Received August 30, 2020, accepted September 8, 2020, date of publication September 15, 2020,
date of current version September 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3024181

A Novel Optimized Semi-Blind Scheme for Color Image Watermarking

ADNAN MUSTAFA CHEEMA[1], SYED MUHAMMAD ADNAN[1], AND ZAHID MEHMOOD[2]
[1]Department of Computer Science, University of Engineering and Technology at Taxila, Taxila 47050, Pakistan
[2]Department of Computer Engineering, University of Engineering and Technology at Taxila, Taxila 47050, Pakistan

Corresponding authors: Zahid Mehmood (zahid.mehmood@uettaxila.edu.pk) and Adnan Mustafa Cheema (adnan.mustafa@uettaxila.edu.pk)

ABSTRACT Image watermarking is a robust solution for solving key issues like copyright protection and proof of ownership of digital data. Existing schemes of image watermarking mostly used grayscale or binary images as embedded watermarks, while only a few watermarking schemes are developed for color images. In this article, we propose a novel robust semi-blind image watermarking scheme based on finite ridgelet transform (FRT), discrete wavelet transform (DWT), singular value decomposition (SVD), particle swarm optimization (PSO), and Arnold transform to protect copyright and verify the authenticity of color images.Firstly, the color image is converted from RGB to YCbCr color space, and the luminance component (Y) is taken into account to insert the watermark data. In this study, the principal component (PC) of the watermark image is directly inserted into the corresponding singular value of the cover image by the scaling factor to avoid the false positive problem (FPP). To further improve security, Arnold transform is applied to process the Y channel of the watermark image before inserting it in the cover image. Besides, PSO optimizes the embedding factor matrices.The qualitative evaluation factors like peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) are used to assess the visual quality, while normalized correlation coefficient (NCC) is used to assess the resemblance between the watermarked and the restored watermarked images. The performance of the proposed scheme is evaluated using geometric, non-geometric, and combinational attacks, and its comparison is performed with different image watermarking schemes to prove its robustness.

INDEX TERMS Color image watermarking, false-positive free, finite ridgelet transform, copyright protection, particle swarm optimization.

I. INTRODUCTION

In recent years, distributing multimedia data (including images, videos, audios, etc.) on the network become easy and inexpensive. Nowadays, the copyright protection of color images used for digital information has become the most pressing issue which detracted more attentiveness of researchers [11], [24]. Therefore, to protect the multimedia data, we must design a robust, secure, reliable, and efficient copyright protection scheme. Numerous information security schemes such as encryption, steganography, cryptography, perceptual property, and watermarking have been proposed [1], [8], [12]. The digital watermarking scheme presents one of the best solutions between them [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Gianluigi Ciocca.

Digital watermarking is an effective information embedding scheme so that it's not easily perceived by others. In this scheme, the hidden watermark shouldn't degrade the image quality and it is invisible to provide copyright protection [1]–[5], [11], [21], [27]. The block diagram of the digital image watermarking is shown in Fig. 1. The inserted watermark data consists of different forms, including fingerprint or owner's identity, copyright messages, the license data, grayscale or color images, etc. [21], [24]. Watermarking schemes can be divided into various groups based on a different number of qualities [8], [26]. The watermarking scheme is grouped into three classes based on the availability of actual image contents during the watermark extraction stage, which is non-blind, semi-blind, and blind schemes. In a non-blind scheme, an unwatermarked cover image is required while extracting an

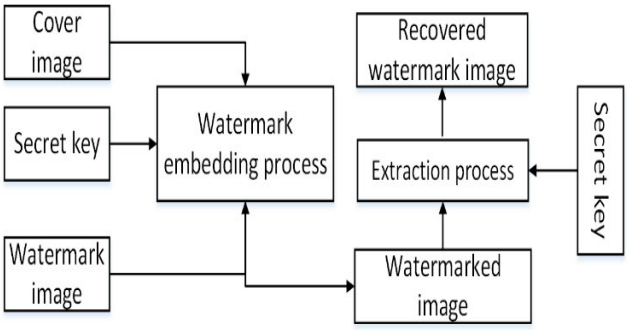


FIGURE 1. The basic concept of digital image watermarking.

embedded secret watermark image [1], [8], [12], [26]. In semi-blind scheme, additional information is used while extracting watermarks rather than the un-watermarked image [1], [8], [12], [35], [46]. In blind scheme, the embedded secret watermark image is extracted without referring to the cover image [1], [3], [7]–[10], [16], [26], [27]. The watermark scheme is often divided into two classes based on human perception, such as visible and non-visible watermarking schemes [1], [8], [12], [26], [27].

In the visible image watermarking scheme, the watermark is inserted into the cover image in a way that the user can see the hidden water-mark [1], [26]. In the invisible watermarking scheme, the watermark is inserted in the cover image in a manner that is accessed only by the authorized user [1], [12], [18], [26].

Digital watermarking technology has made considerable strides over the last ten years. However, conventional watermarking schemes are primarily designed for grayscale images, while color image watermarking schemes have not been sufficiently explored. This is mainly since the grayscale image is easy to process and it only contains details about the luminance of the image. In contrast to binary and grayscale images, color images can significantly increase the capacity and loyalty of information. In the color image watermark, color perception is based on luminance as well as chrominance. Color images can be divided into three primary color channels as compared with single-channel grayscale images; thus color image watermarking is more challenging. The literature provides a variety of decomposition schemes for color images such as YIQ, YCbCr, RGB, and HSI. Among them, YCbCr is the most popular color space, since the YCbCr color space is built along with many other color models to deal with this kind of image processing applications.

Watermarking is mainly based on the watermark insertion process which is performed in two key domains (such as spatial and frequency domains) [1], [12], [13]. The spatial domain modifies pixels of the cover image for watermarks embedding [1], [12], [24], [46]. Numerous spatial domain-based schemes like LSB, PVD, etc. are used for watermark insertion. The most recent research reveals that the schemes focused on the spatial domain cannot solve the following deficiencies [12], [24], [26]: (1) not robust against the non-geometric and geometric attacks. (2) Inconsistent watermark capacity, and (3) the resemblance between the cover as well as the recovered watermark image is low. Therefore, researchers are also proposing watermark schemes within the frequency domain. The frequency-domain based algorithms has different applications, such as watermarking algorithms developed using frequency-domain operations like discrete wavelet transform (DWT) [1], [5], [13], [17], [24], [48], [50]. The frequency-domain of the cover data is originally broken down into different frequencies. The frequency domain-based watermark schemes are sub-classified into discrete Fourier transform (DFT) [52], stationary wavelet transform (SWT) [11], discrete cosine transform (DCT) [14], [19], [27], etc. The DWT divides the image into a series of different sub-bands or sub-images [1], [24]. The high-frequency sub-images provide details on edge elements, and low-frequency sub-images (which provides smoothness information) are again divided into low as well as high-frequency sub-images [1], [12], [24]. As the low-frequency sub-images carries the highest energy, the change here causes the image quality to degrade significantly [1], [1], [32]. High-frequency sub-images are commonly used for watermarking attacks, as evidence indicates that the human visual system (HVS) is typically less prone to high-frequency coefficients [1], [24]. Therefore, the high-frequency sub-images are regarded as being the most important sub-images for watermark embedding [31], [32].

A. MAJOR CONTRIBUTIONS OF THE PROPOSED WATERMARK SCHEME

1) Instead of manually selecting the scaling factors as in [11], [13], [34], [38], the proposed watermark scheme apply particle swarm optimization (PSO) to automatically find the best value of the scaling factors based on the target PSNR and predefined conditions to obtain the highest possible robustness without losing transparency.
2) To remove the false-positive problem (FPP)-based security risk, the proposed watermark scheme uses an improved false positive free color watermarking scheme-based security method, which combines the Arnold transform to provide legal ownership and copyright protection for legitimate users.
3) The proposed watermark scheme provides a high embedding capacity, good watermark imperceptibility, and strong robustness against all geometric attacks (i.e. rotation, scaling, cropping, and cutting), non-geometric attacks (i.e. Gaussian filtering, sharpness, salt and pepper noise, median filtering, JPEG compression), and combinational attacks (both geometric and non-geometric attacks) as compared with state-of-the-art image watermarking schemes.
4) The proposed watermark scheme uses a novel watermark embedding scheme by considering the cover image luminance (Y) channel of the YCbCr color component instead of the RGB color components to

TABLE 1. The classification of related image watermarking schemes.

Scheme	WM Type	Type	Processing domain	Description	Pros	Cons
Bagheri et al. [5]	Color	Blind	Transform	DWT-HVS-SVD-PSO	Free of a false-positive problem (FPP), Provide twice times the payload capacity compared to its similar schemes	Less secure, less robust against some geometric attacks like rotation, scaling.
Singh et al. [8]	Grayscale	Semi-blind	Transform	NSCT-RDWT-SVD	No information is lost during decomposition and reconstruction of the wavelet.	RDWT scheme is computationally costly and its scaling factors are selected manually.
Panday et al. [11]	Color	Non-blind	Transform	SWT-SVD	Effective for low bandwidth channels as well as security	Less PSNR and not robust against compression attacks, scaling factors are selected manually.
Tan et al. [12]	Color	Non-blind	Transform	DWT-SVD	CCMES scheme provide almost perfect robustness for all attacks	Imperceptibility is worst.
Ernawan et al. [13]	Color	Blind	Transform	RDWT-HVS-SVD	Free of a false-positive problem (FPP), Proving high robustness and imperceptibility	Its thresholds are selected manually.
Roy et al. [34]	Color	Non-blind	Transform	DCT-SVD	Free of a false-positive problem (FPP)	Its scaling factors are selected manually, Not very robust against geometric attacks.
Tarhouni et al. [44]	Color	Blind	Transform	2D-DCT	high level of imperceptibility and robustness against non-geometric attacks	Less secure, high embedding extraction time.
Kang et al. [59]	Grayscale	Blind	Transform	DWT-DCT-SVD-PSO	High imperceptibility and robustness	Trouble in resisting rotation attack.

avoid high lossy compression used by different image compression-based image watermarking schemes.

The rest of the sections of this article are categorized as follows: The second section provides detail of the recent image watermarking schemes. The third section introduces the basic knowledge required for the image watermarking schemes. The detail of the proposed watermark scheme is provided in the fourth section. The fifth section provides detail of the experimental results and discussions. Finally, section six presents the conclusion and future work of the proposed watermark scheme.

II. RELATED WORK

Recently, researchers have been working on integrating watermarking techniques based on wavelet transform coefficients and SVD to improve the robustness of watermarked images against non-geometric and geometric attacks [14], [15], [24], [27], [41], [50], [54]. Furthermore, hybrid schemes that combine these transforms with SVD are very successful in recent years [24], [37], [41]. In the SVD-based scheme, the watermark image is usually placed in the singular value of the cover image [45], [49]. Normally, two common techniques used to insert watermark information into a cover image are: the first technique is to insert the secret image directly into the cover image's singular value [8], [13], [24], [27], [32] and the second technique is to insert the value of the secret image into the cover image's singular value [11], [21]. Mostly literature of digital image watermarking only inserts the secret image's singular value into the cover image's singular value. Compared with traditional image processing techniques, even geometric distortion, the SVD-based scheme shows better strength and robustness. However, watermark embedding using the SVD technique can lead to ambiguity in the false-positive problem (FPP) [32], [45], [50], [51]. An intruder could freely get the right secret information from an illegal image, which is taken from the web or a publicly accessible source. When any image whose inserted watermark is different from the restored watermark, can obtain the correct forged restored watermark, an FPP occurs. Moreover, the issue of FPP can be resolved using the principal component (PC) [17], [32], [50], [51], [53]. Hence, the high robustness, greater embedding strength, and resistance to a false-positive problem (FPP) with good perceptual quality of a watermarking scheme remain a major issue among researchers. Table 1 presents a summary of the literature on image watermarking schemes. In recent decades, color image watermarking has become a popular research area among researchers worldwide, rather than grayscale image watermarking [21]. Compared with grayscale and binary image schemes, color images have two main advantages: a large amount of data can be hidden; the information capacity of color images is twenty-four (24) times greater than that of binary images [11]. Recently, researchers mostly concentrate on the digital watermarking scheme for grayscale images [24], [48], or binary images [54]. However, there are only a few efficient digital watermarking schemes for color images [2], [11], [21], [32]. In the literature, the majority of watermarking schemes are designed for binary or gray-level images [37], [48], [54]. In [24], the author proposed a hybrid image watermarking scheme based on DWT and SVD for protecting grayscale images. In this scheme, the RGB image is transformed into the YCbCr color space and the watermark is inserted into the Y channel of the cover image. The optimized DWT and SVD-based watermark schemes are proposed in [50], which can solve the problem of false-positive while

maintaining invisibility and robustness by mean of principal component (PC) and perceptual adjustment of images. In this scheme, the watermark is inserted into the grayscale image. Multiple scaling factors (MSF) are used in [54] to insert the singular matrix value of the secret binary watermark into the singular matrix value of the LL3 sub-band of the cover image. Few color image watermarking schemes use color images as watermarks, however, a comparison to the color cover image, the size is smaller due to the reduced perception efficiency [11], [21], [32]. At present, a huge challenge is the layout of a watermarking scheme which inserts a watermark into a color image in a transform domain of the same size and dimensions. When a watermark image that is equal to the size of the binary image, is inserted into the original image, the invisibility and robustness of the watermark image are severely impaired. In [2] and [7], the original three-dimensional secret color image is split into 32 × 32 pixels three distinct R, G, and B channels. The secret image is inserted in the 1st column of the Q color cover matrix of the image size 512 × 512 pixels. In [28], the original cover image of size 512 × 512 pixels is segmented in the R, G, and B channels, and then each channel is subjected to Schur decomposition. After that, a watermark image of size 32 × 32 pixels is inserted into a unitary matrix of the color cover image.

To increase the overall performance of the watermarking schemes: visual quality and robustness are two key indicators, and the trade-off between them is always a challenging problem [48]. Moreover, if we want a watermarking scheme to be more robust, then watermarked image quality may be sacrificed. In recent years, many bio-inspired algorithms are used to solve the aforementioned problems of watermarking, such as firefly algorithm (FA) [54], differential evolution (DE) [26], [55], artificial bee colony (ABC) [6], [32], [51], fruit fly optimization algorithm (FOA) [48], teaching-learning-based optimization (TLB) [47], and particle swarm optimization (PSO) [27], [31], [56]–[60]. PSO is an adaptive population dependent optimization approach that focused on fish education or social behavior of birds gathering. It can optimize the image watermarking scheme [36] when the embedding objectives are conflicting. A PSO-based watermarking scheme provides an objective function to find an ideal outcome in the search area [55]. The primary goal of this presented scheme is to develop a novel color scheme that can offer high robustness, strong imperceptibility, high embedded capacity, and reasonable resistance to geometric attacks on copyright protection and ownership identification. The FRT, DWT, and SVD schemes are used to study color image watermarking in the transform domain, as these domains recently proved to be robust [13], [24], [37], [39], [41], [45], [49].

