IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 24, 2022, accepted May 7, 2022, date of publication May 13, 2022, date of current version May 20, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3174964

Efficient Watermarking Method Based on Maximum Entropy Blocks Selection in Frequency Domain for Color Images

ROOP SINGH[1], LILA IZNITA IZHAR[2], (Member, IEEE), IRRAIVAN ELAMVAZUTHI[2], (Senior Member, IEEE), ALAKNANDA ASHOK[3], SUMIT AOLE[4], AND NAVEEN SHARMA[5]

[1]Department of Electronics and Communication Engineering, Uttarakhand Technical University, Sudhowala, Dehradun, Uttarakhand 248007, India
[2]Smart Assistive and Rehabilitative Technology (SMART) Research Group, Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Bandar Seri Iskandar 32610, Malaysia
[3]Dean College of Technology, G. B. Pant University of Agriculture and Technology, Pantnagar, Uttarakhand 263153, India
[4]Department of Instrumentation Engineering, Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, Maharashtra 431606, India
[5]Biomedical and Applications Division, CSIR-Central Scientific Instrumentation Organization, Chandigarh 160030, India

Corresponding author: Lila Iznita Izhar (lila.izhar@utp.edu.my)

This work was supported by the Yayasan Universiti Teknologi PETRONAS (YUTP), Malaysia, under Grant 015LC0-134.

ABSTRACT False-positive problem (FPP) is a one of the challenging tasks for the researchers. It authenticates the wrong owner to access the multimedia content. To overcome, the FPP problem, this paper introduces an efficient watermarking method based on the selection of highest entropy blocks. In this method, cover and watermark images are initially shuffled through Arnold transform. Then, the encrypted images are further processed by a 2-level discrete wavelet transform followed by singular value decomposition. The proposed method has been evaluated with geometrical, filtering, noise, and contrast adjustment attacks on the standard image datasets against five recently developed watermarking methods. The simulation results reveal that the proposed method outperforms the existing methods.

INDEX TERMS Color watermarking, False positive problem, Arnold transform, Discrete wavelet transform, Singular value decomposition.

I. INTRODUCTION

Security to multimedia content (image, text, audio, video) is a challenging issue globally [1]. The multimedia content can be secured through the frequently employed methods, namely steganography, cryptography, and digital watermarking. However, out of these said methods, both steganography and cryptography methods cannot stop illegal data transfer and distribution over the Internet. As a result, digital watermarking approach mitigates these concerns by including certain information into the cover image as a watermark while maintaining the image quality [2]. The embedding and extraction are two of the most critical phases of any watermarking method. Watermarking methods are grouped into three categories based on the extraction procedure, namely semi-blind, non-blind, and blind. In the semi-blind methods, the watermark and key are needed during the watermark extraction. Non-blind are those methods which require both cover and watermark images. Blind methods require the original key to retrieve watermark images. A robust and reliable watermarking method should possess the following fundamental characteristics [3]:

1) Computational cost: Watermark embedding and extraction should be done with minimal computing effort. This is especially important when dealing with high-quality images. While calculating the computational cost, it is essential to consider the time required to embed and retrieve the watermark. A healthy trade-off must be maintained between robustness and computing complexity.
2) False positive rate: False positive issue arises when the embedded watermark is not identical to the retrieved watermark. This property has been primarily utilized for copyright protection and ownership.
3) Imperceptibility: Perceptual transparency is critical for a watermarking system. The observer should not be

The associate editor coordinating the review of this manuscript and approving it for publication was Varuna De Silva.

able to discern a watermark. There should be no detectable artifacts introduced into the original image by the data-embedding process.

4) Robustness: Detection of the digital watermark is possible even after the image has been attacked. The attacks can be in the forms of linear or nonlinear filtering, image enhancement, resizing, and compression to evaluate the robustness.
5) Security: a watermark must remain hidden and unnoticeable to anybody other than the intended recipient. The watermark should only be available to those who have the proper credentials, and can be often applied using cryptographic keys to meet this security need. A set of private secret keys may only be obtained by a person who is the legitimate owner of the intellectual property image.

Generally, watermark might be hidden in either spatial or frequency domains. Histogram shifting (HS), spread spectrum (SS), and least significant bit (LSB) are often used methods in the spatial domain to alter the watermark [4]. It is possible to achieve high imperceptibility by using these domain methods that are computationally efficient and have a large embedding capacity. In addition, watermarking attacks are not resistant to these methods. The watermarks are hidden using the cover image's wavelet coefficients in the frequency domain. These frequency-domain methods include DFT (discrete Fourier transform), DCT (discrete cosine transform), SVD (singular value decomposition), DWT (discrete wavelet transform), and RDWT (redundant DWT) [5]. These methods perform superior to spatial domain methods in terms of robustness [2]. Researchers have studied many watermarking methods based on grayscale and color images [6]–[8]. However, grayscale images contain less information than the color images. Instead of relying on grayscale watermarking methods, researchers are now working on color image watermarking strategies [9].

Watermarking methods based on the DFT transform proposed by Fares *et al.* [10]. This approach employs two DFT variations, namely FDFT and QDFT, to obscure the watermarks. In an SVD based Watermarking scheme carried out by Shieh *et al.* [11], both cover and watermark images are initially exposed to chaotic permutation and then both images are partitioned into predefined block sizes. Experimentation has shown that the suggested scheme outperforms the considered method in all the aspects. A DCT-correlation based watermarking method devised by Das *et al.* [12] hides watermark based on correlation. A DWT-based watermarking algorithm developed by Garg *et al.* [6] adds PN sequences into the wavelet coefficients. The single-domain strategies outlined in this article cannot deliver acceptable performance. To increase the overall performance, several digital watermarking methods are often combined [13].

A DCT-SVD based watermarking approach for copyright protection devised by Roy *et al.* [14] conceals scrambled watermark into DCT coefficient blocks. The results of the simulations reveal that the suggested approach provides excellent resilience and high imperceptibility. A method devised by Lai *et al.* [15] embeds watermarks into the DWT coefficients. Experiments have shown that this method is both reliable and efficient. Huang *et al.* [16] also suggested a hybrid watermarking method based on DCT-SVD domain. In this method, SVD and DCT are used together to provide great resilience while maintaining imperceptibility. Using a DCT-DWT watermarking system, Abdulrahman *et al.* [17] developed a copyright-protecting watermarking scheme. Singh *et al.* [7] presented a hybrid DWT-SVD watermarking method in DCT domain. In this method, 4×4 blocks of DCT middle coefficients are employed to hide watermark followed by SVD. This method is impervious to attacks. According to the research, SVD-based watermarking methods are prone to false positives.

