of size $n \times n$. Hence, HD is computed as follows:

$$H = \left(P_1P_2 \ldots P_{n-3}P_{n-2}\right)^T B \left(P_1P_2 \ldots P_{n-3}P_{n-2}\right) \quad (3)$$

where:

$$Q = P_1P_2 \ldots P_{n-3}P_{n-2} \quad (4)$$

### C. Singular Value Decomposition

SVD is a procedure that allows to retrieve the geometric structures of an image. It decomposes a rectangular matrix into three matrices: U, S, and V. S is a diagonal matrix with non-negative diagonal elements, $S = \text{diag}(s1, s2, ..., sn)$ [18]. The diagonal elements, called singular values, satisfy the order $s1 \geq s2 \geq ... \geq sn$. It is important to emphasize that the singular values of S reflect the luminance levels of the image and a slight change in them does not affect the image quality. They remain largely unchanged even after attack, a useful property in

watermarking schemes. Multiplying U by S gives the principal component matrix:

$$PC = USV^T \quad (5)$$

The principal component contains the distinctive characteristics of any matrix. Therefore, it is exploited in this study to verify ownership.

### *D. Arnold Transform*

To further secure the embedded signature, Arnold scrambling is applied to it. The Arnold scrambling transformation is formulated as [19]:

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \bmod N \quad (6)$$

$$u, v, u', v' = \{1, 2, \cdots, N\}$$

where $(u, v)$ and $(u', v')$ are the pixel coordinates of the original and scrambled images, respectively, and N is the side length of the processed square image. The original watermark is restored by applying the inverse transformation, defined as:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} u' \\ v' \end{pmatrix} \bmod N \quad (7)$$

### *E. Artificial Bee Colony*

ABC is a well-known refinement procedure proposed by Karaboga in 2005 that optimizes the objective function [20]. It is a straightforward optimization approach inspired by the foraging behavior of a swarm of bees. The ABC algorithm relies on three types of bees: employed bees, onlooker bees, and scout bees. ABC has been widely adopted because of its many advantages, such as fast convergence, few initial parameters, and simple realization. In this work, ABC is used to find the appropriate scaling coefficients that optimize the robustness-imperceptibility tradeoff.

## III. PROPOSED WATERMARKING SCHEME

The proposed watermarking method consists of three parts, which are described in this section: embedding the watermark into the host image, extracting the watermark, and finding optimal embedding scaling factors.

### *A. Watermark Embedding System*

The structure of the embedding process is shown in Figure 1. It consists of the following steps:

- First, the color cover I and the color watermark image w are converted to the YCbCr color space to obtain the components $I_Y$, $I_{Cb}$, $I_{Cr}$ and $w_Y$, $w_{Cb}$, $w_{Cr}$, respectively.
- Select $w_Y$, the luminance component, and randomize it by applying the Arnold transform to obtain $w'_Y$.
- Apply the one-level 2D-DWT to the components $I_Y$ and $w'_Y$ to decompose them into four sub-bands $I_{YLL}$, $I_{YLH}$, $I_{YHL}$, $I_{YHH}$ and $w'_{YLL}$, $w'_{YLH}$, $w'_{YHL}$, $w'_{YHH}$, respectively.

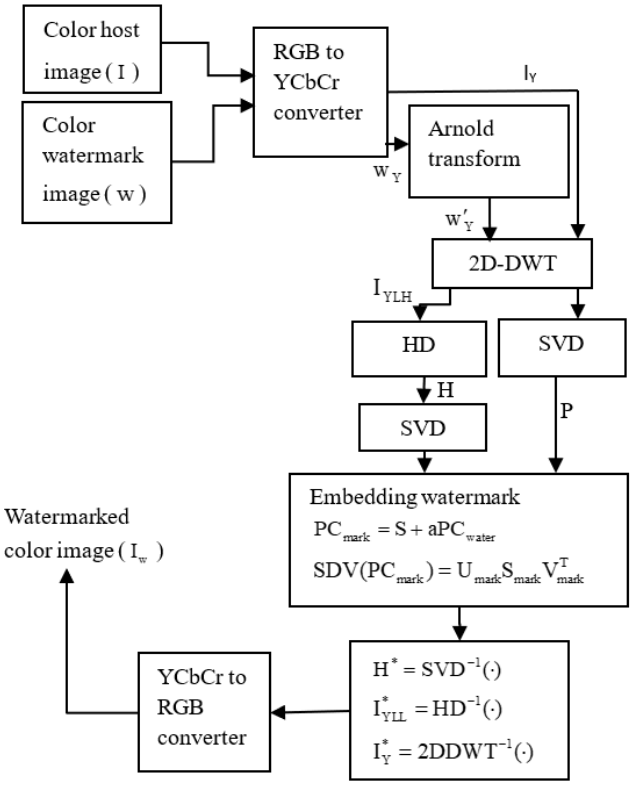



Fig. 1. Flowchart of the embedding system.