The proposed watermark scheme uses FRT, DWT, SVD, PSO, and Arnold transform to provide robust color image watermarking in the transform domain. To provide additional security in the proposed watermark scheme, it uses Arnold transform with several iterations as a security key. Experimental results indicate that the proposed scheme provides high visual quality and show resistance to all geometric, non-geometric, and combinational attacks. It also provides imperceptibility, high embedded capacity, reasonable resistance to attacks on copyright protection, and ownership identification.

III. PRELIMINARIES

The proposed watermark scheme utilizes the FRT, DWT, SVD, PSO, and Arnold transform to increase the robustness, invisibility, embedded capacity, and security. The details of some basic concepts of FRT, DWT, SVD, PSO, and Arnold transform are provided in the following sub-sequent sections.

A. FINITE RIDGELET TRANSFORM (FRT)

Ridgelet transforms (RT) is the latest multi-resolution directional transform that effectively handles a line or super-plane singularities. The key idea is to map the singularity of the line into the singularity of the point using the Radon transform [43]. Compared with conventional wavelet transform, RT finds a further application on color image watermarking [39], [43]. Wavelets transform is an image part with point singularities, while RT is the edge-shaped part of the image. The finite ridgelet transform (FRT) is a version of a discrete ridgelet transforms (DRT), which provides a numerical precision because DRT requires low computational complexity. Besides, more directional information is included in the representation of ridgelets. The proposed watermarking scheme uses FRT to get high robustness, better invisibility, and high embedded capacity. In general, the FRT of an image is computed into two steps [39], [43]:

1. Calculate the DRT in the first step and then apply the one-dimensional DWT. The DRT can also be obtained by calculating a two-dimensional FFT and then applying 1D-IFFT in the thirty-two (32) radial directions of the radon method.
2. In the second step, apply a one-dimensional DWT on each output of DRT to get the finite ridgelet transform (FRT).

Fig. 2 shows the sailboat image and its ridgelet coefficients. The key benefit of FRT is that it can breaks down any N × N size image into its 2N × 2N ridgelet coefficients. This FRT property is used in the proposed watermarking scheme to increase the insertion capacity of the watermarking.

B. DISCRETE WAVELET TRANSFORM (DWT)

DWT is a very well-known digital tool that converts digital images from the spatial domain to the frequency/transform domain [1], [12], [24]. It is extensively used in several applications, such as digital image processing, as it provides more detailed representation and analysis of color images [32]. One of its applications in image processing includes the decomposition of images into frequency channels of constant bandwidth. DWT is divided into four different sub-bands or sub-images. Fig. 3 shows the various processing levels

FIGURE 2. Sailboat image (a) Sailboat image of size 512 × 512 pixels (b) its ridgelet coefficients of size 1024 × 1024 pixels.

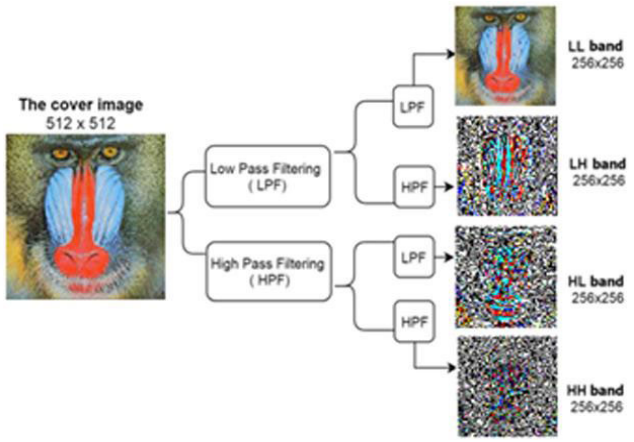


FIGURE 3. An example of a one-level transform of DWT.

of DWT. Approximate (LL), sub-image contains the average image value or consists of rough digital image description, whereas detailed sub-images (HL) consist of the edge area of the digital image [1], [24]. Generally, inserting watermark information in low-frequency (LL) or approximate sub-image will decrease the image quality easily, and inserting secret information in high-frequency (vertical, horizontal, diagonal) sub-images and the digital image does not cause any significant damage. Multilevel wavelet theory allows further decomposition to be carried out before the sub-images fulfill the watermark criterion [1]. DWT not only enhances the invisibility, but it also increases the level of security because of the spreading of hidden information over the whole image during the inverse transform.

C. SINGULAR VALUE DECOMPOSITION (SVD)

SVD is a powerful mathematical technique employed to provide matrix analysis tools [24]. SVD plays a key part in applications of image processing such as digital watermarking [14]. SVD breaks down the symmetric matrix to 3 sub-matrices to separate the singular values in terms of a diagonal matrix [5], [8], [46]. SVD is represented by

$$F_i = U_i \sum\nolimits_i V_i^T \tag{1}$$

Image F_i singular values (SV's) are stored in Σ_i of size $Z \times Z$. The matrix's diagonal values are still arranged in downward order. This diagonal value is called the SV of the F_i matrix. The SV's satisfy $\Sigma_i 1 \geq \Sigma_i 2 \geq \Sigma_i 3 \ldots \geq \Sigma_i Z \geq 0$. The less singular (lower order) reproduction of matrix F_i reduces the quality of the F_i matrix. Conversely, the accuracy of matrix F_i is not impaired by a slight difference in singular values. The highest Σ_i (SVs) not only hold much of an image's energy but also demonstrate the resistance to different attacks. Some of the benefits of SVD are as follows:

1. If there is tiny trouble in the image, the singular value (Σ_i) can remain unchanged.
2. The Σ_i can depict the image's intrinsic algebraic nature and brightness, the singular vectors (U and V^T) describe the image geometry.
3. SVD applied on the rectangle as well as square matrices and matrice sizes are variable like a square or rectangle.

In the presented scheme, to ensure the robustness, the secret watermark is inserted into the SVD domain's singular values (Σ_i).

D. FALSE POSITIVE PROBLEM (FPP)

The main shortcoming in the SVD-based scheme is an FPP. Since the SV (Σ_i) of the secret data is inserted in the cover image, the FPP arises when the recovered watermark image is identified without knowing the original watermark image [45]. Any citing image is used to extract a watermark image. Unusually, this scenario results in an uncertain situation, and therefore the problem of ownership can't resolve [51]. Anybody can use his/her citing image to claim the other image. Take two CI and WI images and do SVD operation for both of these images, $CI \gg U_{CI}\Sigma_{CI}V_{CI}^T$ and $WI \gg U_{WI}\Sigma_{WI}V_{WI}^T$.

If we transfer the singular values (Σ_i) among images CI and WI, we will get $U_{CI}\Sigma_{WI}V_{CI}^T \approx CI$ and $U_{WI}\Sigma_{CI}V_{WI}^T \approx WI$, respectively. The authors [32], [45], [51], [53] employ the reality that the SVD dimension can retain enough image information. In the proposed scheme, the watermark image's principal component (PC) is inserted in the cover image's singular value.

E. YCbCr COLOR SYSTEM

Color space or color system is a mathematical model and explains how the colors are represented in multimedia systems [32]. Minor transformation in colors produces a noticeable difference in visual perception [11]. YCbCr color space is one of computing's most famous color spaces and is widely used for image processing-based applications like digital video and image compression schemes, etc. YCbCr model reflects color with one luminance element (Y) and two chrominance elements Cb, Cr. By using the description relationship in the Eq. (2), the conversion from RGB to YCbCr color space can be achieved and vice-versa, defined mathematically as follows [11], [21], [32].

$$\begin{vmatrix} R \\ G \\ B \end{vmatrix} = \begin{vmatrix} +1.000 & -0.000 & +1.403 \\ +1.000 & -0.344 & -0.714 \\ +1.000 & +1.773 & +0.000 \end{vmatrix} \begin{vmatrix} Y \\ Cb \\ Cr \end{vmatrix} \tag{2}$$

$$\begin{vmatrix} Y \\ Cb \\ Cr \end{vmatrix} = \begin{vmatrix} +0.299 & +0.587 & +0.114 \\ -0.169 & -0.331 & +0.500 \\ +0.500 & -0.419 & -0.081 \end{vmatrix} \times \begin{vmatrix} R \\ G \\ B \end{vmatrix} + \begin{vmatrix} 0 \\ 128 \\ 128 \end{vmatrix} \tag{3}$$

Compared with the RGB color space, the YCbCr color space can ensure a stronger correlation, because the YCbCr color space is related to brightness, so the effect is better. The embedding of the watermark is carried out in luminance element (Y), as it reflects the image intensity; as long as it is lenient against various operations like JPEG compression, it is the right space for hiding data.

F. SECURITY FOR WATERMARK IMAGE

To provide additional security and high robustness in the proposed scheme, it uses Arnold transform with several iterations as a security key. Scrambling is employed during transformation to change an image into an entirely different form or worthless image, and it is a pre-processing process during the hiding of digital image information.

In the proposed scheme, if the secret key information, which is used during the scrambling process, is not known, no one can retrieve the secret watermark image. Furthermore, it also dismissive the local relations of its pixels, thus increases the strength of scrambling and provide additional security in the proposed watermark scheme.

1) ARNOLD TRANSFORM

In the proposed scheme, Arnold transform (AT) based scrambling is employed to transform the secret image before incorporating it in the cover image, so that the intruder cannot obtain the secret image data from the watermarked image. It can be seen in Fig. 4 that the scrambling of the image is modified to other forms by eliminating the spatial relationship of pixels. Besides, accurate restoration of a watermark is not possible without knowing the secret key used during scrambling. The two dimensional Arnold scrambling is expressed by the following Eq. (4):

$$\begin{pmatrix} k' \\ l' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} mod\ M \tag{4}$$

and k, l, k′, l′ = 0 to M−1, l′ + +. Here k and l are the pixel locations of the color image; k′ and l′ are the pixel positions after iterative computations of a scrambled image; whereas M indicates the size of the watermark image.

2) ANTI-ARNOLD TRANSFORM

In the proposed scheme, an anti-Arnold transform is employed to restore the image from the scrambled image, defined in Eq. (5).

$$\begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} k' \\ l' \end{pmatrix} mod\ M \tag{5}$$

and k, l, k′, l′ = 0 to M−1, l′ + +. Here k and l are the pixel locations of the restored color image; k' and l' are the pixel position of a scrambled image; whereas M indicates the size of the watermark image.

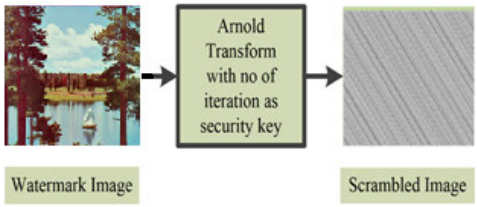


FIGURE 4. Scrambling process.

G. PARTICLE SWARM OPTIMIZATION (PSO)

PSO is a population-based adaptive optimization method that finds the optimal solution employing a particle population [27]. In a PSO population, every feasible candidate solution is regarded as a bird in the search domain. The PSO is built using two-dimensional space by simulation of birds flocking [31]. After that, if a bird moves in a specific order, then every bird in the community attempts to pursue it and get the same destination.

Some attractive features of PSO are that it does not need to optimize any functional gradient knowledge, it only uses basic mathematical operators and is conceptually very simple [56]. It is used to solve various problems of optimization in different applications like training on neural networks and minimizing functions [57]. In PSO, a particle is defined as a population of individuals. Additionally, each particle features a position X, a velocity V, and a fitness value. The particles change their speed throughout in different iterations, each particle in the community moves quickly towards its own best individual known as Pbest and Pbi [58], [59]. The processes depend on their own flight experience and their fellow flight experience [58]. In the current population, particles having the highest value among all Pbest (Pbi) is called Gbest (Pgbest) [57]–[60].

This kind of value (each swarm-associated particle) is slowly increased and reached as iterations progress towards an optimum solution. Therefore, it is obvious that all other particles move towards it if any particle has a better solution. Designing any optimization problem with PSO requires an appropriate population size, several design variables, fitness function (FF), and termination criteria [59]. In the first generation, the population started using random numbers. All numbers in the population can be used as a feasible solution to the optimization problem [58]. The fitness function (FF) is used to test each single-generation solution and to check the best solution. Thus, the PSO algorithm modifies all the solutions to the current generation. A new set of solutions in the PSO led to subsequent population growth [60]. The PSO algorithm compares the performance of each next-generation solution with the current corresponding solution, and if a better solution is found then replaces it, otherwise, keep it the same.

The proposed scheme of this article uses a particle swarm to find the right solution based on the PSO algorithm in digital image watermarking scheme. Each particle in PSO is a solution to the candidate's problem. The numbers of

particles denoted by m are used in this article to initialize the population. The best individual position of the i^{th} particle search space $Pbi = (pbi_1, pbi_2 \ldots . pbi_D)$, and the best global position of $pgbest = (pg_1, pg_2 \ldots . pg_D)$, among all Pbi.

$$V_{id}^{m}(y+1) = I_w \times V_{id}^{m}(y) + C_1 r_1 \left(Pb(i) - X_{id}^{m}(y)\right) + C_2 r_2 \left(P_{gbest} - X_{id}^{m}(y)\right) \quad (6)$$

$$X_{id}^{m}(y+1) = X_{id}^{m}(y) + V_{id}^{m}(y+1) \quad (7)$$

PSO employs Eq. (6) and Eq. (7) to update the velocity of each particle in the t^{th} iteration ($t = 1, 2, 3 \ldots$) as well as its position [27]. Where $V_{id}^{m}(y)$, X_{id}^{m} is the velocity, and position of the particles at i^{th} iteration, Pb(i), and P_{gbest} are defined as the personal best position and the global best position, respectively. The r_1, r_2 indicates random numbers, and their values vary from 0 and 1, while C_1, C_2 represent acceleration factors, and I_w inertia weight is responsible for the convergence of the proposed scheme.