Singh *et al.* [18] developed a watermarking method based on NSCT domain to incorporate a watermark into an image. In this method, the cover image is modified using the RDWT transform to achieve maximum payload capacity, while the AT transform increases security and robustness. In the color model YC_bC_r, Roy *et al.* [2] suggested a watermarking method based on RDWT for color images. A scrambled grayscale image is used in this approach to conceal a watermark in the luminance (Y) component. Watermarking attacks cannot compromise the suggested system, as shown by the simulations. Furthermore, Roy *et al.* [19] also offered an RDWT-DCT based blind watermarking approach. In this scheme, scrambled logos are put into horizontal wavelet coefficients to form a watermarked image. Ernawan *et al.* [20] devised a blind watermarking system for a grayscale image in RDWT domain. Here, An encrypted watermark image is used to alter the U matrix value of the LL sub-band of the cover image. In contrast, Arnold scrambling is used to generate the encrypted watermark image. The existing watermarking techniques are summarized in Table 1 for better understanding. From the literature, it can be concluded that the above mentioned methods fails to mitigate the FPP problem and computationally intensive [21]. Furthermore, DWT-based watermarking systems offer the advantages of multi-resolution, superior energy compression, and an undetectable visual quality.

Therefore, the key contribution of this manuscript is as follows:

1) This paper introduces an efficient, false-positive problem-free based semi-blind watermarking scheme in DWT-SVD domain for color images.
2) The maximum entropy blocks are employed to hide watermark which reduces the computation cost.
3) The false-positive problem issue is mitigated by embedding watermark into the principal components of cover image.

The rest of the manuscript is organized as follows: Section 2 examines the watermarking methods associated with this paper. Section 3 covers the proposed method, whereas Section 4 examines the experimental outcomes. Section 5 brings the paper to a conclusion.

TABLE 1. Comparative analysis of existing color watermarking schemes based on pros and cons.

Author	Used Method	Domain	Pros	Cons	Application
Su et al. [4]	2D-DFT	Spatial	Computationally efficiently	Vulnerable to attacks	Copyright
Fares et al. [10]	DFT	Frequency	Robust over compression and filtering attacks	Low embedding capacity	— — — —
Shieh et al. [11]	SVD, Chaotic mixing	Frequency	Lossless	quality degraded	Copyright
Das et al. [12]	DCT	Frequency	Robust over JPEG compression	Less Secure	— — — —
Garg et al. [6]	DWT, spread spectrum	Frequency	Enhance security	quality degrade	Authentication
Roy et al. [14]	DCT, SVD	Address diagonal line problem	Frequency	Computational expensive	Copyright
Lai et al. [15]	DWT, SVD	Frequency	High robustness	— — — —	— — — —
Huang et al. [16]	SVD, DCT	Frequency	Improve transparency	Less robustness	— — — —
Abdulrahman et al. [17]	DWT, DCT	Frequency	High transparency	Vulnerable to print/scan attacks	— — — —
Singh et al. [7]	DWT,DCT, SVD	Frequency	Low time complexity	Copyright	
Singh et al. [18]	RDWT, SVD	Frequency	Better quality of extracted watermark	Computationally expensive	— — — —
Roy et al. [2]	SVD, RDWT	Frequency	Shift-invariant	High computationally cost	Authenticity
Roy et al. [19]	RDWT, DCT	Frequency	High embedding capacity	Computationally intensive	— — — —
Ernawan et al. [20]	RDWT,SVD	Frequency	Highly robust under JPEG2000	Higher computational cost	— — — —

II. PRELIMINARIES

A. DISCRETE WAVELET TRANSFORM

DWT uses low pass and high pass filters to split an image into four equal-sized bands. These sub-bands are LL (low frequency), LH (horizontal), HL (vertical), and HH (diagonal), respectively. In DWT, the high pass filter isolates the edges from the cover image, whereas the low pass filter approximates (reproduce the same) the cover image. At decomposition at each level, the low-frequency sub-band (LL) yields the approximation coefficients. The rest of the three sub-bands provide specific information regarding local changes in brightness in the cover image. The low-frequency sub-band (LL) preserves the maximum energy of the cover image. The LH sub-band gives detailed information vertically with the horizontal edge level. The HL sub-band contains detailed information horizontally with the vertical edge level. A watermark can be placed into any sub-band due to the multi-resolution characteristics of DWT. Usually, embedding a watermark in LL sub-band affects the imperceptibility, whereas it improves the robustness. Moreover, embedding watermark information into high-frequency sub-bands improves the imperceptibility while compromising with robustness. The complete procedure of 2-level DWT is depicted in Figure 1.

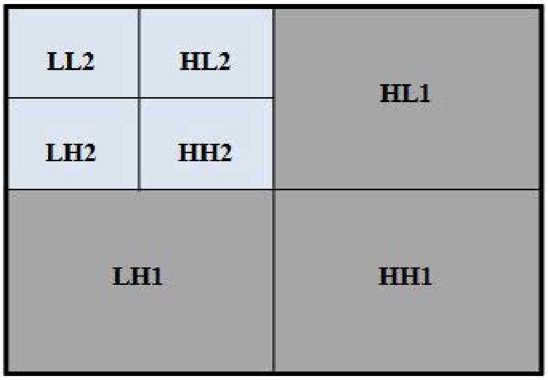


FIGURE 1. Performing 2-level DWT on a matrix.

B. SINGULAR VALUE DECOMPOSITION

A matrix can be diagonalized symmetrically using SVD transform in linear algebra. A real or complex rectangular matrix H of size $r_1 \times c_1$ can be factorized into U, S, and the transpose of V matrices, respectively. A matrix of size $r_1 \times r_1$ is a right orthogonal matrix and represented by U. Similarly, a matrix of size $r_1 \times c_1$ with non-negative real numbers is a rectangular diagonal matrix and represented by S, and a matrix of size $c_1 \times c_1$ is a left orthogonal matrix and represented by V. The columns of U matrix represent left singular vectors. Similarly, V matrix columns represent right singular vectors. S matrix diagonal values are always written in descending order, represented as singular values. Mathematically, SVD is performed on a matrix (H) by Eq. (1).

$$SVD(H) = U_h S_h V_h^T \tag{1}$$

There are some advantages of SVD in watermarking application.

1) The singular values (S) define the image's brightness, while the geometric features of the image are represented by the singular vectors (U, V).
2) If S is stable, then modest changes to the image's singular values will not cause large changes in S.
3) Singular values are listed in decreasing order, and many have lesser values than the initial singular value. It can have a slight and non-noticeable effect on image quality by updating or ignoring such small data during the reconstruction step.

C. ARNOLD TRANSFORM

The Arnold transform (AT) reorders the values of each pixel in an image to improve security and produce a chaotic image. Arnold transform uses an iterative procedure to translate the values of individual pixels to the values of new pixels.

The AT of a 2-D matrix is defined by Eq. (2).

$$\begin{bmatrix} a_x \\ b_x \end{bmatrix} = \begin{bmatrix} 1 & m \\ n & mn+1 \end{bmatrix} \begin{bmatrix} a_{x-1} \\ b_{x-1} \end{bmatrix} mod(s) \tag{2}$$

III. PROPOSED METHOD

This section covers the proposed method which has two phases, namely embedding and extraction. The proposed method hides a watermark into the maximum entropy blocks (MEB) using DWT-SVD(DS), termed as MEB-DS. The proposed method is feasible for practical applications since its extraction and detection procedures do not use original image, as shown in Equation 16 (the only side information is required). Therefore, the proposed method is semi-blind which authenticates and provides the security to multi-media content. Figure 2 illustrates embedding and extraction phases of the MEB-DS.