- Select the sub-band $I_{YLL}$, as the embedding position and perform the Hessenberg decomposition on it by applying (1). $I_{YLL}$ contains most of the information and can withstand diverse forms of manipulation to ensure robustness.
- Apply SVD on sub-band $w'_{YHL}$, extract the principal component of the sub-band $PC_{water}$ and save the $V^T_{water}$ matrix for later watermark extraction.

$$w'_{YHL} = U_{water}S_{water}V^T_{water} \quad (8)$$

$$PC_{water} = U_{water}S_{water} \quad (9)$$

- Select the upper Hessenberg matrix H (from step 4), apply SVD on it, and save the S matrix for watermark extraction.

$$H = USV^T \quad (10)$$

- Embed the $PC_{water}$ into the diagonal matrix S of the upper Hessenberg matrix H of the cover by using the scaling factor α obtained by the ABC algorithm as:

$$PC_{Smark} = S + \alpha PC_{water} \quad (11)$$

- Perform SVD on $PC_{Smark}$ and save $U_{mark}$ and $V^T_{mark}$ matrices for watermark extraction.
- The watermarked upper Hessenberg matrix $H^*$ is obtained by the inverse SVD as:

$$H^* = US_{mark}V^T \quad (12)$$

- A new sub-band $I^*_{YLL}$ is reconstructed by the inverse Hessenberg decomposition, given by:

$$I^*_{YLL} = QHQ^T \quad (13)$$

- Apply one-level inverse 2D-DWT to $I^*_{YLL}$, $I_{YLH}$, $I_{YHL}$, $I_{YHH}$ to obtain the watermarked luminance component $I^*_Y$.
- Combine $I^*_Y$ with $I_{Cb}$ and $I_{Cr}$ to reconstruct the watermarked image in the YCbCr space, and then convert it to RGB space to obtain the watermarked image $I_w$.

*B. Watermark Extraction System*

The extraction procedure is implemented as illustrated in Figure 2 and it is described in the following steps:

- Transform the watermarked image $I_w$ to the YCbCr space to obtain the components $I_{wY}$, $I_{wCb}$, and $I_{wCr}$.
- Use $I_{wY}$ as it is the part where the watermark luminance information is, and apply 2D-DWT to it to obtain sub-bands $I_{wYLL}$, $I_{wYLH}$, $I_{wYHL}$ and $I_{wYHH}$.
- Select the sub-band $I_{wYLL}$ and perform the Hessenberg decomposition on it, as:

$$I_{wYLL} = Q_w H Q_w{}^T \quad (14)$$

- Select the upper Hessenberg matrix $H_w$ and apply SVD on it, as:

$$H_w = U_w S_w V_w{}^T \quad (15)$$

- Use the keys $U_{mark}$ and $V^T_{mark}$, saved in the embedding process, to obtain:

$$PC^*_{Smark} = U_{mark} S_{mark} V^T_{mark} \quad (16)$$

- Use the key S, saved in the implanting process, and extract the principal component of the watermark:

$$PC^*_{water} = \frac{PC^*_{Smark} - S}{\alpha} \quad (17)$$

- Use the key $V^T_{water}$, saved in the implanting process, to get the watermark sub-band $w^*_{YHL}$ as:

$$w^*_{YHL} = PC^*_{water} V^T_{water} \quad (18)$$

- Apply one-level inverse 2D-DWT to the four sub-bands $w_{YLL}$, $w^*_{YLH}$, $w_{YHL}$, and $w_{YHH}$ to obtain the scrambled watermark luminance component $w^{*\prime}_Y$.
- Perform the Arnold inverse transform on $w^{*\prime}_Y$ to obtain the unscrambled watermark luminance component $w^*_Y$.
- Merge the $w^*_Y$ component with the $w_{Cb}$, $w_{Cr}$ components obtained and saved during the embedding phase, and perform conversion to RGB space to obtain the extracted watermark $w^*$.