IV. PROPOSED WATERMARKING SCHEME

In the proposed scheme, the nominated color cover image [CI_{RGB}] and the color watermark image [WI_{RGB}] are converted to the YCbCr color space from the RGB color space using Eq. 2, and the (Y) luminance component of the YCbCr color space is selected for the insertion of a watermark. Arnold scrambling (AT) is employed for encrypting the watermark image to provide additional security before inserting a watermark into the cover image.

The Y component of the original image is amended by the principal component (PC) of the scrambled watermark image using an optimized strength factor. In the next phase, FRT is applied to the Y component of the original image to obtain ridgelet coefficients. Then one-level DWT is applied to the ridgelet coefficients of the original image, resulting in different multi-resolution subbands or sub-images. These include approximate, vertical, horizontal, and diagonal sub-images. Among them, low-frequency sub-images only belong to approximate (LL) sub-image wavelet coefficients, and other (LH, HL, HH) sub-images belong to high-frequency sub-images. Both HH and the HL sub-images are emitted to separate the most suitable explanation of these high-frequency sub-images. Because the HH sub-image contains image structure and edge information, and the HL sub-image is more susceptible to the human visual system (HVS). Therefore, the HL sub-image is considered to be the most appropriate among all high-frequency sub-images (LH, HH) for the insertion of a watermark. The proposed scheme uses the HL sub-image for watermark insertion while keeping other bands intact to maintain the edge information of the image and apply SVD to the HL sub-image. Finally, using the optimized strength factor, the principal components (PC) of the encrypted watermark image are modified by the cover image to get the watermarked image. The proposed scheme is divided into two steps; the first step is the embedding of a watermark and the second step is the extraction of a watermark. The watermark embedding steps are further divided into three phases which are; (a) pre-processing, (b) embedding of the watermark, and (c) post-processing. The methodology of the proposed scheme is discussed in the following sub-sequent sections. Furthermore, the process of embedding and extracting a watermark from the color image is shown in the form of block diagrams in Fig. 5 and Fig. 6, respectively.

A. WATERMARK EMBEDDING ALGORITHM

Assume, $CI_{RGB} = g(x_1, y_1)$ denotes the original color cover image of dimensions 512 × 512 pixels, where $g(x_1, y_1)$ is the image intensity at the point (x_1, y_1). Similarly, assume $WI_{RGB} = g(i_1, j_1)$ denotes the color watermark image of dimensions 512 × 512 pixels, where $g(i_1, j_1)$ denotes the image intensity at the point (i_1, j_1) to be embedded in the original color image. The watermark insertion process is based on multiple decompositions which are FRT, DWT, and SVD. This section explains the procedure of inserting a watermark image in the proposed watermark scheme. The phases of the inserting watermark image are as follows:

The proposed scheme for embedding a watermark in the color image is described in three phases; 1) pre-processing for watermark embedding, 2) watermark embedding, and 3) post-processing after watermark embedding. The detail of these phases is provided as follows:

a) Pre-processing phases

Phase E1: The conversion of the given color cover image (CI_{RGB}) and color watermark image (WI_{RGB}) from the RGB color system to YCbCr is carried in the first stage using Eq. (2), which leads to channels CI_Y, CI_{Cb}, CI_{cr}, and WI_Y, WI_{Cb}, WI_{Cr}, respectively. The luminance channel (CI_Y) is selected for embedding the watermark in the color image because of its higher intensity than the other two chrominances, defined as follows:

$$[CI_Y, CI_{Cb}, CI_{Cr}] = YCbCrConversion(CI_{RGB}) \quad (8)$$

$$[WI_Y, WI_{Cb}, WI_{Cr}] = YCbCrConversion(WI_{RGB}) \quad (9)$$

Phase E2: In this phase, the proposed watermark scheme apply n times Arnold scrambling on the WI_Y watermark (WI_{RGB}) image channel to obtain the WI'_Y scrambled watermark image in terms of an encrypted watermark. The private key (k) is applied to the watermark image using Arnold transform to improve the robustness and protection of the watermarked image. The length of the private key k = 25 is considered during the watermark insertion process.

$$WI'_Y = AT(WI_Y) \quad (10)$$

Phase E3: In this phase, the scrambled watermark image WI'_Y is decomposed by applying a DWT to obtain LL'_{WI}, LH'_{WI}, HL'_{WI}, HH'_{WI} sub-images, as defined in Eq. (11). The proposed scheme uses the horizontal sub-image (HL'_{WI}) to perform SVD to achieve the $U(HL'_{WI})$, $\Sigma(HL'_{WI})$, and $V^T(HL'_{WI})$ matrices, as defined in Eq. (12).

$$[LL'_{WI}, LH'_{WI}, HL'_{WI}, HH'_{WI}] = DWT\left(WI'_Y\right) \quad (11)$$

$$[U\left(HL'_{WI}\right)\Sigma\left(HL'_{WI}\right)V^T\left(HL'_{WI}\right)] = SVD\left(HL'_{WI}\right) \quad (12)$$

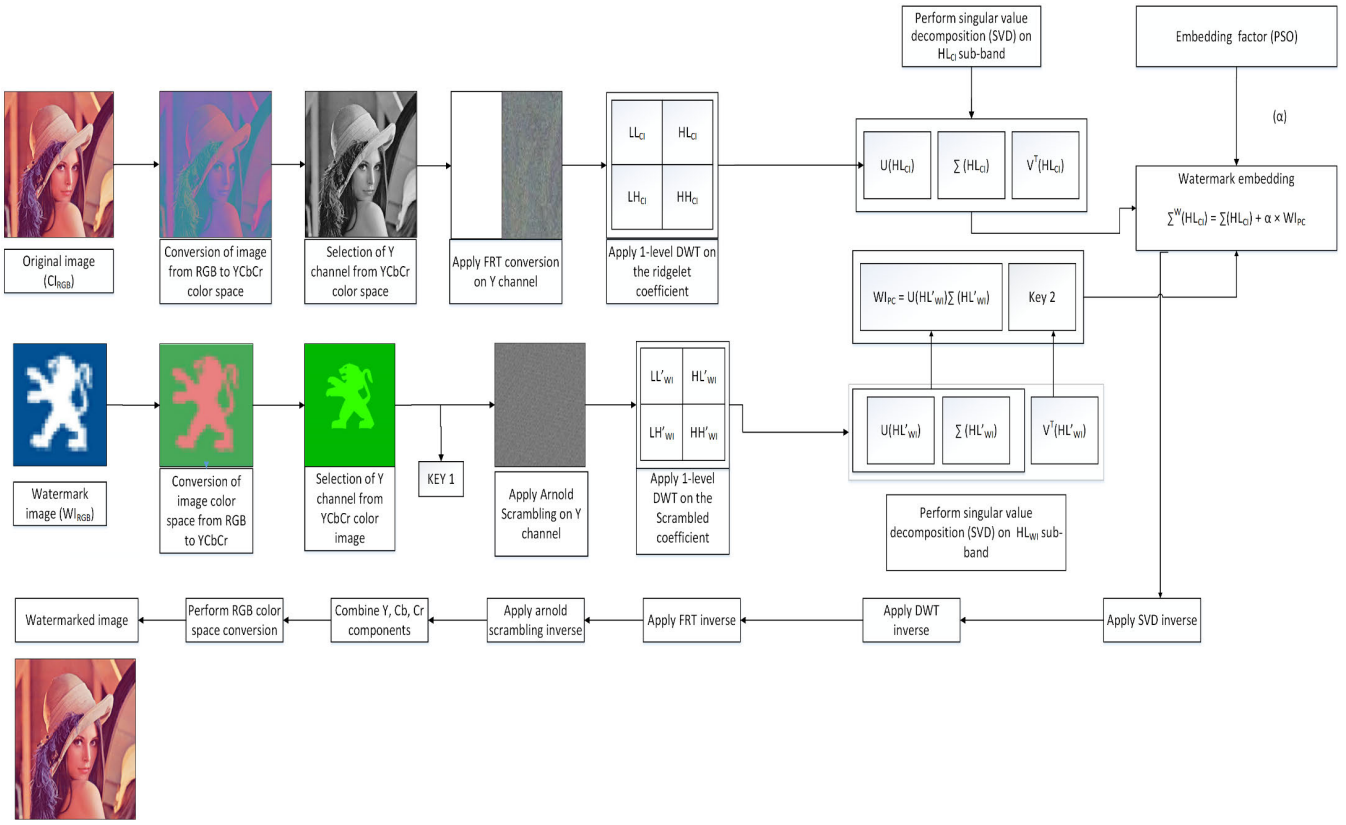


FIGURE 5. Watermark embedding process of the proposed watermark scheme.

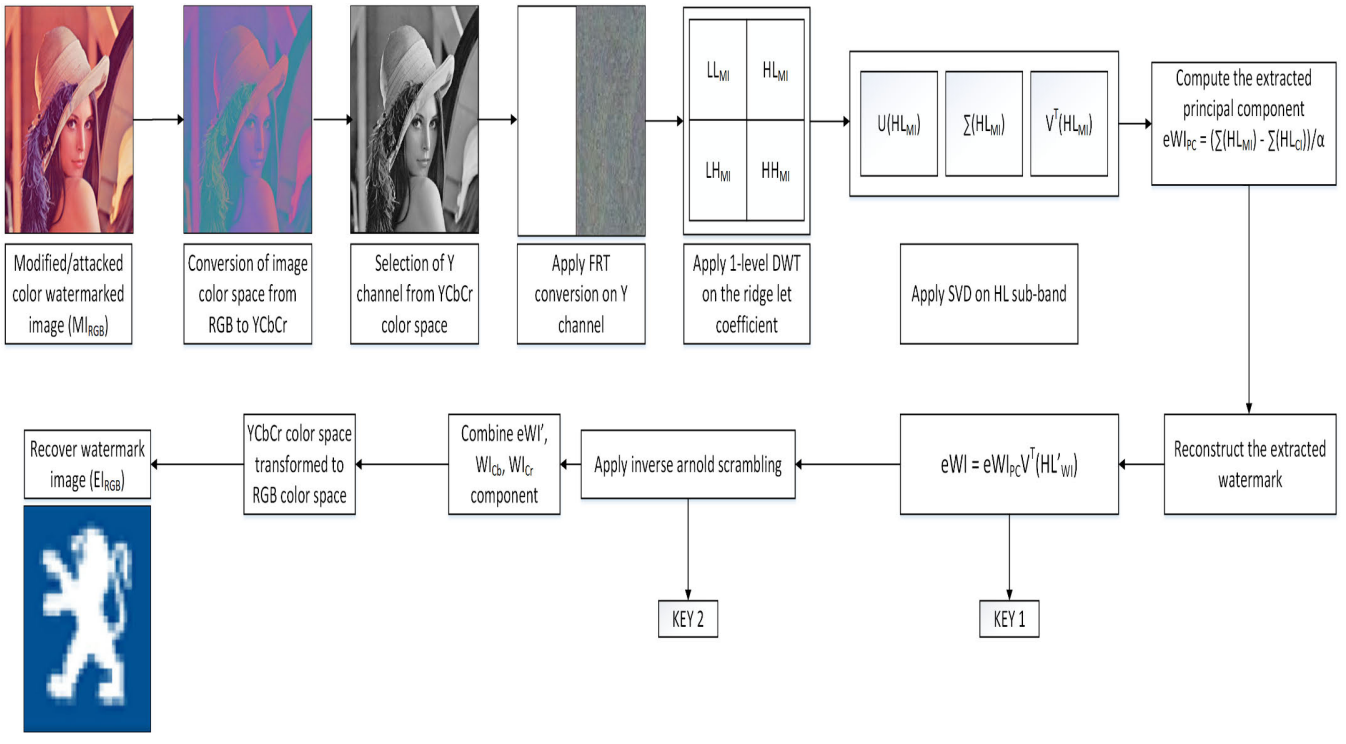


FIGURE 6. Diagram of the watermark extraction process used by the proposed watermark scheme.

where $\Sigma(HL'_{WI})$ denotes the singular value matrix, $U(HL'_{WI})$ denotes the left singular vector, and $V^T(HL'_{WI})$ denotes the right singular vector. The $U(HL'_{WI})$ and $\Sigma(HL'_{WI})$ matrices are inserted in the color cover image using PC, while in the

extraction stage, the matrix $V^T(HL'_{WI})$ is held as a secret key to reconstruct the watermark image.

Phase E4: In this phase, the FRT conversion is applied to the color cover image of the CI_Y channel to obtain the ridgelet coefficient of the color cover image which extracts the edge coefficients, defined as follows:

$$RC_{CI} = FRT\ (CI_Y) \tag{13}$$

Phase E5: In this phase, one-level DWT is applied on the RC_{CI} to get four separate frequency sub-images (approximations), which are LL_{CI} sub-image, and (vertical, horizontal, diagonal) three LH_{CI}, HL_{CI}, HH_{CI} sub-images. The proposed watermark scheme uses a horizontal (HL_{CI}) sub-image for the insertion of the watermark in the color image, which is defined as follows:

$$[LL_{CI}, LH_{CI}, HL_{CI}, HH_{CI}] = DWT\ (RC_{CI}) \tag{14}$$

Phase E6: In this phase, the high-low (HL_{CI}) frequency sub-image from the first decomposition level of the DWT is selected, and SVD is applied to it to obtain the $U(HL_{CI})$, $\Sigma(HL_{CI})$, and $V^T(HL_{CI})$ matrices as defined in Eq. (15). $\Sigma(HL_{CI})$ represents singular values, in which information about the encrypted watermark is inserted.

$$[U\ (HL_{CI})\ \Sigma\ (HL_{CI})\ V^T\ (HL_{CI})] = SVD\ (HL_{CI}) \tag{15}$$

b) Watermark embedding phases

Phase E7: In this phase, the principal component (PC) WI_{PC} of the scrambled watermark channel is calculated by multiplying the left singular $U(HL_{WI})$ vector with the singular value $\Sigma(HL_{WI})$ matric (found in phase E3), defined as follows:

$$WI_{PC} = U(HL'_{WI})\Sigma\left(HL'_{WI}\right) \tag{16}$$

Phase E8: In this phase, the principal component of the color watermark image found in phase E7 is multiplied with embedding strength alpha (α). After that, resultant values are added to the singular values obtained in step E6. This phase is mathematically defined as follows:

$$\Sigma^w\ (HL_{CI}) = \Sigma\ (HL_{CI}) + \alpha \times WI_{PC} \tag{17}$$

where $\Sigma(HL_{CI})$ and $\Sigma^w(HL_{CI})$ denote the singular values of cover and watermarked images, respectively. Alpha (α) denotes the strength factor (SF) that handles the trade-off between invisibility and robustness.

c) Post-processing phases

Phase E9: In this phase, the inverse SVD (ISVD) is applied to obtain the scrambled wavelet form HL'_{WI}. The first level inverse DWT (IDWT) is applied on a modified HL'_{WI} sub-image and the other three LL'_{WI}, LH'_{WI}, and HH'_{WI} sub-images to obtain the altered ridgelet coefficients of WI'_Y component of the color watermark image as defined in Eq. (19).

$$HL'_{WI} = ISVD[U\ (HL_{CI})\ \Sigma'\ (HL_{CI})\ V^T\ (HL_{CI})] \tag{18}$$

$$WI'_Y = IDWT[LL_{CI}, LH_{CI}, HL_{CI}, HH_{CI}] \tag{19}$$

Phase E10: In this phase, anti-FRT (IFRT) is applied to altered ridgelet coefficients to obtain an amended CI'_Y watermarked luminance component that is defined as follows:

$$CI'_Y = IFRT\ (RC_{CI}) \tag{20}$$

Phase E11: In this phase, the anti-Arnold scrambling is performed on CI'_Y component to acquire unscrambled watermarked luminance part CI_Y^N.