A. EMBEDDING PHASE

This section presents the entire embedding procedure in detail. Arnold transform first encrypts both the cover and watermark images to improve overall security. Further, both encrypted images are followed by a 2-level DWT and HH sub-band is opted out for embedding. This sub-band is subsequently separated into 8 × 8 blocks followed by SVD to insert watermark into principal component. The magnitude of principal components is comparatively higher than the singular components [22]. Therefore, embedding watermark into the maximum entropy blocks of principal components improves the PSNR and NC values as well as reduce computational cost. The embedding method's steps are as follows:

1) The cover (c) and watermark (w) images are of size $(M \times M)$ respectively.
2) Perform AT on both images (c, w) which results in scrambled images ($\tilde{c}$, $\tilde{w}$).
3) Apply 2-level DWT on scrambled cover image ($\tilde{c}$) as Eq. (3)

$$\begin{aligned}[LL_{c1}, LH_{c1}, HL_{c1}, HH_{c1}] &= DWT2(\tilde{c},'haar') \\ [LL_c, LH_c, HL_c, HH_c] &= DWT2(LL_{c1},'haar')\end{aligned} \tag{3}$$

4) Apply 2-level DWT on scrambled watermark image ($\tilde{w}$) as Eq. (4)

$$\begin{aligned}[LL_{w1}, HL_{w1}, HL_{w1}, HH_{w1}] &= DWT2(\tilde{w},'haar') \\ [LL_w, HL_w, HL_w, HH_w] &= DWT2(LL_{w1},'haar')\end{aligned} \tag{4}$$

5) Sub-band HH_2 is selected to conceal watermark and divide it into 8 × 8 blocks by Eq. (5).

$$Block_N = \frac{S/4 \times S/4}{S/32 \times S/32} \tag{5}$$

where N denotes the total blocks of size 8 × 8
6) Calculate entropy of each block by Eq. (6).

$$E_N = -\sum \left(h. \star \log_2(h)\right) \tag{6}$$

where h defines the histogram counts of each block.
if $entropy(Block_N) > Avg.entropy(Block)$
$M_N = Maximum\ entropy\ block$
else
return
end
7) Now, perform SVD on Maximum entropy blocks (M_N) by Eq. (7).

$$[U_c, S_c, V_c] = SVD(M_N) \tag{7}$$

8) Calculate principal component (B_{pc}) to avoid false-positive issue by Eq. (8).

$$B_{pc} = U_c \times S_c \tag{8}$$

9) Embed the watermark sub-band coefficients (HH_w) into principal component (B_{pc}) using Eq. (9).

$$HH_{pc} = B_{pc} + \alpha(HH_w) \tag{9}$$

10) Apply inverse SVD (ISVD) to obtain modified matrix $(HH_2^\star)$ as Eq. (10).

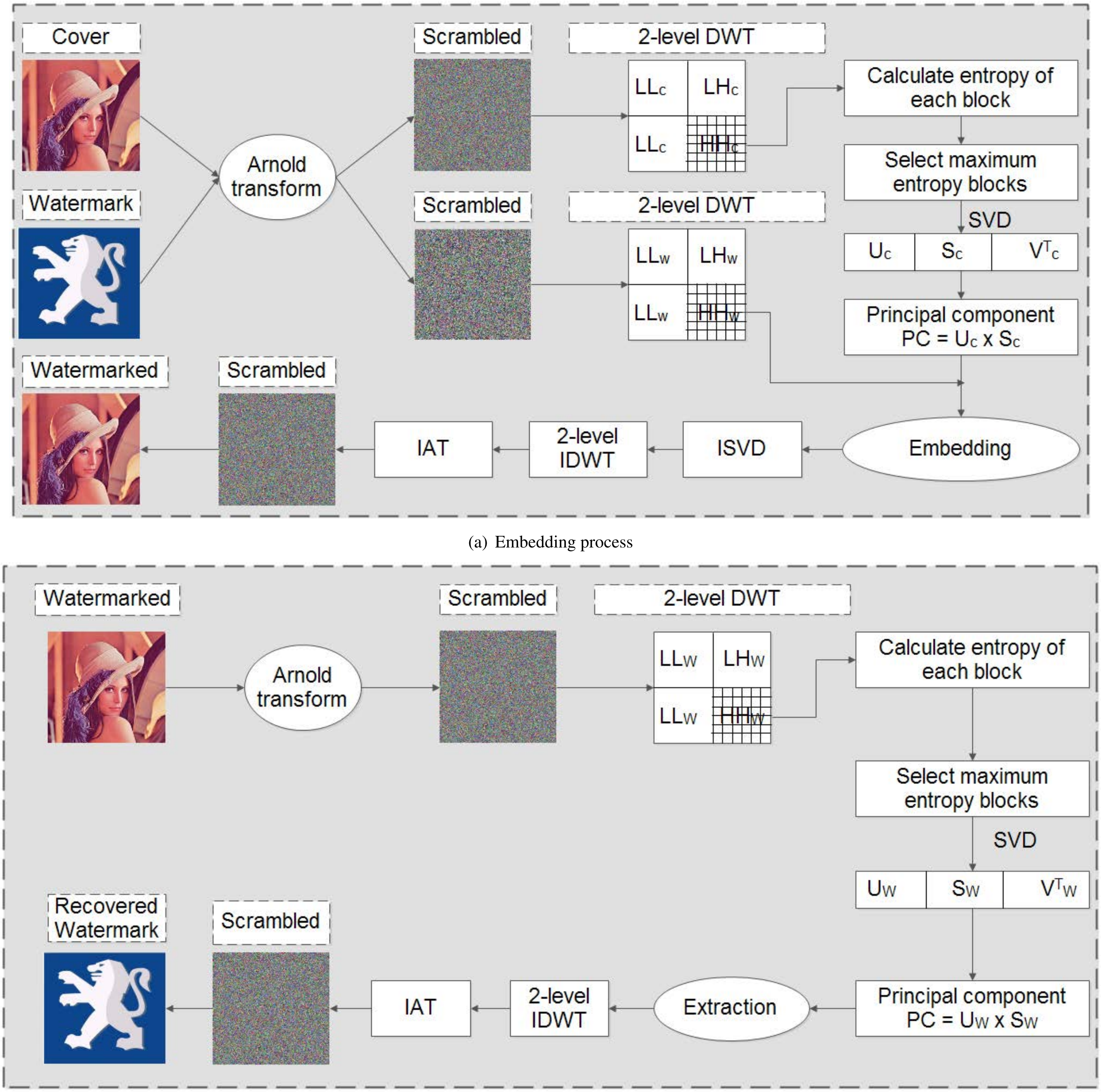
$$HH_2^\star = HH_{pc} \times V_c^T \tag{10}$$

11) Perform 2-level inverse DWT (IDWT) on $HH_2^\star$ to obtain the encrypted watermarked image $(\widetilde{W_{HH}})$ by using Eq. (17)

$$\begin{aligned} W_{HH} &= IDWT2[LL_2, LH_2, HL_2, HH_2^\star,'haar'] \\ \widetilde{W_{HH}} &= IDWT2[LL_{c1}, LH_{c1}, HL_{c1}, W_{HH},'haar'] \end{aligned} \tag{11}$$

12) Finally, perform inverse AT (IAT) on $\widetilde{W_{HH}}$ to get watermarked image (W) as Eq. (12).

$$W = IAT(\widetilde{W_{HH}}) \tag{12}$$



(a) Embedding process

(b) Extraction process

FIGURE 2. The embedding and extraction phases of the proposed method (MEB-DS).