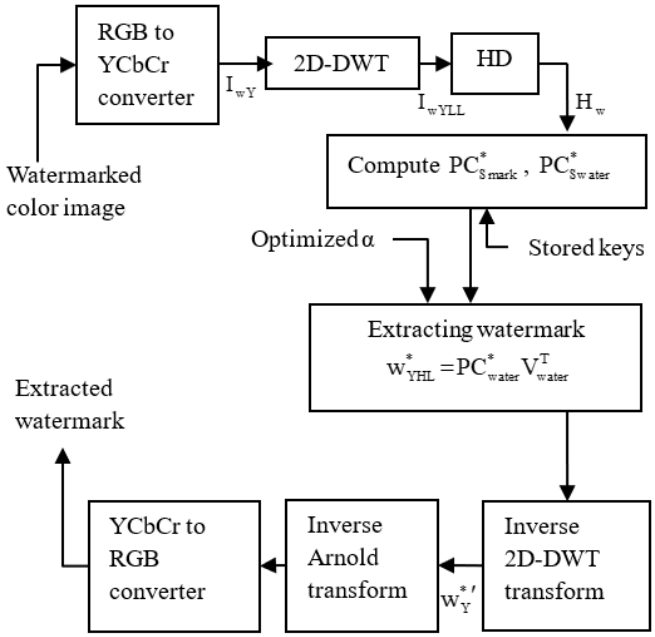



Fig. 2. Flowchart of the extraction process.

*C. Artificial Bee Colony Optimization of Scaling Coefficients*

The imperceptibility and robustness of the proposed scheme are critically dependent on the scaling coefficient value, and thus it is essential to determine the best value that provides a balance between them for each embedding in the singular values. Imperceptibility is commonly quantified by benchmarking standards such as the Peak Signal to Noise Ratio (PSNR) for color images [21]:

$$PSNR_{average}(dB) = \frac{\sum_{k=1}^{3} PSNR_k(dB)}{3} \quad (19)$$

where $PSNR_k(dB)$ with k=1,2,3 denotes the PSNR of the R, G, and B components of a color image, respectively:

$$PSNR_k(dB) = 10Log_{10}\left(\frac{MN\left[Max\left(I(i,j,k)\right)\right]^2}{\sum_{i=0}^{M}\sum_{j=0}^{N}\left[I(i,j,k) - I_w(i,j,k)\right]^2}\right) \quad (20)$$

where $I(i,j,k)$ and $I_w(i,j,k)$ represent the values of pixel $(i,j)$ in the element k of the host I and watermarked $I_w$ color images, respectively. Max denotes the maximum pixel value of $I(i,j,k)$ and M, N are the dimensions of the image [21]. A higher PSNR signifies a closer resemblance between the

original and the watermarked images, which indicates a higher imperceptibility of the watermarking technique.

The Normalized Correlation (NC) is usually used to weight the robustness of the structure, i.e., to estimate the degree of similarity between the original and the recovered watermarked images [21]. It is defined by:

$$NC = \frac{\sum_{k=1}^{3}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left(W(i,j,k)W^{*}(i,j,k)\right)}{\sqrt{\sum_{k=1}^{3}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[W(i,j,k)\right]^{2}} * \sqrt{\sum_{k=1}^{3}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[W^{*}(i,j,k)\right]^{2}}} \quad (21)$$

where W and $W^{*}$ represent the original and retrieved watermarks, respectively. P, Q are the width and height of the watermark, respectively. A higher NC, close to 1, indicates that the retrieved watermark is more similar to the original watermark and the watermarking routine is more robust. In this work, ABC provides an appropriate balance between imperceptibility and robustness. The main idea is to achieve greater robustness against numerous attacks under the principle of maintaining imperceptibility. The procedure for optimizing the embedding scaling factors (α) is displayed in Figure 3 and the parameter values of ABC are given in Table I. We apply P different types of attacks on the watermarked color image $I_w$. The average robustness, given by (22), is the objective function to be maximized while ensuring that the PSNR remains equal to or above the target threshold.

$$\text{Robustness}_{\text{average}} = \frac{\sum_{i=0}^{P} NC\left(W, W_i^{*}\right)}{P} \quad (22)$$

where P denotes the number of attacks. The fitness function (Ft) of the ABC algorithm is defined as:

$$\text{Minimize Ft} = \frac{1}{\text{Robustness}_{\text{average}}} \quad (23)$$

TABLE I. PARAMETER VALUES OF ABC OPTIMIZATION

| ABC optimization settings | Values |
|---|---|
| Swarm size | 25 |
| The highest number of iterations | 25 |
| Limit | 12 |
| Starting range | [0.002, 1] |
| Count of employed bees | 50% of swarm size |
| Count of onlooker bees | 50% of swarm size |
| Count of scout bees | 50% of swarm size |
| Attacks | Noise adding, filtering, sharpening, compression, rotation, and translation |

## IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed watermark pattern was validated under MATLAB (R2017a) environment with 4 host images, baboon, pepper, airplane, and sailboat [22], and two watermarks, Peugeot logo and an 8-color image. They are all 24-bit color and have a resolution of 512×512. They are displayed in Figure 4.