Phase E12: In this phase, the watermarked CI_Y^N (luminance) is integrated with other parts CI_{Cb} and CI_{Cr} that are obtained in phase E1, and transformed a color system from YCbCr to RGB using Eq. (3) to acquire the watermarked color image MI_{RGB}, defined as follows:

$$MI_{RGB} = RGBConversion\left(CI_Y^N, CI_{Cb}, CI_{Cr}\right) \tag{21}$$

B. WATERMARK EXTRACTION ALGORITHM

The method of watermark extraction is the opposite of the watermark insertion phase, where the inserted watermark is obtained by employing the relevant data that is only available to the legitimate user acquired by embedding the side data ($V^T(HL'_{WI})$), scaling factor-alpha (α), WI_{Cb}, and WI_{Cr}. The modified watermarked image is transformed from the RGB to the YCbCr color system in the first phase of watermark extraction. After that FRT and DWT are applied to the Y component of the YCbCr color space respectively, and horizontal sub-band (HL) is selected, and SVD is applied to it. The singular value matrix gained by using a color cover image is subtracted from the singular value matrix gained by using a color watermarked image, and the strength factor is divided by the gained result to obtain the extracted principal components. The extracted principal components are multiplied with side data to gain the watermarked principal components. Finally, anti-SVD, anti-DWT, and anti-FRT are applied to obtain the recovered watermark and extracted watermark information (refer to Fig. 7). The watermark extraction steps are also divided into three phases: a) pre-processing, b) watermark extraction, and c) post-processing. The details of these phases are provided as follows:

a) Pre-processing phases of watermark extraction

Phase X1: In this phase, the modified/attacked watermarked image (MI_{RGB}) is transformed to YCbCr from the RGB color system using Eq. (2), and the Y component is used for watermark extraction. This conversion of the watermarked image (MI_{RGB}) produces three components which are denoted by MI_Y, MI_{Cb}, and MI_{Cr}. This process can be defined mathematically as follows:

$$[MI_Y, MI_{Cb}, MI_{Cr}] = YCbCrConversion\ (MI_{RGB}) \tag{22}$$

Phase X2: In this phase, FRT is applied to the luminance component (MI_Y) of attacked watermarked color image to obtain ridgelet coefficients. It can be defined as follows:

$$RC_{MI} = FRT\ (MI_Y) \tag{23}$$

Phase X3: In this phase, one-level DWT is applied to the ridgelet coefficients of the MI_Y component to obtain different

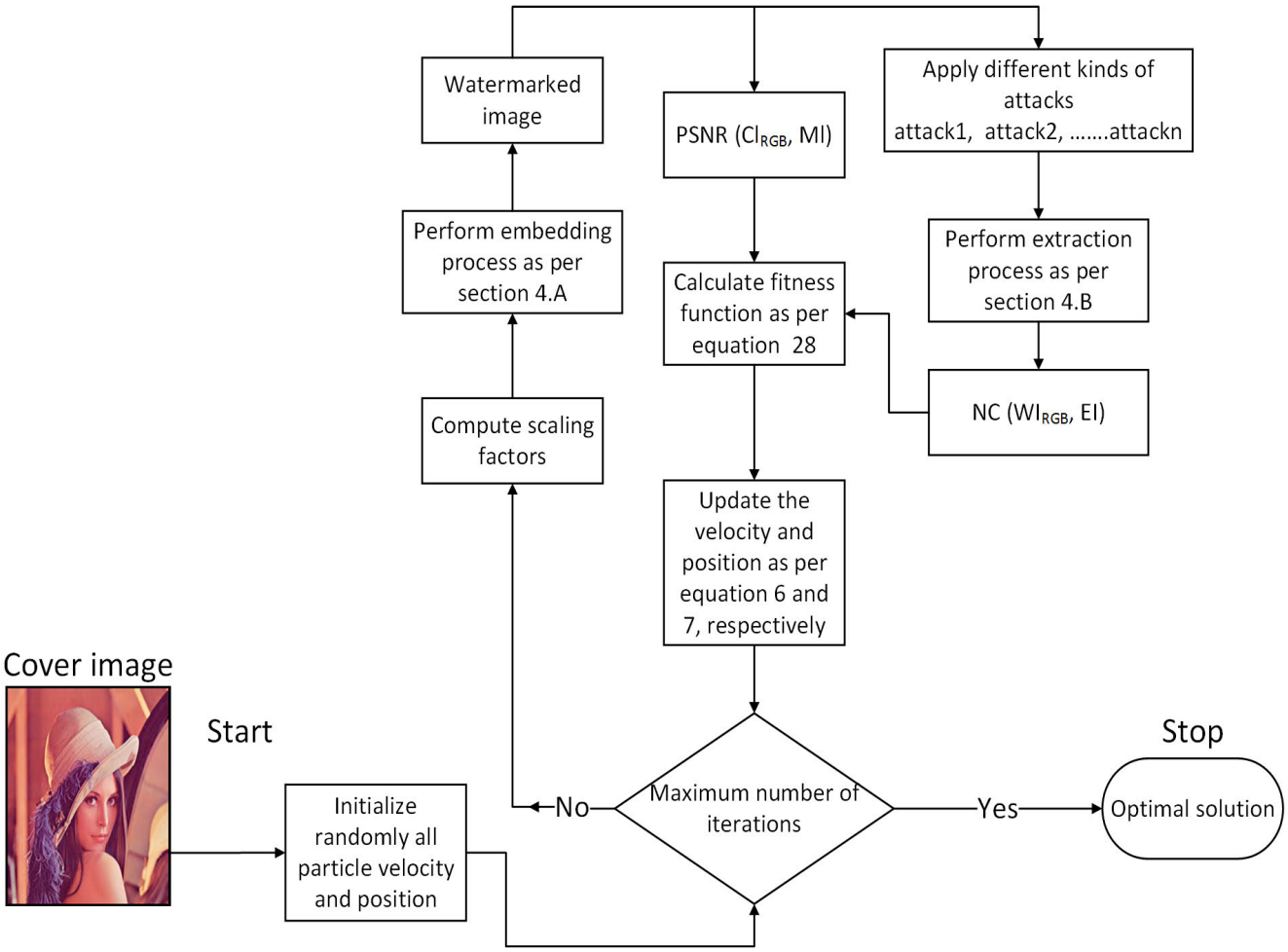


FIGURE 7. Flow chart of the PSO to optimize scaling factors for image watermarking of the proposed scheme.

wavelet sub-images denoted by LL_{MI}, LH_{MI}, HL_{MI}, and HH_{MI}. The HL_{MI} sub-image is used for the extraction of a watermark image, defined as follows:

$$[LL_{MI}, LH_{MI}, HL_{MI}, HH_{MI}] = DWT\,(RC_{MI}) \quad (24)$$

Phase X4: In this phase, SVD is applied to the horizontal wavelet sub-image HL_{MI}, and the resulting matrices U, Σ, and V^T are obtained. It can be defined as follows:

$$[U\,(HL_{MI})\,\Sigma\,(HL_{MI})\,V^T\,(HL_{MI})] = SVD\,(HL_{MI}) \quad (25)$$

b) Watermark extraction phases

Phase X5: In this phase, the extracted principal components are computed using embedded watermark image $\Sigma(HL_{MI})$, which is obtained in step X4. This procedure is defined as follows:

$$eWI_{PC} = 1/\propto(\Sigma(HL_{MI}) - \Sigma(HL_{CI})) \quad (26)$$

where eWI_{PC} denotes the extracted PC and the coefficient $\Sigma(HL_{CI})$ is obtained from the watermark insertion of phase E6. The symbol alpha (α) is the strength factor (SF) that handles the trade-off between invisibility and robustness.

Phase X6: In this phase, the extracted eWI_{PC} principal components are multiplied with the right singular $V^T(HL'_{WI})$ vectors (kept as a hidden key), to reconstruct the extracted watermark luminance component. This phase can be defined as follows:

$$eWI = eWI_{PC}V^T(HL_{WI}) \quad (27)$$

c) Post-processing phases

Phase X7: In this phase, the anti-Arnold scrambling is applied to the luminance component (eWI).

Phase X8: In this phase, the extracted luminance component (eWI′) is combined with other components (i.e. WI_{Cb} and WI_{Cr}), which are obtained during the embedding phase.

Phase X9: In this phase, the resultant image in the YCbCr color system is converted into the RGB color system to obtain the EI_{RGB} color extracted watermark image.

C. OPTIMIZATION OF SCALING FACTORS USING PSO

The visual quality and robustness of the watermarking scheme mainly depend on the strength factor (α). A slight increase in the strength factor value provides better perceptual

quality for the watermarked image, but it decreases the quality of the recovered watermark image. Similarly, a large value of the strength factor (α) results in a reduced visual quality but gives greater robustness. Therefore, it is necessary to seek the best value of the strength factor, which strikes a balance between invisibility and robustness for each value embedded with singular values. The strength factors are selected manually in most existing research of image watermarking, without realizing that the strength factor depends on the image. In other words, each image requires a different strength factor value to deliver the maximum possible visual quality and robustness. By using bio-inspired optimization schemes, it is also possible to solve the problem of finding the best strength factor to overcome the clash between invisibility and robustness. For this purpose, the proposed watermark scheme uses PSO to automatically find the strength factor to insert the watermark's principal component (PC) in the singular value of the cover image's SVD decomposition.

In the optimization procedure of the proposed watermark scheme, a single objective function-based PSO is used to obtain the strength factor (SF). The value of the strength factor is analyzed for each iteration of the PSO after applying different attacks. The nearest optimum strength factor is given after the iterative process of PSO. The methodology of the PSO process is shown in Fig. 7 for determining the optimal strength factor for α. To start optimization, PSO employs randomly generated preliminary solutions generated between 0 and 1 by a random number generator. As illustrated in Fig. 7, in the 1st iteration, the proposed scheme arbitrarily initializes the total position of particles in the search area. Every single particle moves continuously inside the search space. The watermarked image robustness and visual quality should be measured to develop the proper fitness function. The fitness function of the PSO used by the proposed scheme can be defined as follows [27]:

$$f = \frac{n}{\left(PSNR + \sum_{i=1}^{n} NC_i\right)} \tag{28}$$

where f represents the fitness function, PSNR is used to calculate the invisibility among the cover and the watermarked image, and NC_i is used to calculate the resemblance among the watermark and the restored watermark images. Whereas n denotes the total amount of different operations, carried out on a watermarked image during the optimization of the PSO strength factor. When the watermark is inserted into the cover image, the PSNR value is measured during each iteration; common attacks check the robustness of the watermarked image and measure the NC value as shown in Fig. 7. The main process of the PSO can be divided into two steps namely ''watermark embedding and watermark extraction'' that are used by the proposed watermark scheme. Besides, all other steps of process and decision making play an important part in PSO for finding the best strength factor.

Furthermore, the considered attacks are JPEG compression with reliability or a quality factor 30 and 90, median filtering with window sizes of 3 to 3 and 5 to 5, adding 0.02 and 0.1 density salt and pepper noise, added mean of 0 and deviation of 0.01 with Gaussian noise of 0.03, PSO uses gamma corrections with a gamma value of 0.5, cropping values of 0.25 and 0.50, and scaling values of 0.25 and 4.0 to test the optimal strength factor and calculate the target value. The fitness function of the PSO used to get the optimal embedding coefficient matrices is defined in Eq. (28). To find the best value of the strength factor (α), different values of the PSO parameters (i.e. the particle size m, acceleration factors C1, C2, the highest amount of iterations factor T, and inertia weight $I_{w)}$ used by the proposed watermark scheme are shown in Table 2.

TABLE 2. Parameters of the PSO that are used by the proposed watermark scheme.

Parameter	m	I_w	C_1	C_2	T
Value	30	0.8	2	2	50

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

Generally, the effectiveness of the proposed watermark scheme is determined by its imperceptibility, robustness, embedded payload, and security. The proposed watermark scheme is primarily focused on color images, and it's important to match this scheme with other similar schemes [4]–[6], [21] as comparison schemes to prove the dominance of the proposed watermark scheme in terms of the invisibility and robustness. It is implemented on a laptop with a 1.3 GHz CPU, 8 GB memory, Microsoft Windows 10 (64-bit version), and MATLAB R2017a (64-bit version). The extensive experiments are performed to examine the effectiveness of the proposed watermark scheme using a variety of standard images.

A. EXPERIMENTAL SETUP

The performance evaluation of the proposed watermark scheme is performed using different standard color images like Lena, Mandrill, Pepper, TTU, F16, and Sailboat, and the same images are used for a comparative evaluation of the proposed watermark scheme. These images are taken from the different databases namely USC-SIPI [29] and CVG-UGR [30]. The resolution of each color image is 512×512×3 pixels that are used as cover images, as shown in Fig. 8 (a-f).

The proposed watermark scheme also uses two 512×512×3 resolution images as watermark images, as shown in Fig. 8 (g-h).