B. EXTRACTION PHASE

In extraction phase, an embedded watermark image is extracted by performing a reverse operation of the embedding process on watermarked image. It is divided into four sub-bands by applying 2-level DWT to watermarked images. The sub-band LL is considered, followed by SVD to extract the watermark logo. The extraction procedure is detailed step by step below.

1) Consider watermarked image (W) of dimensions ($S \times S$).
2) Perform AT on watermarked image (W) to obtain scrambled image $\tilde{W}$.
3) Apply 2-level DWT on scrambled watermarked image ($\tilde{W}$) as Eq. (13).

$$\begin{aligned}&[\tilde{LL}_{W1}, \tilde{HL}_{W1}, \tilde{HL}_{W1}, \tilde{HH}_{W1}]\\&\quad = DWT2(\tilde{W}, ' haar')\\&[\tilde{LL}_{W}, \tilde{HL}_{W}, \tilde{HL}_{W}, \tilde{HH}_{W}]\\&\quad = DWT2(\tilde{HH}_{W1}, ' haar') \qquad (13)\end{aligned}$$

4) Select sub-band (HH_W) and divided it into 8 × 8 blocks through Eq. (5).
5) Calculate entropy of each block by Eq. (6).
6) Select maximum entropy blocks ($\tilde{B}_N$) by step 6 of embedding method.
7) Perform SVD on maximum entropy blocks ($\tilde{B}_N$) as Eq. (14).

$$SVD(\tilde{B}_N) = U_W \times S_W \times U_W^T \tag{14}$$

8) Calculate principal component ($\tilde{B}_{pc}$) by Eq.(15).

$$\tilde{B_{pc}} = U_W \times S_W \tag{15}$$

9) Extract watermark image using Eq. (15) and Eq. (8) through Eq. (16).

$$E_{HH} = \frac{\tilde{B}_{pc} - B_{pc}}{\alpha} \tag{16}$$

10) Perform 2-level inverse DWT (IDWT) on E_{HH} to obtain the encrypted watermark image ($\tilde{w}_{HH}$) by using Eq. (17)

$$\begin{aligned} w2_{HH} &= IDWT2[LL_w, LH_w, HL_w, E_{HH}, 'haar'] \\ \tilde{w_{HH}} &= IDWT2[LL_{w1}, LH_{w1}, HL_{w1}, w2_{HH}, 'haar'] \end{aligned} \tag{17}$$

11) Finally, Perform IAT on $\tilde{w_{HH}}$ to recover watermark logo ($w^\star$) as Eq. (18)

$$w^\star = IAT(\tilde{w}_{HH}) \tag{18}$$

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This section critically evaluates the efficacy of the proposed method (MEB-DS) over imperceptibility and robustness. The imperceptibility is evaluated by two matrices, namely PSNR (peak signal to noise ratio) and SSIM (structural similarity index measure), whereas NC (normalized correlation) examines the robustness. A standard dataset having ten RGB color images is used to simulate the performance of the considered methods under different watermarking attacks. The Lena, Barbara, Airplane, Pepper, Baboon, Tulip, Sailboat, Swan, Bear, and Deer are used as cover images, while the Peugeot logo is used as a watermark. Figure 3 depicts both cover and watermark images respectively. The simulation results are carried out on a computer system having 16.0 GB RAM, dual-core 3.7 GHz CPU, and MATLAB 2020a. In terms of imperceptibility and robustness, we have compared the proposed method to five other watermarking methods, including Roy *et al.* [19], Zhang *et al.* [23], Liu *et al.* [24], Bhatti *et al.* [13], and Ernawan *et al.* [20].

A. IMPERCEPTIBILITY ANALYSIS

The PSNR and SSIM matrices evaluate imperceptibility between cover and watermarked images. PSNR is calculated by Eq. (19).

$$PSNR(c, W) = 10 \log_{10} \left(\frac{I_{max}^2}{MSE} \right) \tag{19}$$

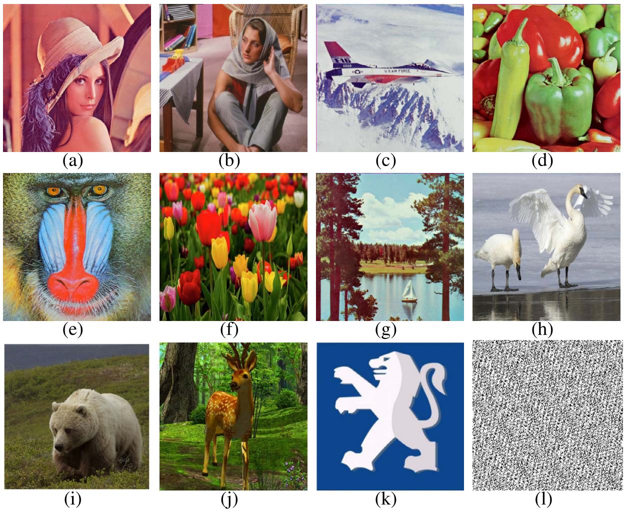


FIGURE 3. Cover (a-j) and watermark (k-l) images: (a) Lena, (b) Barbara, (c) Airplane, (d) Peppers, (e) Baboon, (f) Tulip, (g) Sailboat, (h) Swan, (i) Bear, (j) Deer, (k) Watermark, and (l) Scrambled.

$$PSNR(RGB) = \frac{1}{3}(PSNR_R + PSNR_G + PSNR_B) \tag{20}$$

where MSE is calculated by Eq. (21).

$$MSE = \frac{1}{M^2} \sum_{x=0}^{M-1} \sum_{y=0}^{M-1} (c(x, y) - W(x, y))^2 \tag{21}$$

SSIM is calculated by Eq. (22).

$$SSIM(c, W) = \frac{(2\mu_c \mu_W + c_1)(2\sigma_c \sigma_W + c_2)}{(\mu_c^2 + \mu_W^2 + c_1)(\sigma_c^2 + \sigma_W^2 + c_2)} \tag{22}$$

where σ_c is cover image standard deviation and μ_c is the cover image mean. c_1 and c_2 are constants.

Both Figures 4, 5, and Table 2 depict qualitative and quantitative analysis of the proposed method (MEB-DS) in terms of imperceptibility and robustness. This figure illustrates how similar the watermarked images are to the cover images. The MEB-DS has attained average PSNR, SSIM, and NC values as ***47.40***, ***0.9998***, ***0.9996*** respectively over the considered cover images, as shown in Table 2. Moreover, Table 3 tabulates the PSNR values, whereas Figure 6 also depicts the PSNR values over the considered methods. The table and figure show that the MEB-DS is better than the existing methods. Hence, the MEB-DS hides watermark logo efficiently without degrading cover image quality.