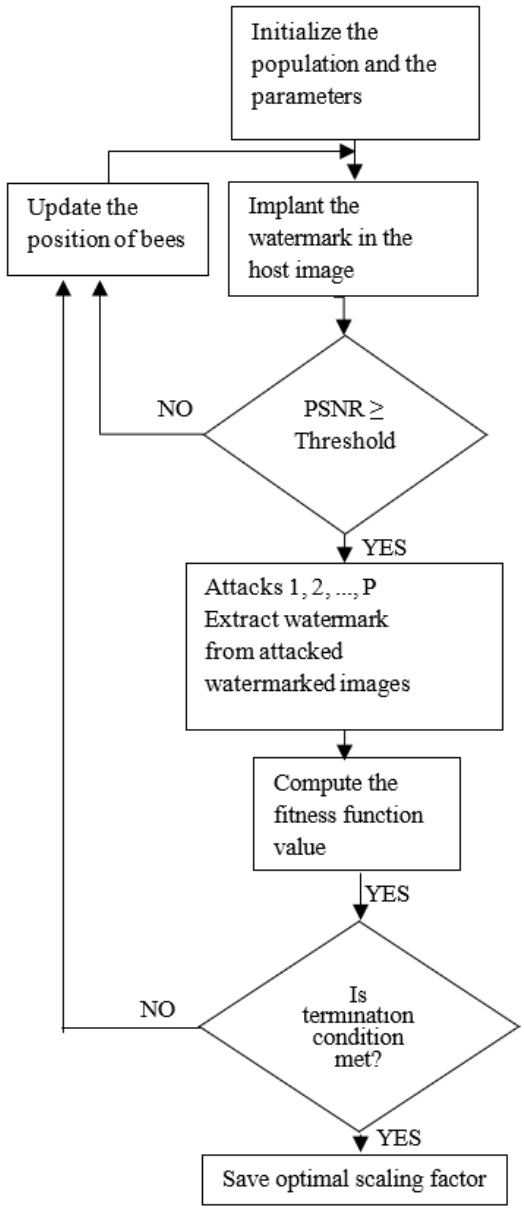
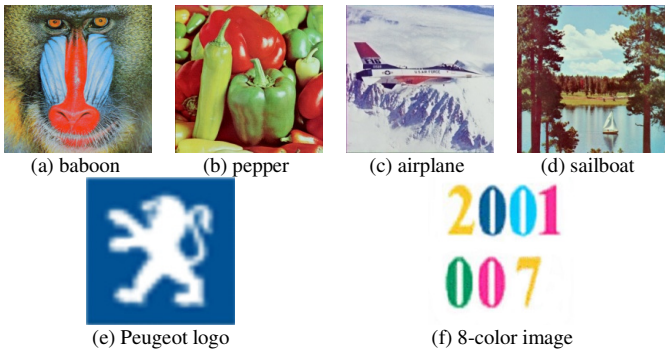



Fig. 3. The optimization process of the embedding scaling factors (α).



(a) baboon (b) pepper (c) airplane (d) sailboat

(e) Peugeot logo (f) 8-color image

Fig. 4. Color host images (a-d) and color watermark images (e-f).

### *A. Imperceptibility Results and Comparative Analysis*

When the PSNR is greater than 35 dB, the watermark is considered imperceptible [23]. From Table II, the values of PSNR are greater than 46 dB for different host images and two watermarks, indicating that our scheme has high imperceptibility. NC is equal to 1, indicating that the mark is fully recovered.

TABLE II. IMPERCEPTIBILITY RESULTS

| Host images | Watermark images | | | |
|---|---|---|---|---|
| | Peugeot logo | | 8-color image | |
| | PSNR (dB) | NC | PSNR (dB) | NC |
| Baboon | 46.0233 | 1 | 46.5473 | 1 |
| Pepper | 46.5200 | 1 | 47.1339 | 1 |
| Airplane | 46.4928 | 1 | 47.1122 | 1 |
| Sailboat | 47.0590 | 1 | 47.5427 | 1 |

We compared the PSNR values of the proposed scheme with those of recent works, using the same host image airplane and the Peugeot logo. We found that our scheme has better invisibility: 45.3999 dB for [24], 44.4467 dB for [25], 46.0184 dB for [26], and 46.4928 dB for our scheme.