B. PERFORMANCE PARAMETERS

Three performance evaluation metrics namely PSNR, SSIM, and normalized cross-correlation (NCC or NC) are used to analyze the performance of the proposed watermark scheme. The PSNR is the best-known image quality metric that is used to assess the quality of watermarking schemes and it is

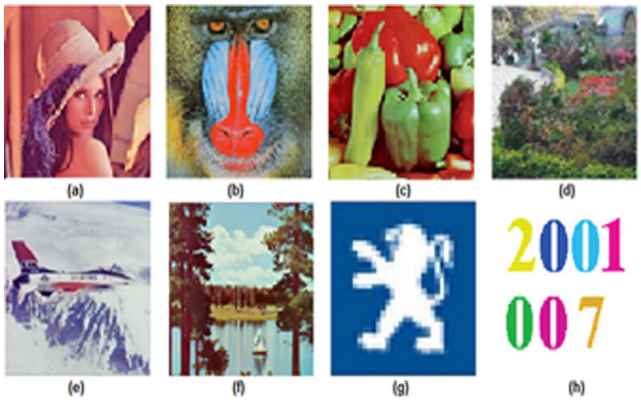


FIGURE 8. Cover images: (a) Lena, (b) Mandrill, (c) Peppers, (d) TTU, (e) F16, and (f) Sailboat; Watermark images: (g) Peugeot Logo, and (h) 8-color image.

mathematically defined as follows:

$$PSNR\,(CI, MI) = 10 \times \log 10 \frac{255^2}{\frac{1}{PQ}\sum_{i=1}^{P}\sum_{j=1}^{Q}\{CI(i,j) - MI\,(i,j)\}^2} \quad (29)$$

where (i, j) denotes the image coordinates, CI denotes the color cover image, MI denotes the watermarked color image, and P, Q denotes the total number of rows and columns of the image. The greater the value of PSNR, the higher the resemblance between the watermarked image and the cover image. For the invisibility capability, the structural similarity image index (SSIM) is an image quality assessment parameter that is also used to check the resemblance between both the color cover image (CI) and the watermarked color image (MI) [11]. Besides, SSIM aims to enhance conventional schemes such as PSNR, and it turns out to be inconsistent with the human visual system (HVS) [33]. The SSIM is mathematically defined as follows:

$$\mathrm{SSIM\,(CI, MI)} = \mathrm{l\,(CI, MI)} \times \mathrm{c\,(CI, MI)} \times \mathrm{s\,(CI, MI)} \quad (30)$$

where,

$$\mathrm{l\,(CI, MI)} = \frac{2\mu_{\mathrm{CI}}\mu_{\mathrm{MI}} + \mathrm{C1}}{\mu_{\mathrm{CI}}^2 + \mu_{\mathrm{MI}}^2 + \mathrm{C1}} \quad (31)$$

$$\mathrm{c\,(CI, MI)} = \frac{2\sigma_{\mathrm{CI}}\sigma_{\mathrm{MI}} + \mathrm{C_2}}{\sigma_{\mathrm{CI}}^2 + \sigma_{\mathrm{MI}}^2 + \mathrm{C_2}} \quad (32)$$

$$s\,(CI, MI) = \frac{\delta_{CI_{MI}} + C_3}{\sigma_{CI}\sigma_{MI} + C_3} \quad (33)$$

where CI, MI denote the cover and watermarked color images, σ, μ denote the standard deviation and mean, and C_1, C_2, C_3 are three positive constants that are used to prevent a zero denominator, respectively. In the Eq. (31), the luminance (l) measures the proximity of the average luminance (μ_{CI} and μ_{MI}) of two images.

In Eq. (32), c denotes a contrast that measures the proximity of the contrast of the two images while standard deviation σ_{CI} and σ_{MI} are used to measure the contrast. In Eq. (33), s denotes a structure that calculates the correlation coefficient between two CI and MI images. The SSIM is a number lying in [0, 1], and the values near to 1 mean the images are more similar.

Typically a better PSNR or SSIM implies that the watermarked image is quite near to the original image, which suggests that the watermarking scheme is more effective in terms of invisibility [7].

Besides, the proposed watermark scheme also uses normalized cross-correlation (NCC or NC) between the original watermark ($\mathrm{WI_{RGB}}$) and the extracted watermark ($\mathrm{EI_{RGB}}$) to evaluate the robustness of the watermark. Usually, the NC value ranges from 0 to 1. The extracted image is closely similar to the embedded image when the NC value is nearer to 1, which means that the watermark is highly robust. The NCC is mathematically defined as follows:

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} WI\,(x,y) \times EI\,(x,y)}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} WI^2\,(x,y)}\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} EI^2\,(x,y)}} \quad (34)$$

where WI and EI represent the watermark, extracted watermark, (x, y) represents the pixel range, and (M, N) denotes the original watermark image rows and the columns, respectively. If the value of NCC is more than or close to 0.75, the watermark can usually be valid, otherwise, it may be invalid [34].

C. EXPERIMENTAL RESULTS

The experimental results of the proposed watermark scheme are divided into two phases; the first phase provides detail to assess the watermark's invisibility using various watermark images, while the second phase provides detail to evaluate the robustness of the proposed watermark scheme by applying different operations to the watermarked color image.

The proposed watermark scheme is adaptive with high embedded capacity as compared with other considered schemes. The extensive experiments are performed using six standard 24-bit color images of resolution 512×512×3 pixels, as shown in Fig. 8(a-f) adopted as cover images and two standard 24-bits color images of resolution 512 × 512×3 shown in Fig. 8(g-h) as watermark images.

The performance comparison of the proposed watermark scheme is performed with different state-of-the-art color image watermarking schemes [4], [7], [11], [20], [21], [28]. The robustness of the proposed watermark scheme is assessed by applying different image manipulation attacks such as non-geometric and geometrical attacks. The PSO is used to optimize the image quality metric strength and its details are shown in Fig. 11.

D. INVISIBILITY MEASUREMENT

The invisibility or visual quality implies that human eyes are unable to see the hidden image of the embedded watermark in the cover image and the embedded watermark could not

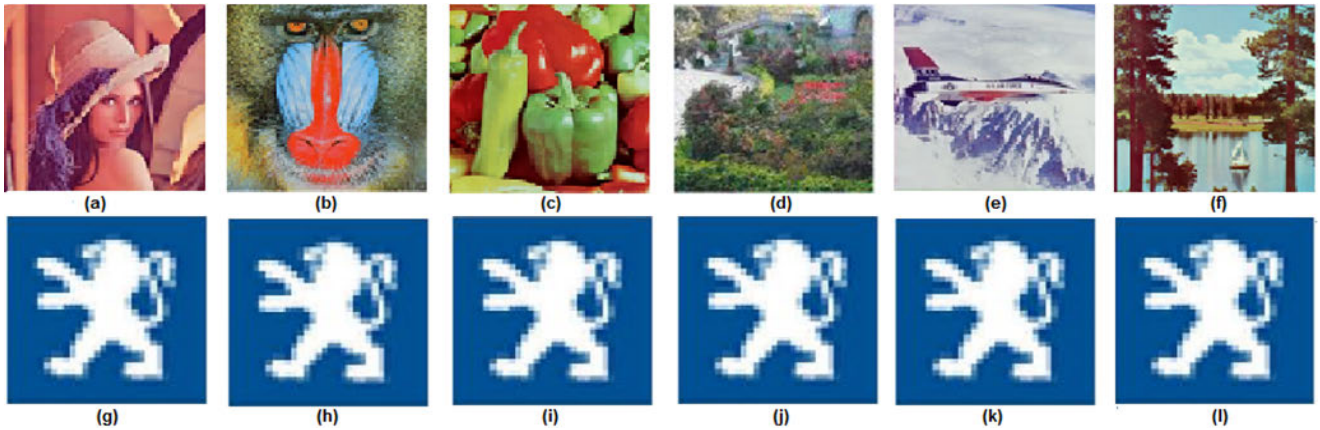


FIGURE 9. (a) Watermarked Lena image, (b) Watermarked Mandrill image, (c) Watermarked Peppers image, (d) Watermarked TTU image, (e) Watermarked F16 image, (f) Watermarked Sailboat image; (g) extracted watermark from (a), (h) extracted watermark from (b), (i) extracted watermark from (c), (j) extracted watermark from (d), (k) extracted watermark from (e), (l) extracted watermark from (f).

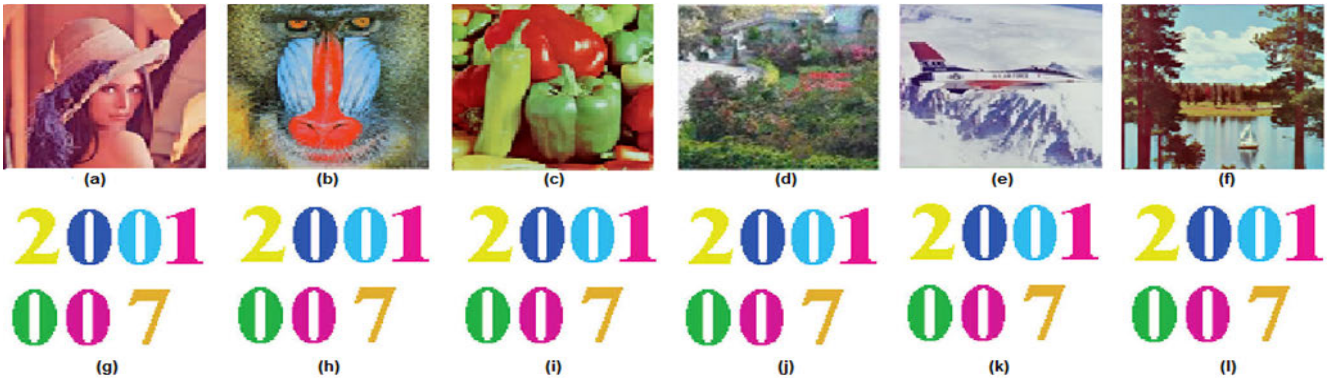


FIGURE 10. (a) Watermarked Lena image, (b) Watermarked Mandrill image, (c) Watermarked Peppers image, (d) Watermarked TTU image, (e) Watermarked F16 image, (f) Watermarked Sailboat image; (g) extracted watermark from (a), (h) extracted watermark from (b), (i) extracted watermark from (c), (j) extracted watermark from (d), (k) extracted watermark from (e), (l) extracted watermark from (f).

affect the image's visual appearance. The watermark impact factor (α) plays a key role to assess the performance of the watermarking scheme. To test the visual quality of the embedded watermark, we have inserted the watermark images from Fig. 8 (g-h) into the cover images in Fig. 8 (a-f). Fig 9 (a-f) and Fig. 9 (a-f) display the resulting watermarked images after hiding the watermark images. The color images are shown in Fig. 9 (g-l) and Fig. 10 (g-l) shows the extracted watermark images.

The experimental analysis of the proposed scheme in terms of PSNR, SSIM, and NCC is provided in Table 3. In Table 3, insert the Peugeot logo and 8-color watermark images in the cover images of Lena, Mandrill, Peppers, TTU, F16, and Sailboat, respectively. According to the experimental details provided in Table 3, the PSNR values are greater than 40dB, and SSIM values are close to 1. It is agreed that the two images (watermarked and cover images) are said to be identical if their PSNR value is greater than 40dB or their SSIM value is closer to 1 [11]. Thus, the watermarked image and the cover image are therefore identical, which shows the robust performance of the proposed watermark scheme in terms of the visual quality of the watermarked image and extracted watermark image.

TABLE 3. Performance analysis of the proposed watermark scheme in terms of the PSNR, SSIM, and NCC parameters.

Cover image	Watermark image	PSNR	SSIM	NCC
Lena	Peugeot Logo	45.5728	0.9990	1.0000
Mandrill	Peugeot Logo	45.3375	0.9986	1.0000
Pepper	Peugeot Logo	45.6712	0.9976	1.0000
TTU	Peugeot Logo	45.3418	0.9980	1.0000
F16	Peugeot Logo	45.0533	0.9984	1.0000
Sailboat	Peugeot Logo	45.2016	0.9970	1.0000
Lenas	8-color image	45.0325	0.9992	1.0000
Mandrill	8-color image	45.5578	0.9989	1.0000
Pepper	8-color image	45.9059	0.9983	1.0000
TTU	8-color image	45.3345	0.9988	1.0000
F16	8-color image	45.5635	0.9990	1.0000
Sailboat	8-color image	45.4088	0.9975	1.0000

To assess the performance of the proposed watermark scheme, its performance comparison is performed with different state-of-the-art image watermarking schemes by considering optimization algorithms [4]–[6], [21]

TABLE 4. Comparative analysis in terms of PSNR, SSIM, and NCC values of the proposed watermark scheme with existing watermarking schemes (using an optimized algorithm) (bold values of the performance evaluation parameters indicate the best performances).

Method	Proposed scheme			Method [4]			Method [5]			Method [6]			Method [21]		
Images/ Metric	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC
Lena	**45.572**	**0.999**	**1.000**	36.74	0.99	1.00	43.032	N.A.	1.000	35.92	0.98	1.00	39.01	0.99	0.99
Mandrill	**45.337**	**0.998**	**1.000**	35.05	0.98	0.99	40.033	N.A.	1.000	35.67	0.96	1.00	39.03	0.99	0.99
Pepper	**45.671**	**0.997**	**1.000**	36.59	0.99	0.99	40.000	N.A.	1.000	35.23	0.96	1.00	38.99	0.99	0.99
Sailboat	**45.201**	**0.997**	**1.000**	36.45	0.98	0.99	40.290	N.A.	1.000	35.06	0.97	1.00	39.04	0.99	0.99

TABLE 5. Comparative analysis in terms of PSNR, SSIM, and NCC values of the proposed watermark scheme with existing watermarking schemes (using a non-optimized algorithm) (bold values of the performance evaluation parameters indicate the best performances).

Method	Proposed Method			Method [3]			Method [20]			Method [22]			Method [28]		
Images\ Metric	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC	PSNR	SSIM	NCC
Lena	**45.5728**	**0.9990**	**1.0000**	36.35	0.98	1.00	35.803	0.9881	1.00	40.113	0.993	1.000	40.47	0.975	1.00
F16	**45.3375**	**0.9986**	**1.0000**	36.31	0.98	1.00	38.316	0.9705	1.00	36.965	0.9865	1.000	38.59	0.957	1.00
Pepper	**45.6712**	**0.9976**	**1.0000**	36.68	0.96	1.00	35.986	0.9709	1.00	40.999	0.9928	0.989	41.43	0.981	0.99
TTU	**45.2016**	**0.9970**	**1.0000**	36.46	0.98	1.00	37.325	0.9864	1.00	39.029	0.9968	1.000	40.97	0.982	1.00

FIGURE 11. Performance of the proposed watermark scheme in case of watermarked and restore watermarked images under different SF values.