B. ROBUSTNESS ANALYSIS

The NC value measures robustness between watermark and recovered watermark images against 15 attacks over Lena image. Mathematically, NC is expressed by Eq. (23).

$$NC(w, w^\star) = \frac{\sum_{x=1}^{M} \sum_{y=1}^{M} w(x, y) w^\star(x, y)}{\sqrt{\sum_{x=1}^{M} \sum_{y=1}^{M} w(x, y)^2} \sqrt{\sum_{x=1}^{M} \sum_{y=1}^{M} w^\star(x, y)^2}} \tag{23}$$

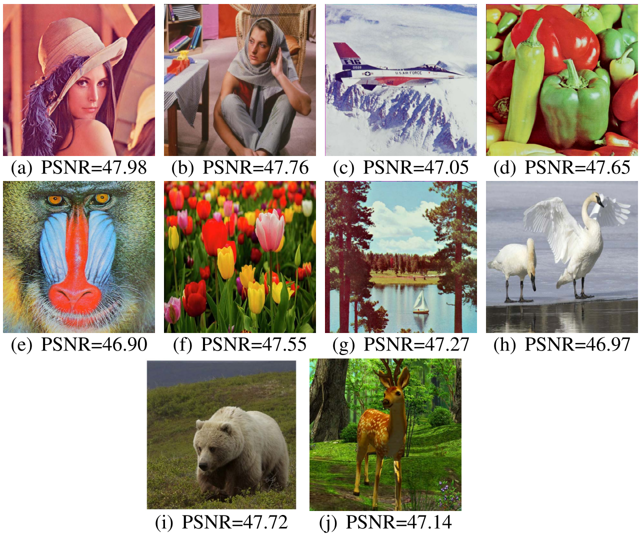

(a) PSNR=47.98 (b) PSNR=47.76 (c) PSNR=47.05 (d) PSNR=47.65
(e) PSNR=46.90 (f) PSNR=47.55 (g) PSNR=47.27 (h) PSNR=46.97
(i) PSNR=47.72 (j) PSNR=47.14

FIGURE 4. The qualitative and quantitative analysis of proposed method in terms of imperceptibility.

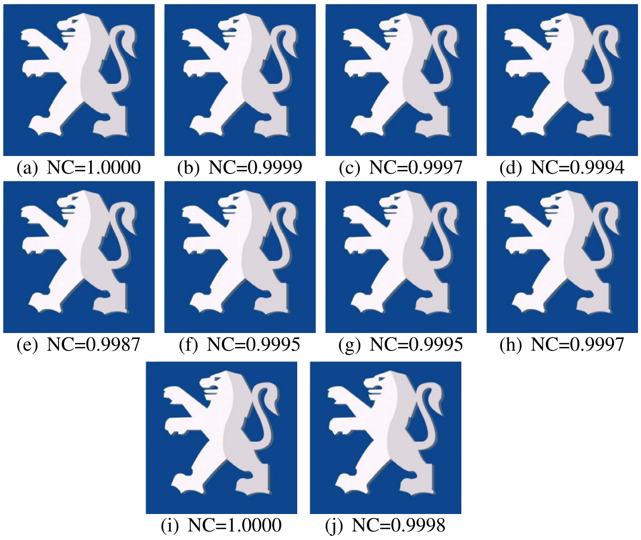

(a) NC=1.0000 (b) NC=0.9999 (c) NC=0.9997 (d) NC=0.9994
(e) NC=0.9987 (f) NC=0.9995 (g) NC=0.9995 (h) NC=0.9997
(i) NC=1.0000 (j) NC=0.9998

FIGURE 5. The qualitative and quantitative analysis of proposed method in terms of robustness.

These attacks are grouped into four categories: Geometrical, filtering, noise and contrast adjustment attacks. The details of these attacks are given. Moreover, each class is further discussed below.

1) **Geometrical attacks:** Rotation [RO (45°)], Scaling [RS (75%), Cropping [CR (50%)], Translation [TR (50, 50)], Shear [SR (x=1, y=0.2)], and Cutting [CU (20, 20)].
2) **Filtering attacks:** Wiener filtering [WF (5, 5)], Median filtering [MF (5, 5), and Average filtering [AF (5, 5)].
3) **Noise attacks:** Speckle noise [SN (0.05)], Salt & pepper noise [SPN (0.02), and Gaussian noise [GN (0, 0.1)].

TABLE 2. The performance of MEB-DS over considered images against no attack.

Cover image	PSNR	SSIM	NC
Lena	47.98	1.0000	1.0000
Barbara	47.76	0.9999	0.9999
Airplane	47.05	0.9998	0.9997
Pepper	47.65	0.9997	0.9994
Baboon	46.9	0.9996	0.9987
Tulip	47.55	0.9996	0.9995
Sailboat	47.27	0.9997	0.9995
Swan	46.97	0.9998	0.9997
Bear	47.72	1.0000	1.0000
Deer	47.14	0.9997	0.9998
Average	**47.40**	**0.9998**	**0.9996**

TABLE 3. Comparative analysis of PSNR values over considered methods.

Cover image	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
Lena	47.98	40.67	39.87	40.19	45.9	41.23
Barbara	47.76	40.60	39.83	39.97	44.87	41.04
Airplane	47.05	40.57	39.8	39.80	45.11	40.87
Pepper	47.65	39.90	39.77	39.55	44.92	41
Baboon	46.9	40.16	38.97	39.89	44.76	40.88
Tulip	47.55	40.61	39.15	39.73	43.85	40.28
Sailboat	47.27	39.95	39.75	39.64	43.82	39.89
Swan	46.97	40.10	39.56	38.98	44.74	40.16
Bear	47.72	40.29	38.92	39.00	44.86	40.23
Deer	47.14	40.13	39.64	40.64	44.27	40.09
Average	**47.40**	**40.30**	**39.53**	**39.74**	**44.71**	**40.57**

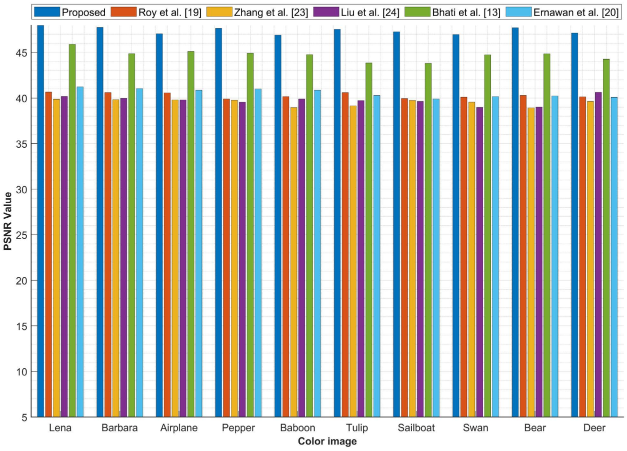


FIGURE 6. Comparative analysis of PSNR values over considered methods.