### *B. Robustness Results and Comparative Analysis*

The proposed algorithm was tested with diverse image attacks corresponding to non-geometric attacks (filtering, adding noise, and JPEG compression), geometric attacks (rotation, scaling, cropping, and cutting) and combinational attacks. A comparative analysis with the recent schemes in [24, 25, 27], under the same attacks and parameters, with the Peugeot logo as watermark and airplane as the cover, is illustrated in Table III. Another comparison with the recent techniques in [28, 29], done with the 8-color image as watermark and airplane as cover, is shown in Table IV.

TABLE III. ROBUSTNESS COMPARISON BETWEEN THE PROPOSED SCHEME AND THE SCHEMES IN [24, 25, 27], BASED ON NC VALUES

| Attacks | Parameters | Methods with cover airplane and Peugeot logo watermark | | | |
|---|---|---|---|---|---|
| | | [24] | [25] | [27] | Proposed |
| JPEG compression | 70 | - | - | 0.9959 | 0.9985 |
| | 90 | 0.9986 | 0.9988 | - | 0.9986 |
| Salt and pepper noise | 0.01 | - | 0.9920 | 0.9922 | 0.9978 |
| | 0.05 | 0.9918 | 0.9337 | - | 0.9902 |
| Gaussian noise | 0.01 | - | 0.9772 | 0.9956 | 0.9948 |
| | 0.05 | 0.9146 | 0.8380 | - | 0.9742 |
| Speckle noise | 0.01 | - | 0.9841 | 0.9917 | 0.9968 |
| | 0.05 | 0.9822 | 0.8653 | - | 0.9860 |
| Median filter | 3×3 | - | - | 0.9952 | 0.9977 |
| Gaussian filter | 3×3 | 0.9960 | 0.9963 | 0.9962 | 0.9981 |
| | 5×5 | - | 0.9932 | - | 0.9981 |
| Sharpening | | 0.9745 | 0.9733 | 0.9935 | 0.9954 |
| Mean filter | 3×3 | 0.9944 | 0.9948 | 0.9941 | 0.9956 |
| | 5×5 | - | 0.9818 | - | 0.9867 |
| Cropping | 0.20 | 0.8871 | 0.9239 | - | 0.9956 |
| Rotation | 10° | 0.8182 | 0.8445 | - | 0.9805 |
| | 5° | - | 0.8984 | 0.9930 | 0.9867 |
| Rescale | 0.5 | - | - | 0.9962 | 0.9975 |
| | 2 | - | - | 0.9970 | 0.9985 |
| Gamma correction | 0.8 | - | 0.9800 | - | 0.9944 |

TABLE IV. ROBUSTNESS COMPARISON BETWEEN THE PROPOSED SCHEME AND THE SCHEMES IN [28, 29] BASED ON NC VALUES

| Attacks | Parameters | Methods with cover airplane and 8-color image watermark | | |
|---|---|---|---|---|
| | | [28] | [29] | Proposed |
| JPEG compression | 30 | 0.7541 | 0.9881 | 0.9992 |
| JPEG 2000 | CR=10 | 0.8405 | 0.9998 | 0.9992 |
| Gaussian noise | 0.003 | 0.6478 | 0.9965 | 0.9990 |
| Salt and pepper noise | 0.01 | 0.9251 | 0.9872 | 0.9989 |
| Median filter | 2×2 | 0.7009 | 0.9992 | 0.9992 |
| Cropping | 0.50 | 0.9625 | 0.8200 | 0.9856 |
| Zoom-out | 1:2 | 0.7999 | 0.9989 | 0.9991 |
| Rotation | 30° | 0.8224 | 0.8274 | 0.9869 |

The proposed scheme outperforms all these methods in terms of NC performance under most attack scenarios, demonstrating superior robustness. Some outcomes of these attacks are given in Figures 5 and 6.