(detail provided in Table 4) and by not considering optimization algorithms [3], [20], [22], [28] (detail provided in Table 5). The experimental details presented in Tables 4-5 indicate that the proposed watermark scheme provides better the imperceptibility of a watermarked image as compared with its competitor watermarked schemes. The proposed watermark scheme also uses a strength factor (SF) for the generation of watermark color images and considered values of SF for performance analysis are 0.01, 0.03, 0.05, 0.07, 0.09, 0.12, 0.15, and 1.0.

Based on the simulation results shown in Fig. 11, it noticed that the proposed watermark scheme produces better imperceptibility results by obtaining acceptable PSNR and SSIM values using the optimized strength factor value. The NCC value of the actual watermark image (WI_{RGB}) and the recovered watermark image (EI_{RGB}) is also acceptable according to the experimental details shown in Fig. 11. Therefore, it can be concluded that the proposed watermark scheme is effective for the lossless restoration of secret images with watermarks and require a low computational cost.

E. ROBUSTNESS TEST

When watermarked images are passed through the network, the attacker can either attempt to retrieve or destroy the secret information. For a researcher, it is important to design a watermarking algorithm that is robust in case of any such operations. One of the primary requirements of the proposed watermark scheme is that it is robust against many kinds of operations or attacks. In this section, the robustness of the proposed watermark scheme is tested on watermark images against various intentional and unintentional distortions. The performance of the proposed watermark scheme is compared with the related existing watermark schemes (refer to Tables 4-5) for robustness tests by applying the

FIGURE 12. The watermarked image (Lena) and extracted watermark (Peugeot logo) after applying non-geometric attacks (a) JPG (30), (b) JPG (90), (c) JPG 2000 (5:1), (d) JPG 2000 (10:1), (e) S&NP (2%), (f) S&NP (10%), (g) GN (1%), (h) GN (3%), (i) SN (2%), (j) PN, (k) LPF (100,1), (l) LPF (100,3), (m) MF (2×2), (n) MF(3×3), (o) WF (3×3), (p) WF(5×5), (q) SH (2%), (r) BL (2%), (s) HE, (t) GC.

non-geometric and geometric distortions on the watermarked image.

F. ATTACKS AND COMPARATIVE ANALYSIS

There are several standard approaches to attaining maximum robustness, including spread spectrum, redundant embedding, and watermark embedding [24]. We have applied two categories of attacks to analyze the robustness of the proposed watermark scheme. The first type of attack is non-geometric attacks, and the second type involves geometric attacks [16]. The goal of non-geometric attacks is to eliminate the secret data from the watermark image without destroying the protection of the watermark algorithm [44]. Conversely, the purpose of geometric attacks is to make the image and the watermark content in the extraction detector out of sync [34] and regardless of the watermark's existence, the recovered bits are distinct from those hidden bits. Therefore, these attacks can be used to test the significance of the proposed watermark scheme. The proposed watermark scheme demonstrated strong resistance in all attacks whose experimental details are presented in Tables 6-8 with high NCC values. The robust pictorial results of the proposed watermark scheme using Lena and F16 as the cover images as well as the Peugeot logo as the watermark image are shown in Fig. 12 and Fig. 13, respectively.

1) NON-GEOMETRIC ATTACKS

The first type of attack is a non-geometric attack which is mainly a noise operation that affects high-frequency components (such as edges) of the images.

The addition of noise in the watermark image essentially impacts the statistical characteristics of image-processing attacks and reduces the chances of efficient extraction of watermarks. The performance of the proposed watermark scheme is also analyzed against various image compression operations like JPEG compression with distinct quality factor (QF) and JPEG 2000 compression standard with the compression ratio (CR). The JPEG quality factor (QF) values are chosen from 0-100 and values of the JPEG 2000 compression ratio (CR) are chosen from 1-10 for the test images. When the value of the JPEG quality factor is reduced from 90, image compression improves, however, the resultant image quality is significantly reduced. Fig. 12(a-b) and Fig. 12(c-d) show the experimental results of the proposed watermark scheme in case of a watermarked images and extracted watermarked images which are extracted after applying these attacks that provide good resistance to prove the strength of the proposed compression attack regime. The effectiveness and efficiency of the proposed watermark scheme are tested against four different kinds of noises which are salt and pepper noise (S&PN), Gaussian noise (GN), speckle noise (SN), and

TABLE 6. Comparative analysis in terms of the NC value in case of the extracted watermark from attacked Lena image (using an optimized algorithm) (bold values of the performance evaluation parameters indicate the best performances).

Attacks/Methods	Method [4]	Method [37]	Method [59]	Method [21]	Proposed scheme
JPEG compression					
30	0.85	0.8935	0.9924	N.A.	**0.9735**
90	0.90	0.9544	0.9949	N.A.	**0.9975**
Salt and pepper noise					
0.02	0.93	0.9688	0.7871	0.96	**0.9958**
0.1	N.A.	0.8924	0.7685	N.A.	**0.9711**
Gaussian noise					
0.01	0.87	0.9592	0.7364	0.92	**0.9621**
0.03	0.86	0.8444	0.6878	0.90	**0.9479**
Speckle noise					
0.01	N.A.	0.9614	0.8585	0.98	**0.9845**
0.04	N.A.	0.8940	0.7524	0.91	**0.9120**
Median filter					
2×2	0.74	0.9716	0.8585	0.79	**0.9918**
3×3	0.64	0.9602	0.7524	N.A.	**0.8788**
Wiener filter					
3×3	0.89	0.9771	0.9873	0.80	**0.9918**
5×5	N.A.	0.9696	0.9303	N.A.	**0.9488**
Sharpening					
0.2	N.A.	0.9715	1.0000	N.A.	**0.9999**
1.0	N.A.	0.9320	1.0000	N.A.	**0.9999**
Scaling					
0.25	0.74	0.7880	0.8915	0.79	**0.8892**
4.0	0.99	0.9920	0.9932	N.A.	**0.9990**
Cropping					
0.25	0.84	1.0000	0.7511	N.A.	**0.7712**
0.50	0.61	0.5702	0.5748	N.A.	**0.5832**
Histogram equalization	0.98	0.9721	0.9981	0.87	**0.9990**
Rotation					
1°	0.91	0.8746	N.A.	0.84	**0.9588**

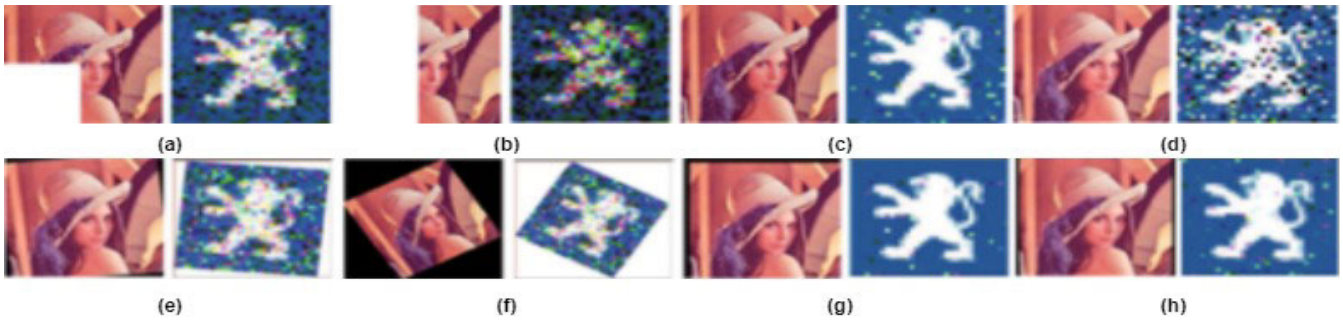


FIGURE 13. The watermarked image (Lena) and extracted watermark (Peugeot logo) after applying geometric attacks (a) RE (25%), (b) RE (400%), (c) CR (25%), (d) CR (50%), (e) RO (1°), (f) RO (30°), (g) TR (20,20), (h) CUT.

Poisson noise (PN) using various density and magnitude. The salt and pepper noise (S&PN) with various noise density values of 0.02 (2%) and 0.1 (10%), respectively are used to process the watermark image. Besides, the Gaussian noise (GN) is among the most widely used statistical noise that may corrupt the watermarked image. The watermarked images are examined against GN using 0 mean and values of variance are set to 0.01 (1%) and 0.03 (3%). Besides, the watermarked images are also examined by adding 0.01 (1%) Speckle noise (SN) and Poisson noise (PN). The extracted images of the watermark and watermarked image after applying these attacks are shown in Fig. 12(e-j). Image filtering or de-noising is another category of non-geometric attacks, which is the most common manipulation in digital image processing. The performance of the proposed watermark scheme is also tested using three types of such attacks. In the filtering attack, the median filter (MF) of size 2×2 to 3×3, the Wiener filter (WF) of size 3×3 to 5×5, and a low-pass filter (LPF) of order 100 are used to analyze the performance of the proposed watermark scheme. The cut-off frequencies of 1db and 3db are used for the watermarked images to analyze the performance of the proposed watermark scheme. Fig. 12(k-p)

TABLE 7. Comparative analysis in terms of the NC value in case of the extracted watermark from attacked Lena image (using a non-optimized algorithm) (bold values of the performance evaluation parameters indicate the best performances).

Attacks/Methods	Method [2]	Method [7]	Method [20]	Method [28]	Proposed scheme
JPEG compression					
30	0.8213	0.7530	0.8528	0.9051	**0.9931**
90	0.9931	0.9829	0.9937	0.9959	**0.9990**
JPEG 2000 compression					
5:1	0.9910	0.9836	0.9931	0.9888	**0.9918**
10:1	0.9990	0.9026	0.9991	0.9118	**0.9645**
Salt and pepper noise					
0.02	0.9541	0.9904	0.9552	0.9911	**0.9958**
0.1	0.8009	0.9362	0.8186	0.9607	**0.9711**
Gaussian noise					
0.01	0.9660	0.8558	0.9712	0.9406	**0.9621**
0.03	0.9162	0.5090	0.9242	0.8283	**0.9479**
Low-pass filter					
100,1	0.9715	0.9584	0.9796	0.9762	**0.9785**
100,3	0.8852	0.7987	0.8888	0.9312	**0.9510**
Median filter					
2×2	0.8709	N.A.	0.9136	0.8883	**0.9918**
3×3	0.5412	N.A.	0.5513	0.8606	**0.8788**
Sharpening					
0.2	0.9991	0.9991	0.9999	0.9999	**0.9999**
1.0	0.8071	0.9974	0.9999	0.9974	**0.9999**
Blurring					
0.2	1.0000	1.0000	1.0000	1.0000	**1.0000**
1.0	0.8855	0.7839	0.8790	0.9058	**0.9284**
Scaling					
0.25	0.9041	0.8004	0.8915	0.8702	**0.8892**
4.0	0.9917	0.9823	0.9932	0.9983	**0.9990**
Cropping					
0.25	0.8968	1.0000	0.7511	0.7725	**0.7712**
0.50	0.6467	0.5702	0.5748	0.5141	**0.5832**

shows the extracted watermark images of the Peugeot logo and watermarked image after applying these filtering attacks. Other non-geometrical attacks are blurring (BL), sharpening (SH), histogram equalization (HE), and Gamma correction (GC), which are also used to analyze the performance of the proposed watermark scheme. In the blurring (BL) operation, the values of the blurring to attack the watermarked image are 0.2 (20 percent) to 1 (100 percent), and the increment size is 0.2. Fig. 12(r) show the effect when the radii of the attacked image is 0.2. The results of sharpening (SH) operation with radii 0.2 (20%) and radii 1.0 (100%) are shown in Fig. 12(q). The histogram equalization (HE) is an image enhancement technique. The performance of the proposed watermark scheme is also assessed based on the amendment of the histogram whose result is shown in Fig. 12(s). The gamma correction (GC) is among the most famous image enhancement methods for adjusting poor image quality. The result of the proposed watermark scheme in the case of a gamma attack by applying a gamma value of 0.5 is shown in Fig. 12(t). Table 6 present the experimental detail of the proposed watermark scheme in terms of NC value and its comparison with recent image watermarking schemes. The results of the proposed watermark scheme in the case of a filtering attack are shown in Fig. 12 (a-t). It can be concluded that the recovered watermark is visible, indicating good resistance to filtering attacks using the proposed watermark scheme. All of these experiments show that the proposed watermarking scheme has strong robustness against some common non-geometric attacks.

2) GEOMETRIC ATTACKS

One more category of the distortions which is generally considered for image watermarking is called geometric attacks. The geometric attacks do not attempt to delete the watermark image itself but deform it by spatially changing the watermark data [34]. After these attacks, the watermark detection device does not recognize the watermark information that remains on the image, nevertheless, the watermark information cannot be fully removed. This type of attack does not replace the original watermark but instead falsifies the original image for confusion in order so that the work's ownership can't be determined. One of the crucial categories is the robustness against geometrical distortions. For the performance analysis of the proposed watermark scheme, five types of geometrical distortions are applied to the watermark images, which are cropping (CR), resizing (RE), rotation (RO), translation (TR), and cutting (CUT). The first type of geometric distortion is image cropping (CR), which relates to the contiguous removal of watermarked image rows or columns, usually from the borders. Fig. 13(c-d) shows the results of the extracted watermark images using the proposed

TABLE 8. Comparative analysis in terms of the NC value in case of the extracted watermark from attacked F16 image (using a non-optimized algorithm) (bold values of the performance evaluation parameters indicate the best performances).