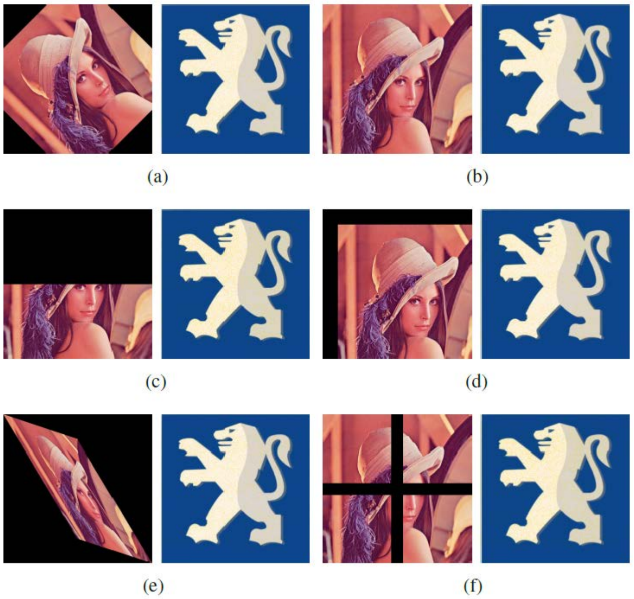


FIGURE 7. The quality of watermarked and recovered watermark images over various geometrical attacks: (a) Rotation (45°), (b) Scaling (75%), (c) Cropping (50%), (d) Translation (50, 50), (e) Shear (x=1, y=0.2), and (f) Cutting (20,20).

4) **Contrast adjustment attacks:** Sharpening [SP], Gamma correction [GC (0.7), and Histogram equalization [HE].

1) **Geometrical attacks:** Watermarked images are subjected to the six geometrical attacks listed above in order to get the NC value. The quality of the recovered watermark logo corresponds to each geometrical attack are shown in Figure 7. The MEB-DS efficiently extracts the better quality watermark logo under each geometrical attack. Moreover, comparative examination of NC values is depicted in Table 4. The proposed method obtains higher NC values as ***0.9937, 0.9976, 0.9897, 0.9961, 0.9990*** against each geometrical attack. In case of cropping attack, Liu *et al.* [24] outperforms over the other methods. Moreover, the average NC value, returned by considered methods are as ***0.9959, 0.9864, 0.9866, 0.9914, 0.9910, 0.9865***. However, the MEB-DS returns the highest average NC value. It can be observed from both Table 4 and Figure 8 that the MEB-DS performs better than the examined methods in this attack category.

TABLE 4. Robustness (NC) measurement for considered methods under various geometrical attacks.

S.No	Attack	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
1	RO	0.9937	0.9788	0.9875	0.9910	0.9903	0.9876
2	RS	0.9976	0.9860	0.9883	0.9915	0.9909	0.9878
3	CR	0.9897	0.9862	0.9860	0.9917	0.9901	0.9904
4	TR	0.9990	0.9894	0.9859	0.9906	0.9917	0.9851
5	SR	0.9961	0.9890	0.9884	0.9921	0.9919	0.9846
6	CU	0.9990	0.9889	0.9834	0.9913	0.9913	0.9832
	Average	**0.9959**	0.9864	0.9866	0.9914	0.9910	0.9865

* *RO: Rotation, RS: Scaling, CR: Cropping, TR: Translation,SR: Shear, CU: Cutting*

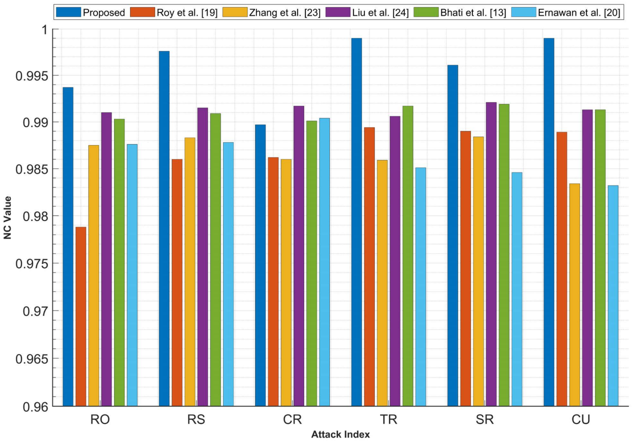


FIGURE 8. Comparative analysis of NC values against geometrical attacks over considered methods.

TABLE 5. Robustness (NC) measurement for considered methods under various filtering attacks.

S.No	Attack	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
1	WF	0.9996	0.9910	0.9890	0.9916	0.9927	0.989
2	MF	0.9992	0.9898	0.9903	0.9921	0.9919	0.9913
3	AF	0.9990	0.9907	0.9897	0.9910	0.9940	0.9901
	Average	**0.9993**	0.9905	0.9897	0.9916	0.9929	0.9901

* *WF: Wiener filtering, MF: Mean filtering, AF: Average filtering*

2) **Filtering attacks:** The three filtering attacks, namely wiener, median, and average with window size (5, 5), are encountered on watermarked images to examine robustness in terms of NC. Figure 9 illustrates the watermarked and extracted watermark images against each filtering attack. From the figure, it can be shown that the MEB-DS recovers the superior quality watermark logos. Furthermore, the comparative analysis of NC values returned by considered methods is depicted in both Table 5 and Figure 10. The MEB-DS returns the highest NC values as ***0.9996, 0.9992, 0.9990*** for wiener, median and average filters respectively. The average NC values returned by considered methods are as ***0.9993, 0.9905, 0.9897, 0.9916, 0.9929, 0.9901***. The MEB-DS achieves the highest average NC value as shown in Figure 10. Therefore, the MEB-DS performs outstanding against filtering attacks.

3) **Noise attacks:** The speckle, salt & pepper, and Gaussian noises are incorporated on watermarked image. The quality of the recovered watermark logos corresponds to each noise attack as illustrated in Figure 11.

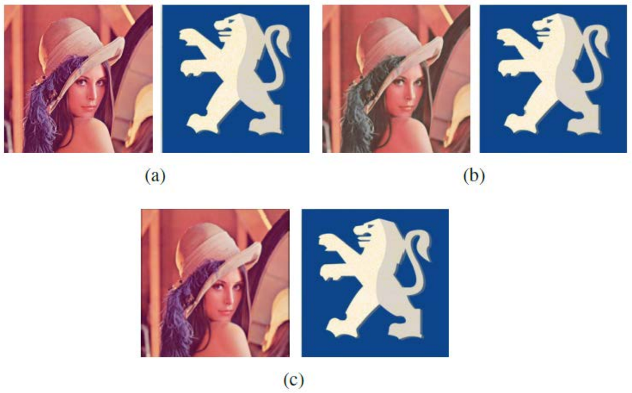


FIGURE 9. The quality of watermarked and recovered watermark images over various filtering attacks: (a) Wiener filtering (5, 5), (b) Median filtering (5, 5), and (c) Average filtering (5, 5).

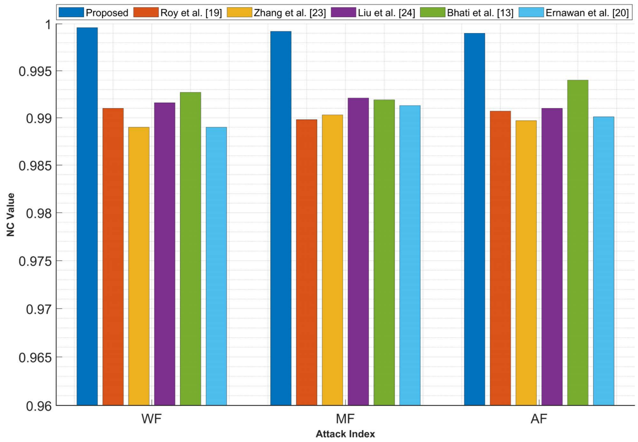


FIGURE 10. Comparative analysis of NC values against filtering attacks over considered methods.