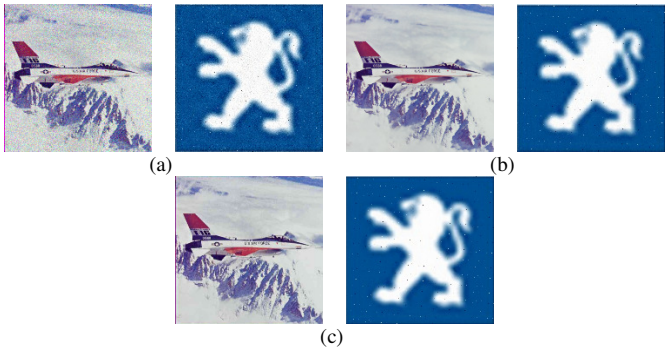


Fig. 5. Watermarked airplane and extracted Peugeot logo after non-geometric attacks: (a) Gaussian noise (1%), (b) Winner filter (5×5), and (c) JPEG compression (30).

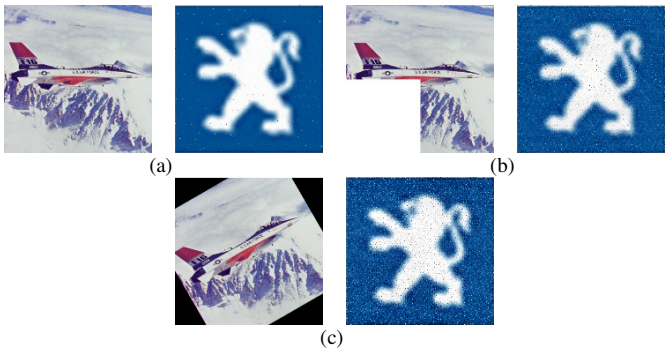


Fig. 6. Watermarked airplane and extracted Peugeot logo after geometric attacks: (a) Cutting (10 columns), (b) Cropping (25%), and (c) Rotation (anticlockwise 30°).

### *C. Multiple Attacks*

The simultaneous application of several attacks on a watermarked image is referred to as a multiple attack. The proposed scheme was also tested against different combinations of attacks. Table V reveals that the NC values of our scheme are higher than 0.97 for all the numerous attacks applied, and they are higher than those of [29, 30] when

performing the same multiple attacks with the same parameters using the color host images baboon and pepper, and the Peugeot logo as the watermark. Figure 7 presents some results of these manipulations on the baboon image with the Peugeot logo embedded.

TABLE V. NC VALUES UNDER MULTIPLE ATTACKS WITH THE SAME PARAMETERS USING THE PEUGEOT LOGO WATERMARK

| Multiple attacks | Host images and methods | | | | | |
|---|---|---|---|---|---|---|
| | Baboon | | | Pepper | | |
| | [30] | [29] | Proposed | [30] | [29] | Proposed |
| Gaussian noise (0.01) + cropping (25%) | 0.9045 | 0.9046 | 0.9934 | 0.8990 | 0.8996 | 0.9861 |
| Median filter (2×2) + translation (20,20) | 0.9923 | 0.9942 | 0.9952 | 0.9918 | 0.9948 | 0.9953 |
| Salt and pepper noise (0.02) + rotation (1°) | 0.9699 | 0.9707 | 0.9973 | 0.9685 | 0.9695 | 0.9970 |
| JPEG compression (Q=90) + translation (10,10) | 0.9710 | 0.9784 | 0.9983 | 0.9700 | 0.9768 | 0.9977 |
| Salt and pepper noise (0.02) + cropping (25%) | 0.9699 | 0.8132 | 0.9922 | 0.9685 | 0.7980 | 0.9868 |
| JPEG compression (Q=30) + rotation (1°) | 0.9045 | 0.9772 | 0.9966 | 0.9130 | 0.9790 | 0.9972 |
| Salt and pepper noise (0.1) + scaling (0.25) | 0.9455 | 0.9332 | 0.9568 | 0.9570 | 0.9660 | 0.9849 |
| Salt and pepper noise (0.02) + cutting (10) | 0.8990 | 0.9484 | 0.9978 | 0.9090 | 0.9448 | 0.9956 |

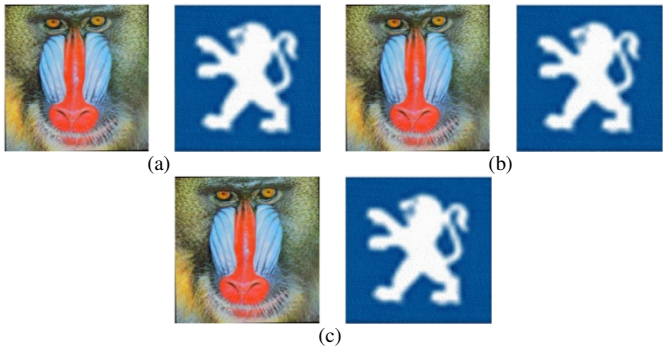


Fig. 7. Watermarked baboon and extracted Peugeot logo under combined attacks. (a) JPEG compression (30) + rotation (anticlockwise 1˚), (b) Median filter (2×2) + translation (20, 20), and (c) Salt and pepper noise (0.02) + cutting (10 columns).