Attacks/Methods	Method [2]	Method [7]	Method [20]	Method [28]	Proposed scheme
JPEG compression					
30	0.8410	0.8353	0.8881	0.9204	**0.9535**
90	0.9942	0.9910	0.9979	0.9988	**0.9980**
JPEG 2000 compression					
5: 1	0.9953	0.9936	0.9956	0.9990	**0.9997**
10: 1	0.9682	0.9716	0.9758	0.9761	**0.9786**
Salt and pepper noise					
0.02	0.9530	0.9846	0.9584	0.9958	**0.9916**
0.1	0.8018	0.9282	0.8312	0.9787	**0.9811**
Gaussian noise					
0.01	0.9728	0.9222	0.9913	0.9577	**0.9785**
0.03	0.5064	0.4555	0.5196	0.8550	**0.8888**
Low-pass filter					
100,1	0.9228	0.9205	0.9675	0.9769	**0.9788**
100,3	0.8350	0.7779	0.8888	0.9524	**0.9612**
Median filter					
2×2	0.9103	N.A.	0.9199	0.9212	**0.9258**
3×3	0.5020	N.A.	0.5513	0.8974	**0.9012**
Sharpening					
0.2	0.9889	0.9999	0.9999	0.9999	**0.9999**
1.0	0.9822	0.9917	0.9999	0.9969	**0.9999**
Blurring					
0.2	0.9889	0.9994	1.0000	1.0000	**1.0000**
1.0	0.8010	0.7488	0.8853	0.8853	**0.9180**
Scaling					
0.25	0.8493	0.8180	0.8677	0.8773	**0.8758**
4.0	0.9668	0.9629	0.9889	0.9997	**0.9999**
Cropping					
0.25	0.7833	1.0000	0.7585	0.7725	**0.7758**
0.50	0.5632	0.5079	0.5748	0.5141	**0.5795**

watermark scheme in the case of 25% and 50% cropping area of the watermark image. The second type of geometric distortion is image resizing (RE) or scaling (SC). In this type, the watermarked images are checked for scaling attack for which watermarked images are scaled to 25% and 400% of its original size. The results of the extracted watermark images using the proposed watermark scheme after the scaling attack are depicted in Fig. 13(a-b). The third geometric distortion is called image rotation (RO). The performance of the proposed watermark scheme is tested by applying a rotation attack of 1° and 30° in a clockwise rotation to verify robustness and its experimental results are shown in Fig. 13(e-f). The other geometric distortions are translation (TR) and cutting (CUT) attacks. The cutting attack is carried out on the watermarked image to show the robustness of the proposed watermark scheme and its results are shown by considering the Lena image as a watermark image to verify the strength of the proposed watermark scheme for such attacks. The results of the extracted watermark images using the proposed watermark scheme after applying translation (20, 20) and cutting (10) attacks are shown in Fig. 13(g-h). It is easy to conclude from the results that the proposed watermarking scheme is robust to different geometric attacks.

Therefore, after analyzing the visual results of the proposed watermark scheme in Fig. 13(a-h) and its comparison in terms of NC value with the existing image watermarking schemes (refer to Tables 6-8), it can be concluded that the proposed watermark scheme produces robust performance in the case of non-geometric and geometric attacks on the watermark images.

G. COMPARISON WITH WATERMARKING SCHEMES BASED ON OPTIMIZATION ALGORITHM

This section presents a comparative analysis of the proposed watermark scheme by considering the optimization factor. The SADE algorithm is used in the scheme [15] to optimize the strength factor value to embed the same size grayscale image into the grayscale cover image.

The improved version of PSO is used in the scheme [59] to embed a grayscale watermark image in the DCT-SVD domain into the grayscale cover image. The artificial bee colony (ABC) and uncorrelated color space (UCS) methods are used in the scheme [6] to insert the color secret image in the color cover image. In the scheme [21], the color secret image of the same size is embedded in the color cover image by using gray wolf optimization to optimize the strength factor. In the first two schemes [15] and [59], the grayscale image is embedded in the grayscale image; these schemes employe various algorithms of optimization as well. In the next two schemes [6] and [21], the color secret image is transformed in the color cover image, but they did not discuss the security threat of FPP.

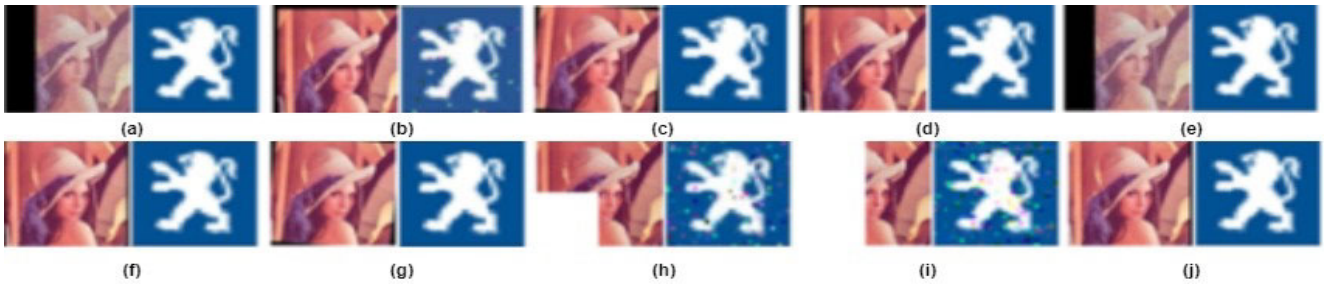


FIGURE 14. The watermarked image (Lena) and extracted watermark (Peugeot logo) after applying combinational attacks (non-geometric and geometric) (a) Gaussian noise (0.01) + cropping (0.25), (b) median filter (2 × 2) + translation (20, 20), (c) salt and pepper noise (0.02) + rotation (1°), (d) JPEG compression (Q=90) + translation (10, 10), (e) salt and pepper noise (0.02) + cropping (0.25), (f) JPEG compression (Q=30) + cutting (10), (g) JPEG compression (Q=30) + rotation (1°), (h) salt and pepper noise (0.1) + scaling (0.25), (i) JPEG compression (Q=90) + scaling (400), (j) salt and pepper noise (0.02) + cutting (10).

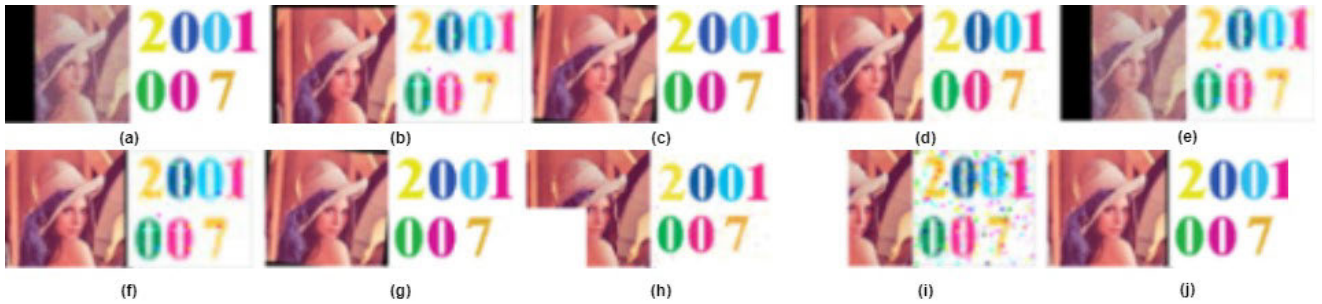


FIGURE 15. The watermarked image (Lena) and extracted watermark (8-color image) after applying combinational attacks (non-geometric and geometric) (a) Gaussian noise (0.01) + cropping (0.25, (b) median filter (2 × 2) + translation (20, 20, (c) salt and pepper noise (0.02) + rotation (1°), (d) JPEG compression (Q=90) + translation (10, 10), (e) salt and pepper noise (0.02) + cropping (0.25, (f) JPEG compression (Q=30) + cutting (10), (g) JPEG compression (Q=30) + rotation (1°), (h) salt and pepper noise (0.1) + scaling (0.25), (i) JPEG compression (Q=90) + scaling (400), (j salt and pepper noise (0.02) + cutting (10).

The comparative performance analysis in terms of NC value of the proposed watermark scheme by applying different attacks on the watermark image of Lena with existing image watermarking schemes by considering the optimization factor is presented in Table 6. After analyzing the experimental results presented in Table 6, it can be concluded that the proposed watermark scheme produces robust performance in terms of NC value by considering the optimization factor.

H. COMPARISON WITHOUT OPTIMIZATION ALGORITHM BASED WATERMARKING SCHEMES

This section present detail of the comparative performance analysis of the proposed watermark scheme with existing watermark schemes without considering the optimization factor. In [7], a color image is inserted into a color cover image using a predefined strength factor and the watermark is extracted using singular values that are more likely to cause false-positive security threats. In other schemes [2], [20], [28], the color image is employed to embed the color cover image as used by the proposed watermark scheme, however, due to the adaptive and optimized nature of the proposed watermark scheme, it produces superior performance in terms of NC value as compared with existing image watermarking schemes. The comparative results of the proposed watermark scheme without using optimization factor with existing watermark schemes are presented in Table 7 by considering a watermark image of the Peugeot logo and a cover image of Lena, and in Table 8 by considering a watermark image of the 8-color image and a cover image of F16.

I. COMBINATIONAL ATTACKS

This section present detail to analyze the performance of the proposed watermark scheme by applying a combination of geometric and non-geometric attacks to test its robustness on all standard test images. A single geometric or non-geometric attack may not be sufficient to demonstrate the robustness of the proposed watermark scheme. Keeping these facts into view, both types of attacks are applied to the watermarked images. The performance analysis of the proposed watermark scheme in terms of NC value of recovered watermark images (i.e. Peugeot logo and 8-color images) by considering combinational attacks is performed and its experimental details are mentioned in Table 9. It can be concluded that the proposed watermark scheme also provides robust performance in case of combinational attacks to the watermark images. The visual results of the watermarked images (i.e. Peugeot logo and 8-color images) and extracted watermarked images after applying combinational attacks are shown

TABLE 9. Comparative analysis of the proposed watermark scheme in terms of NC value using a combination of geometric and non-geometric attacks.

Multiple Attacks/Watermark Image	Peugeot LOGO			8-color image		
	Lena	Mandrill	Pepper	Lena	Mandrill	Pepper
Gaussian noise (0.01) + cropping (0.25)	0.9088	0.9045	0.8990	0.9158	0.9058	0.9022
Median filter (2 × 2) + translation (20, 20)	0.9958	0.9923	0.9918	0.9945	0.9920	0.9915
Salt and pepper noise (0.02) + rotation (1°)	0.9715	0.9699	0.9685	0.9705	0.9690	0.9688
JPEG compression (Q=90) + translation (10, 10)	0.9755	0.9710	0.9700	0.9745	0.9755	0.976
Salt and pepper noise (0.02) + cropping (0.25)	0.9715	0.9699	0.9685	0.9705	0.9690	0.9688
JPEG compression (Q=30) + cutting (10)	0.9010	0.9115	0.8945	0.8990	0.9055	0.8888
JPEG compression (Q=30) + rotation (1°)	0.9245	0.9045	0.9130	0.9190	0.8999	0.9060
Salt and pepper noise (0.1) + scaling (0.25)	0.9588	0.9455	0.9570	0.9420	0.9468	0.9510
JPEG compression (Q=90) + scaling (400)	0.9855	0.9810	0.9800	0.9845	0.9855	0.9860
Salt and pepper noise (0.02) + cutting (10)	0.9015	0.8990	0.9090	0.8990	0.8945	0.9018

TABLE 10. Comparative analysis of the proposed watermark scheme with existing watermark schemes in terms of embedding capacity (bold values indicate the best performances).

Schemes	Watermark image length (In bits)	Cover image (In bits)	Embedding capacity (In bits)
Scheme [7]	32 × 32 × 24	512 × 512 × 24	0.00390625
Scheme [20]	32 × 32 × 24	512 × 512 × 24	0.00390625
Scheme [25]	32 × 32 × 24	512 × 512 × 24	0.00390625
Scheme [28]	32 × 32 × 24	512 × 512 × 24	0.00390625
Proposed method	**512 × 512 × 24**	**512 × 512 × 24**	**1.000000**

in Fig. 14 and Fig. 15, respectively. It can be seen from Table 9 that the proposed watermarking scheme is very robust to different geometric and non-geometric attacks.

J. EMBEDDING CAPACITY ANALYSIS

The embedding (data hiding) capacity of a watermarking scheme is measured as the amount of watermark image bits embedded into the cover image, which can be defined mathematically as follows [39]:

$$EC = \frac{A_W}{A_H}\,(bpp) \tag{35}$$

where EC, AW, AH, and bpp represent the embedded capacity, the number of inserted images, the cover image, and bits per pixel, respectively. For the performance analysis of the proposed watermark scheme, the 24-bits color watermark image of resolution 512×512×3 pixels is inserted into the 24-bits color cover image of resolution 512×512×3 pixels. The total numbers of watermark and cover color images bits are ($512 \times 512 \times 24 = 6,291,456$) 6,291,456 bits as defined in Eq. (36).

$$\text{EC (bpp)} = \frac{512 \times 512 \times 24}{512 \times 512 \times 24} = 1\,(Bits) \tag{36}$$

where three is for color image channels, and one is for the channel of the gray-scale image. The comparative analysis of the proposed watermark scheme with existing watermark schemes in terms of EC is presented in Table 10. It can be concluded that the proposed watermark scheme provides robust performance in terms of EC as compared with existing image watermarking schemes.

K. SECURITY ANALYSIS

In the proposed watermark scheme, the (Y) luminance channel of the YCbCr color space of the watermark image is permuted by Arnold's scrambling scheme using a private key K to ensure the robustness and security of the watermarked image. When recovering the watermark image part from the watermarked image, no one user without the private key (K) can rearrange the watermarked image, thus the proposed watermark scheme provides more security as compared with the existing image watermarking schemes.

Even if one of those hidden keys is incorrect, the correct watermark cannot be extracted using the proposed watermark scheme. The results of this case are shown in Fig. 16 by considering the Peugeot logo and 8-color images as input to the proposed watermark scheme.

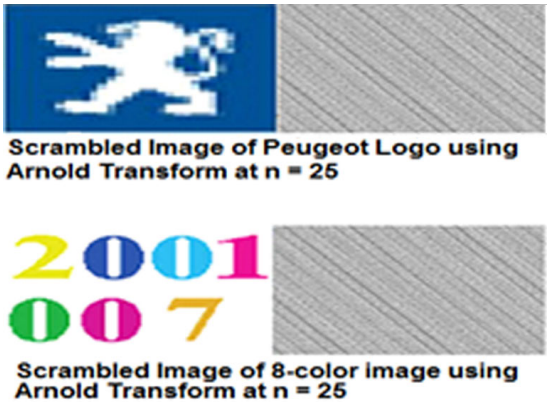


FIGURE 16. Scrambled images of the Peugeot logo and an 8-color image.

FIGURE 17. Result of the false-positive error (a) mandrill image as a watermarked (using the 8-color image as a watermark) (b) NTUST logo (as a false watermark image) (c) false-positive error result (extracted image).