This figure depicts that the MEB-DS recovers a quite recognizable watermark logo under each attack. However, the quality of extracted watermark slightly degraded. Table 6 and Figure 12 compare the NC values over the considered methods. The proposed method returns the highest NC value is ***0.9932*** against speckle noise. Moreover, the average NC values against considered methods are as ***0.9922, 0.9937, 0.9830, 0.9906, 0.9922, 0.9888***. These values confirm that the proposed method and Bhatti *et al.* [13] equally perform over the noise attacks.

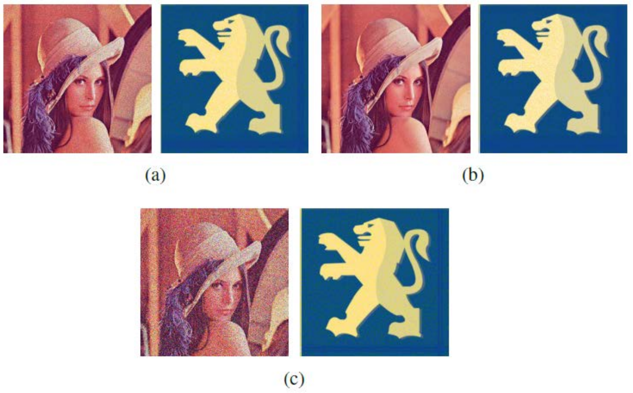


FIGURE 11. The quality of watermarked and recovered watermark images over various noise attacks: (a) Speckle noise (0.05), (b) Salt & pepper noise (0.02), and (c) Gaussian noise (0, 0.1).

TABLE 6. Robustness (NC) measurement for considered methods under various noise attacks.

S.No	Attack	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
1	SN	0.9932	0.9825	0.98678	0.9901	0.9920	0.9867
2	SPN	0.9923	0.9857	0.9797	0.9907	0.9910	0.9907
3	GN	0.9912	0.9830	0.9826	0.9911	0.9937	0.9889
	Average	**0.9922**	0.9837	0.9830	0.9906	**0.9922**	0.9888

* *SN: Speckle noise, SPN: Salt & pepper noise, GN: Gaussian noise*

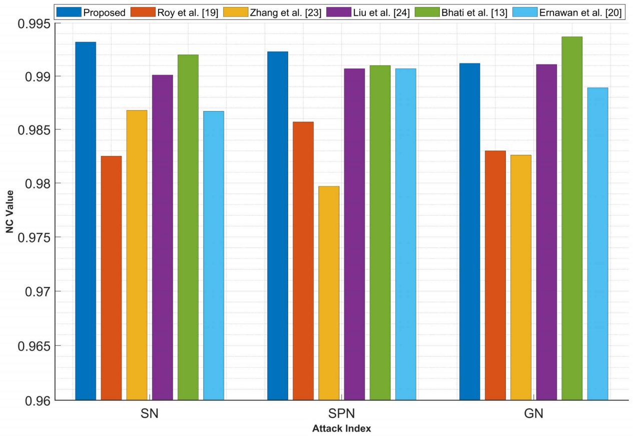


FIGURE 12. Comparative analysis of NC values against noise attacks over considered methods.

4) **Contrast adjustment attacks:** The sharpening, Gamma correction, and histogram equalization are three contrast adjustment attacks which are encountered on watermarked images. The MEB-DS recovers quite similar watermark logo as embedded watermark logo before, shown in Figure 13. The comparative analysis of NC values over considered methods are tabulated in Table 7 and depicted in Figure 14. The MEB-DS attains higher NC values as ***0.9995, 0.9989, 0.9993*** for sharpening, Gamma correction, and histogram attacks respectively. Furthermore, the considered methods return average NC values as ***0.9993, 0.9889, 0.9856, 0.9939, 0.9959, 0.9899***. However, the average NC value returned by the MEB-DS is highest. Therefore, the MEB-DS performs well under this category of attack.

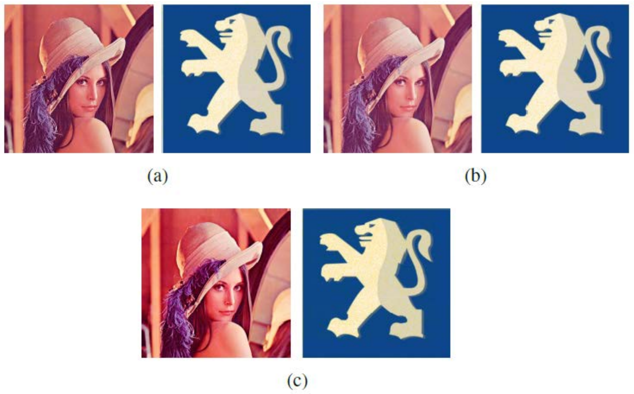


FIGURE 13. The quality of watermarked and recovered watermark images over various contrast adjustment attacks: (a) Sharpening, (b) Gamma correction (0.7), and (c) Histogram equalization.

TABLE 7. Robustness (NC) measurement for considered methods under various contrast adjustment attacks.

S.No	Attack	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
1	SP	0.9995	0.9898	0.9891	0.9984	0.9957	0.9910
2	GC	0.9989	0.9872	0.9797	0.9917	0.9943	0.9890
3	HE	0.9994	0.9896	0.9879	0.9916	0.9978	0.9897
	Average	**0.9993**	0.9889	0.9856	0.9939	0.9959	0.9899

* *SP: Sharpening, GC: Gamma correction, HE: Histogram equalization*

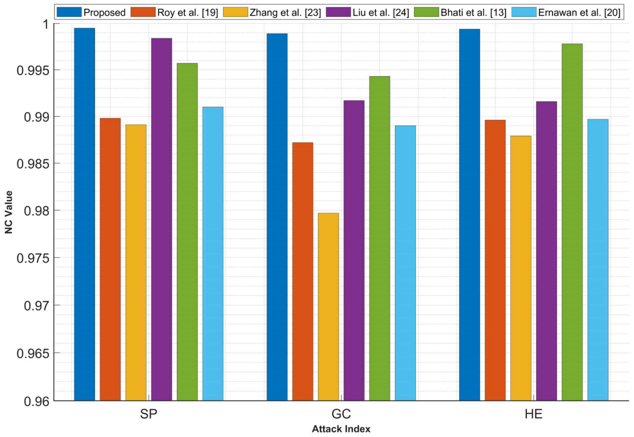


FIGURE 14. Comparative analysis of NC values against contrast adjustment attacks over considered methods.

C. FALSE-POSITIVE PROBLEM ANALYSIS

The reliability and stability of SVD-based watermarking methods make them a popular choice for many applications [15], [25], [26]. Generally, these methods use two approaches to hide the watermark into cover image. The first approach involves inserting the watermark directly into the singular component [15], [25]. Watermark singular matrix values are integrated into a singular component of cover image in the second method. A difficulty with these domain-based approaches is false-positive problem (FPP) which occurs due to hide watermark in the singular components. This can even result in the incorrect owner being authenticated. To alleviate this issue, the proposed method has hidden watermark logo in the principal component.