### *D. Embedding Capacity Analysis*

Embedding capacity refers to the maximum amount of data, measured in bits, that can be embedded into the host image [31]. In our approach, we utilize a 512×512 color cover and a 512×512 color watermark. Consequently, the embedding capacity of our scheme is (512×512×24)/(512×512×3)=8 bpp. This is high compared to the other schemes with (256×256×8)/(512×512×3)=0.6667 bpp [24, 25] and (64×64×24)/(512×512×3)=0,125 bpp [26], respectively.

## V. CONCLUSION

Watermarking technology requires a balance between imperceptibility, robustness, and embedding capacity, without forgetting the security factor. In this paper, we aimed to achieve these properties by proposing an optimized semi-blind watermarking configuration for color images. The watermark utilized is a color image with the same dimensions as the host color image (512×512), which has the advantage of having a high embedding capacity. The proposed structure is based on Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD) transform in the Discrete Wavelet Transform (DWT) domain, since watermarking in the transform domain offers high robustness. HD allowed us to significantly increase the imperceptibility factor. In particular, we used the Artificial Bee Colony (ABC) algorithm to find the best scaling factors, which allowed us to find the right balance between the values of imperceptibility and robustness. To enhance the security, the watermark image was scrambled using the Arnold transformation. The result showed that the proposed watermarking system was highly imperceptible. It was also tested to be robust against common image processing manipulations such as filtering and JPEG compression, geometric attacks such as rotation, and various combinations of attacks such as adding noise and rotation, filtering and translation, or JPEG compression and rotation. In addition, a comparative evaluation against the latest advanced image watermarking techniques demonstrated its superiority in terms of imperceptibility, robustness, and capacity.

## ACKNOWLEDGMENT

The authors would like to thank the General Directorate for Scientific Research and Technological Development of the Algerian Republic in general and the LIS, ETA, laboratories of Setif-1 and Bordj Bou Arreridj Universities.

## REFERENCES

[1] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *INDIN '05. 2005 3rd IEEE International Conference on Industrial Informatics*, Perth, WA, Australia, 2005, pp. 709–716, https://doi.org/10.1109/INDIN.2005.1560462.

[2] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, Dec. 2014, https://doi.org/10.1016/j.eswa.2014.06.011.

[3] H. Tao, L. Chongmin, J. Mohamad Zain, and A. N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, Feb. 2014, https://doi.org/10.1016/S1665-6423(14)71612-8.

[4] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan, and N. N. Xiong, "A Robust Watermarking Scheme in YCbCr Color Space Based on Channel

Coding," *IEEE Access*, vol. 7, pp. 25026–25036, 2019, https://doi.org/10.1109/ACCESS.2019.2896304.

[5] P. V. S. and C. M. P. V. S. S. R., "A robust semi-blind watermarking for color images based on multiple decompositions," *Multimedia Tools and Applications*, vol. 76, no. 24, pp. 25623–25656, Dec. 2017, https://doi.org/10.1007/s11042-017-4355-0.

[6] S. Singh, V. S. Rathore, R. Singh, and M. K. Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 19113–19137, Sep. 2017, https://doi.org/10.1007/s11042-017-4570-8.

[7] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Color image blind watermarking scheme based on QR decomposition," *Signal Processing*, vol. 94, pp. 219–235, Jan. 2014, https://doi.org/10.1016/j.sigpro.2013.06.025.

[8] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66, no. 3, pp. 385–403, May 1998, https://doi.org/10.1016/S0165-1684(98)00017-6.

[9] S.-W. Byun, H.-S. Son, and S.-P. Lee, "Fast and Robust Watermarking Method Based on DCT Specific Location," *IEEE Access*, vol. 7, pp. 100706–100718, 2019, https://doi.org/10.1109/ACCESS.2019.2931039.

[10] V. Solachidis and L. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, Nov. 2001, https://doi.org/10.1109/83.967401.

[11] S. Roy and A. K. Pal, "A Hybrid Domain Color Image Watermarking Based on DWT–SVD," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 2, pp. 201–217, Jun. 2019, https://doi.org/10.1007/s40998-018-0109-x.