L. FALSE POSITIVE PROBLEM (FPP) SOLUTION

In image watermarking, the false-positive problem (FPP), occurs, when an incorrect watermark (which has never been inserted into a cover image) is extracted from the cover image [51]. This scenario occurs when an intruder or illegal user tries to demonstrate the insertion and extraction algorithm of the watermarking scheme in some way to prove their copyright on the cover image. Different image watermarking schemes based on SVD only insert the singular values ($\sum$) of the secret data in the singular values ($\sum$) of the cover image SVD. Whereas SVD elements of the secret watermark image use the left (U) and right singular vector (V^T) as a secret extract key [50], [53]. If both singular vector elements of the erroneous watermark image are employed as a hidden key in the watermark extraction procedure, the watermark detection system may find forged or erroneous watermarks instead of declaring no watermark based on the given key. This is called a false positive problem (FPP). The proposed watermark scheme uses Arnold transform (AT) to scramble the watermark image to avoid the false-positive problem. After that, it calculates the PSNR quality metric of the cover as well as the watermarked image to generate strength factor α. The encrypted channel of the watermark principal component (PC) is merged in the singular values of the cover image by the proposed watermark scheme, which completely ensures that the false positive problem is overcome. Over 25 separate false ownership reports are evaluated for the performance analysis of the proposed watermark scheme, and each time, it can detect a false declaration. The false-positive problem experiment is performed by using the NTUST logo as a fake watermark, which is attempted to extract from the watermarked image in which the 8-color image has been inserted. The visual result is shown in Fig.17.

VI. CONCLUSION AND FUTURE WORK

This article presents a novel semi-blind watermark scheme using the YCbCr color system to fulfill the criteria of invisibility, high robustness, and high embedded capacity. The size of the watermark image is the same as the cover image, thereby increases the embedding capacity of inserting the watermark into the cover image. Arnold scrambling encrypts the watermark image with several iterations as a security key to enhance the security of the proposed watermark scheme. Compared with state-of-the-art image watermarking schemes, the proposed watermark scheme provides a higher payload capacity. It also provides higher watermark image quality (not easily noticeable) and provides strong robustness against different types of attacks. The performance of the proposed watermark scheme is not only tested against common geometric and non-geometric transformation attacks but also verified against certain combinational attacks, which prove its robust performance. The proposed scheme also uses PSO to achieve the best balance between imperceptibility and robustness. As noticed in the experimental results, it produces a better result for the color image watermarking. The comparative analysis shows that this scheme is superior to other similar watermarking schemes in terms of invisibility and robustness. Moreover, it overcomes the issue of a false-positive problem that takes place in most SVD-based image watermarking schemes. The performance of the proposed watermark scheme can be further extended to improve color image performance on 3-D images, videos, and audios as future work.

COMPETING INTEREST

All the authors declare no competing interest.

ACKNOWLEDGMENT

(Adnan Mustafa Cheema, Syed Muhammad Adnan, and Zahid Mehmood contributed equally to this work.)

REFERENCES

[1] K. J. Giri and R. Bashir, "A block based watermarking approach for color images using discrete wavelet transformation," *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 139–146, Jun. 2018.

[2] Q. Su, Y. Niu, X. Liu, and Y. Zhu, "Embedding color watermarks in colorimages based on Schur decomposition," *Opt. Commun.*, vol. 285, no. 7, pp. 1792–1802, Apr. 2012.

[3] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Color image blind watermarking scheme based on QR decomposition," *Signal Process.*, vol. 94, pp. 219–235, Jan. 2014.

[4] E. Vahedi, R. A. Zoroofi, and M. Shiva, "Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles," *Digit. Signal Process.*, vol. 22, no. 1, pp. 153–162, Jan. 2012.

[5] S. Bagheri Baba Ahmadi, G. Zhang, S. Wei, and L. Boukela, "An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics," *Vis. Comput.*, 2020, doi: 10.1007/s00371-020-01808-6.

[6] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *Int. J. Comput. Intell. Syst.*, vol. 8, no. 2, pp. 364–380, Mar. 2015.

[7] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 987–1009, Sep. 2014.

[8] P. Vaidya S. and C. Mouli P. V. S. S. R., "A robust semi-blind watermarking for color images based on multiple decompositions," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 25623–25656, Dec. 2017.

[9] K. Prabha and I. S. Sam, "A novel blind color image watermarking based on Walsh Hadamard transform," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6845–6869, Mar. 2020.

[10] Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "A new algorithm of blind color image watermarking based on LU decomposition," *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1055–1074, Jul. 2018.

[11] M. K. Pandey, G. Parmar, R. Gupta, and A. Sikander, "Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space," *Microsyst. Technol.*, vol. 25, no. 8, pp. 3071–3081, Aug. 2019.

[12] 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.

[13] F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," in *Proc. IEEE 14th Int. Colloq. Signal Process. Its Appl. (CSPA)*, Mar. 2018, pp. 221–226.

[14] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018.

[15] M. H. Vali, A. Aghagolzadeh, and Y. Baleghi, "Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition," *Expert Syst. Appl.*, vol. 114, pp. 296–312, Dec. 2018, doi: 10.1016/j.eswa.2018.07.004.

[16] E. Najafi, "A robust embedding and blind extraction of image watermarking based on discrete wavelet transform," *Math. Sci.*, vol. 11, no. 4, pp. 307–318, Dec. 2017, doi: 10.1007/s40096-017-0233-1.

[17] M. Imran and B. A. Harvey, "A blind adaptive color image watermarking scheme based on principal component analysis, singular value decomposition and human visual system," *Radioengineering*, vol. 26, no. 3, pp. 823–834, Sep. 2017.

[18] C. Patvardhan, P. Kumar, and C. Vasantha Lakshmi, "Effective color image watermarking scheme using YCbCr color space and QR code," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 12655–12677, May 2018.

[19] 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.

[20] Q. Su and B. Chen, "An improved color image watermarking scheme based on Schur decomposition," *Multimedia Tools Appl.*, vol. 76, no. 22, pp. 24221–24249, Nov. 2017.

[21] M. K. Pandey, G. Parmar, R. Gupta, and A. Sikander, "Lossless robust color image watermarking using lifting scheme and GWO," *Int. J. Syst. Assurance Eng. Manage.*, vol. 11, no. 2, pp. 320–331, Apr. 2020.

[22] Q. Su, Y. Liu, D. Liu, Z. Yuan, and H. Ning, "A new watermarking scheme for colour image using QR decomposition and ternary coding," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8113–8132, Apr. 2019.

[23] Q. Su, Z. Yuan, and D. Liu, "An approximate Schur decomposition-based spatial domain color image watermarking method," *IEEE Access*, vol. 7, pp. 4358–4370, 2019.

[24] S. Roy and A. Pal, "A hybrid domain color image watermarking based on DWT-SVD," *Iranian J. Sci. Technol., Trans. Elect. Eng.*, vol. 43, no. 2, pp. 201–217, 2018.

[25] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7491–7513, Mar. 2020.

[26] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8381–8401, Jul. 2016.

[27] L. Zhang and D. Wei, "Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 28003–28023, Oct. 2019.

[28] Q. Su, X. Zhang, and G. Wang, "An improved watermarking algorithm for color image using Schur decomposition," *Soft Comput.*, vol. 24, no. 1, pp. 445–460, Jan. 2020.

[29] University of Southern California. Signal and Image Processing Institute. *USC-SIPI Image Database*. Accessed: Mar. 15, 2017. [Online]. Available: http://sipi.usc.edu/database/

[30] Dd University of Granada. Computer Vision Group. *CVG-UGR Image Database*. Accessed: Mar. 13, 2017. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/

[31] Z. Zheng, N. Saxena, K. K. Mishra, and A. K. Sangaiah, "Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications," *Future Gener. Comput. Syst.*, vol. 88, pp. 92–106, Nov. 2018.

[32] 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," *Appl. Soft Comput.*, vol. 84, Nov. 2019, Art. no. 105696.

[33] K. Balasamy and S. Ramakrishnan, "An intelligent reversible watermarking system for authenticating medical images using wavelet and PSO," *Cluster Comput.*, vol. 22, no. S2, pp. 4431–4442, Mar. 2019.

[34] S. Roy and A. K. Pal, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection," *Roy. Soc. Open Sci.*, vol. 4, no. 6, Jun. 2017, Art. no. 170326, doi: 10.1098/rsos.170326.

[35] S. Singh, V. S. Rathore, R. Singh, and M. K. Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 19113–19137, Sep. 2017.

[36] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "A new aspect in robust digital watermarking," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 179–200, Sep. 2013.

[37] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 17027–17049, Jun. 2019.

[38] R. Noor, A. Khan, A. Sarfaraz, Z. Mehmood, and A. M. Cheema, "Highly robust hybrid image watermarking approach using tchebichef transform with secured PCA and CAT encryption," *Soft Comput.*, vol. 23, no. 20, pp. 9821–9829, Oct. 2019.

[39] R. Thanki and S. Borra, "A color image steganography in hybrid FRT–DWT domain," *J. Inf. Secur. Appl.*, vol. 40, pp. 92–102, Jun. 2018.

[40] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Comput. Standards Interface*, vol. 32, nos. 1–2, pp. 54–60, Jan. 2010.

[41] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Gener. Comput. Syst.*, vol. 101, pp. 1223–1246, Dec. 2019.

[42] P. Verma, M. Saxena, and M. Kumar, "An optimized digital watermarking approach in wavelet domain based on whale optimization algorithm for color image," in *Proc. Int. Conf. Adv. Comput. Manage. (ICACM)*, Aug. 2019. [Online]. Available: https://ssrn.com/abstract=3444776, doi: 10.2139/ssrn.3444776.

[43] S. AlZubi, N. Islam, and M. Abbod, "Multiresolution analysis using wavelet, ridgelet, and curvelet transforms for medical image segmentation," *J. Biomed. Imag.*, vol. 2011, p. 18, Jan. 2011, Art. no. 4.

[44] N. Tarhouni, M. Charfeddine, and C. Ben Amar, "Novel and robust image watermarking for copyright protection and integrity control," *Circuits, Syst., Signal Process.*, vol. 39, no. 10, pp. 5059–5103, Oct. 2020.

[45] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26845–26879, Oct. 2018.

[46] F. Ernawan and M. Kabir, "An improved watermarking technique for copyright protection based on tchebichef moments," *IEEE Access*, vol. 7, pp. 151985–152003, 2019.

[47] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-Based optimization," *J. Inf. Secur. Appl.*, vol. 47, pp. 28–38, Aug. 2019.

[48] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, and R. Zhou, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019.

[49] 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 Syst. Appl.*, vol. 39, no. 1, pp. 673–689, Jan. 2012.

[50] P. Pandey, S. Kumar, and S. K. Singh, "Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 723–748, Sep. 2014.

[51] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Eng. Appl. Artif. Intell.*, vol. 49, pp. 114–125, Mar. 2016.

[52] M. Cedillo-Hernández, F. García-Ugalde, M. Nakano-Miyatake, and H. M. Pérez-Meana, "Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification," *Signal, Image Video Process.*, vol. 8, no. 1, pp. 49–63, Jan. 2014.

[53] J.-M. Guo, D. Riyono, and H. Prasetyo, "Hyperchaos permutation on false-positive-free SVD-based image watermarking," *Multimedia Tools Appl.*, vol. 78, no. 20, pp. 29229–29270, Oct. 2019.

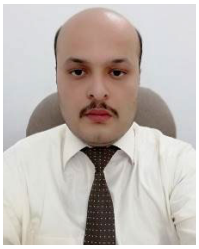
[54] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867, 2014.

[55] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik*, vol. 125, no. 1, pp. 428–434, Jan. 2014.

[56] A. Bassel, M. J. Nordin, and M. B. Abdulkareem, "An invisible image watermarking based on modified particle swarm optimization (PSO) algorithm," *Int. J. Secur. Appl.*, vol. 12, no. 2, pp. 1–8, Mar. 2018.
[57] N. R. Zhou, A. W. Luo, and W. P. Zou, "Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 2507–2523, Jan. 2019.
[58] F. N. Thakkar and V. K. Srivastava, "Performance comparison of recent optimization algorithm Jaya with particle swarm optimization for digital image watermarking in complex wavelet domain," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1769–1791, Oct. 2019.
[59] X. Kang, Y. Chen, F. Zhao, and G. Lin, "Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain," *Soft Comput.*, vol. 24, no. 14, pp. 10561–10584, Jul. 2020.
[60] H.-H. Tsai, Y.-J. Jhuang, and Y.-S. Lai, "An SVD-based image watermarking in wavelet domain using SVR and PSO," *Appl. Soft Comput.*, vol. 12, no. 8, pp. 2442–2453, Aug. 2012.

ADNAN MUSTAFA CHEEMA received the M.C.S. degree from the University Institute of Information Technology (UIIT) and the M.S. degree in software engineering from International Islamic University (IIU), Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in computer science with the University of Engineering and Technology (UET) at Taxila, Taxila, Pakistan. His research interests include medical imaging, image watermarking, and image encryption.

SYED MUHAMMAD ADNAN received the M.S. degree in computer engineering from the Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan, in 2010, and the Ph.D. degree in computer engineering from the University of Engineering and Technology at Taxila, Taxila, Pakistan, in 2014. He is currently serving as an Assistant Professor with the Department of Computer Science, University of Engineering and Technology at Taxila. His research interests include acoustic scene analysis, multimedia signal processing, and machine learning.



ZAHID MEHMOOD received the B.S. degree (Hons.) in computer engineering from the COMSATS University of Sciences and Technology, Wah Campus, Pakistan, in 2009, the M.S. degree in electronic engineering with a specialization in signal and image processing from International Islamic University (IIU), Islamabad, Pakistan, in 2012, and the Ph.D. degree in computer engineering with a specialization in content-based image retrieval (CBIR) from the University of Engineering and Technology (UET) at Taxila, Taxila, Pakistan, in 2016. He is currently the Team-Lead of the Forensic Analysis, Machine Learning, and Information Retrieval (FAMLIR) Research Group. He has published more than 70 publications in impact factor journals (ISI indexed) and international conferences. His research interests include content-based image retrieval (CBIR), medical imaging, deep learning, image forensic, computer vision, and machine learning. He is also a Reviewer of international journals and conferences, such as IEEE Access, *Pattern Recognition*, *Information Fusion*, *Soft Computing*, *Pattern Recognition Letters*, *Neural Computing and Applications*, *Neurocomputing*, the *Journal of Electronic Imaging*, the *Journal of Information Science*, *Computers and Electrical Engineering*, PAMI, and CVPR.