[12] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1167–1180, Jul. 1999, https://doi.org/10.1109/5.771070.

[13] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002, https://doi.org/10.1109/6046.985560.

[14] Q. Su, G. Wang, G. Lv, X. Zhang, G. Deng, and B. Chen, "A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8781–8801, Mar. 2017, https://doi.org/10.1007/s11042-016-3522-z.

[15] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *International Journal of Computational Intelligence Systems*, vol. 8, no. 2, pp. 364–380, Jan. 2015, https://doi.org/10.1080/18756891.2015.1001958.

[16] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 7, pp. 674–693, Jul. 1989, https://doi.org/10.1109/34.192463.

[17] Q. Su, "Novel blind colour image watermarking technique using Hessenberg decomposition," *IET Image Processing*, vol. 10, no. 11, pp. 817–829, Nov. 2016, https://doi.org/10.1049/iet-ipr.2016.0048.

[18] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection," *Expert Systems with Applications: An International Journal*, vol. 39, no. 1, pp. 673–689, Jan. 2012, https://doi.org/10.1016/j.eswa.2011.07.059.

[19] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," in *2009 First International Conference on Information Science and Engineering*, Nanjing, China, 2009, pp. 1164–1167, https://doi.org/10.1109/ICISE.2009.347.

[20] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing*, vol. 84, Nov. 2019, Art. no. 105696, https://doi.org/10.1016/j.asoc.2019.105696.

[21] Q. Su, Y. Niu, X. Liu, and Y. Zhu, "Embedding color watermarks in color images based on Schur decomposition," *Optics Communications*, vol. 285, no. 7, pp. 1792–1802, Apr. 2012, https://doi.org/10.1016/j.optcom.2011.12.065.

[22] "SIPI Image Database," *USC Viterbi*. https://sipi.usc.edu/database/database.php?volume=misc.

[23] Q. Zheng, N. Liu, and F. Wang, "An Adaptive Embedding Strength Watermarking Algorithm Based on Shearlets' Capture Directional Features," *Mathematics*, vol. 8, no. 8, Aug. 2020, Art. no. 1377, https://doi.org/10.3390/math8081377.

[24] Y. Dong, R. Yan, Q. Zhang, and X. Wu, "A Hybrid Domain Color Image Watermarking Scheme Based on Hyperchaotic Mapping," *Mathematics*, vol. 12, no. 12, Jun. 2024, Art. no. 1859, https://doi.org/10.3390/math12121859.

[25] Y. Dong, R. Yan, and C. Yin, "An adaptive robust watermarking scheme based on chaotic mapping," *Scientific Reports*, vol. 14, no. 1, Oct. 2024, Art. no. 24735, https://doi.org/10.1038/s41598-024-76101-w.

[26] S. Sharma, H. Sharma, J. B. Sharma, and R. C. Poonia, "A secure and robust color image watermarking using nature-inspired intelligence," *Neural Computing and Applications*, vol. 35, no. 7, pp. 4919–4937, Mar. 2023, https://doi.org/10.1007/s00521-020-05634-8.

[27] R. Dwivedi and V. K. Srivastava, "IWT based robust and secure color image watermarking using Hessenberg decomposition and SVD," *Journal of Optics*, Aug. 2024, https://doi.org/10.1007/s12596-024-02141-0.

[28] H. Wang, Z. Yuan, S. Chen, and Q. Su, "Embedding color watermark image to color host image based on 2D-DCT," *Optik*, vol. 274, Mar. 2023, Art. no. 170585, https://doi.org/10.1016/j.ijleo.2023.170585.

[29] B. Latreche, H. Naimi, and S. Saadi, "A secure and robust color image watermarking method using SVD and GAT in the multiresolution DCHWT domain," *The Journal of Engineering and Exact Sciences*, vol. 9, no. 10, pp. 17317–01e, Nov. 2023, https://doi.org/10.18540/jcecvl9iss10pp17317-01e.

[30] A. M. Cheema, S. M. Adnan, and Z. Mehmood, "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," *IEEE Access*, vol. 8, pp. 169525–169547, 2020, https://doi.org/10.1109/ACCESS.2020.3024181.

[31] R. Thanki and S. Borra, "A color image steganography in hybrid FRT–DWT domain," *Journal of Information Security and Applications*, vol. 40, pp. 92–102, Jun. 2018, https://doi.org/10.1016/j.jisa.2018.03.004.