TABLE 8. The comparative analysis of time complexity (in seconds).

S.No	Procedure	Proposed	Roy et al. [19]	Zhang et al. [23]	Liu et al. [24]	Bhatti et al. [13]	Ernawan et al. [20]
1	Used method	AT, DWT, SVD	AT, RDWT, DCT	AT, SVD	DWT, HD, SVD, FOA	QFT, AT, CE	AT, RDWT, SVD
2	Embedding	5.09	14.21	8.17	17.31	9.13	13.90
3	Extraction	4.57	10.90	7.80	11.87	7.15	10.75
	Average	**4.83**	12.56	8.26	14.59	8.14	12.33

* *AT: Arnold transform, HD: Hessenberg decomposition, FOA: Fruit fly optimization algorithm, QFT: Quaternion Fourier transform, CE: Chaotic encryption*

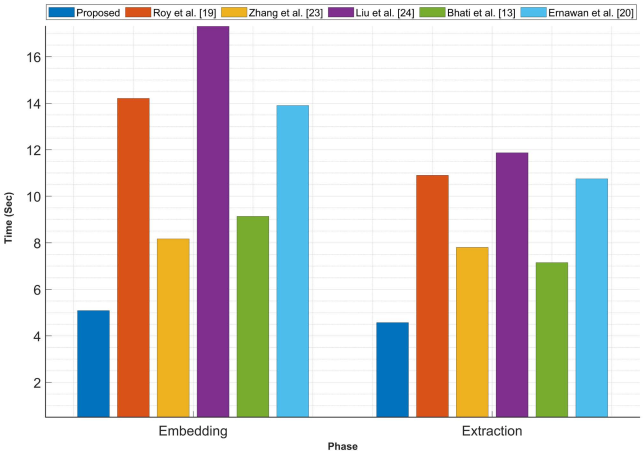


FIGURE 15. Comparative analysis of embedding and extraction time values over considered methods.

D. TIME COMPLEXITY ANALYSIS

This section computes the complexity of the MEB-DS along with existing methods in terms of time. The time complexity is proportional to the time required for embedding and recovering a watermark. The MEB-DS has been compared to five recently existing methods. Liu *et al.* [24] method uses DWT, SVD, HD, and FOA algorithms, termed as DWT-FOA. Bhatti *et al.* [13] method uses Quaternion Fourier transform (QFT), Arnold transform, and Chaotic encryption (CE), termed as (QFT-AC). The proposed method uses only three methods: Arnold Transform, DWT, and SVD. However, the proposed method relies on maximum entropy blocks to hide the watermark. Table 8 and Figure 15 compare all methods over embedding and extraction time. The table demonstrates that the proposed method takes significantly less time to hide and recover the watermark logo than the existing methods. As a result, the proposed method is very efficient due to its low time complexity.

V. CONCLUSION AND FUTURE WORK

Color images are becoming more prevalent in people's lives due to the fast growth of Internet technology, and the need for color image copyright management is becoming increasingly urgent. Therefore, this paper introduced a false-positive free watermarking method based on the selection of maximum entropy blocks in frequency domain. The proposed method improves the imperceptibility by hiding watermarking into the maximum entropy blocks. Moreover, false-positive problem is mitigated by embedding watermark within the principal components. Under different watermarking attacks, the proposed method has been assessed on standard image datasets in terms of PSNR, SSIM, and NC values. The experimental findings confirm that the proposed method performs superior to the considered methods. This work can be extended over video datasets to resolve the camcording issue.

REFERENCES

[1] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.

[2] S. Roy and A. K. Pal, "An SVD based location specific robust color image watermarking scheme using RDWT and Arnold scrambling," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2223–2250, Jan. 2018.

[3] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "Robust image watermarking scheme in lifting wavelet domain using GA-LSVR hybridization," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 1, pp. 145–161, Jan. 2018.

[4] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, and T. Yao, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398–30409, 2019.

[5] T. Zong, Y. G. Xiang, S. Guo, and Y. Rong, "Rank-based image watermarking method with high embedding capacity and robustness," *IEEE Access*, vol. 4, pp. 1689–1699, 2016.

[6] S. Garg and R. Singh, "An efficient method for digital image watermarking based on PN sequences," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 9, p. 1550, 2012.

[7] D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, Jun. 2017.

[8] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Color image blind watermarking scheme based on QR decomposition," *Signal Process.*, vol. 94, no. 1, pp. 219–235, Jan. 2014.

[9] K. M. Hosny, M. M. Darwish, and M. M. Fouda, "Robust color images watermarking using new fractional-order exponent moments," *IEEE Access*, vol. 9, pp. 47425–47435, 2021.

[10] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, Apr. 2020, Art. no. 164562.

[11] J.-M. Shieh, D.-C. Lou, and M.-C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Comput. Standards Interface*, vol. 28, no. 4, pp. 428–440, Apr. 2006.

[12] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, Mar. 2014.

[13] U. A. Bhatti, Z. Yu, J. Li, S. A. Nawaz, A. Mehmood, K. Zhang, and L. Yuan, "Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption," *IEEE Access*, vol. 8, pp. 76386–76398, 2020.

[14] 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, 2017, Art. no. 170326.

[15] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.

[16] F. Huang and Z.-H. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR," *Pattern Recognit. Lett.*, vol. 25, no. 15, pp. 1769–1775, Nov. 2004.

[17] 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, Jan. 2019.

[18] 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.

[19] S. Roy and A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3577–3616, Feb. 2017.

[20] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *Vis. Comput.*, vol. 36, no. 1, pp. 19–37, Jan. 2020.

[21] W. H. Alshoura, Z. Zainol, J. S. Teh, M. Alawida, and A. Alabdulatif, "Hybrid SVD-based image watermarking schemes: A review," *IEEE Access*, vol. 9, pp. 32931–32968, 2021.

[22] 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.

[23] H. Zhang, C. Wang, and X. Zhou, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 45, p. 45, Aug. 2017.

[24] 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.

[25] J. M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *J. Vis. Commun. Image Represent.*, vol. 25, pp. 1149–1163, Jul. 2014.

[26] 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.

ROOP SINGH received the B.Tech. degree from the Bengal Engineering College, Kolkata, the M.E. degree (Hons.) in electronics and communication engineering from the Autonomous Engineering College, MITS Gwalior, and the Ph.D. degree from Uttarakhand Technical University, Dehradun, India. He is currently working as a Research Associate in biomedical engineering at the Indian Institute of Technology (IIT) Delhi. He has around ten years of experience in industry/research/ academics. His research interests include digital image processing, signal processing, and computer vision.

LILA IZNITA IZHAR (Member, IEEE) received the B.Eng. degree in electrical and electronic engineering from the University of the Ryukyus, Japan, the M.Sc. and Ph.D. degrees in electrical and electronic engineering from Universiti Teknologi PETRONAS (UTP), and the Diploma degree in electrical and electronic engineering from Imperial College London. She is currently a Senior Lecturer at the Electrical and Electronic Engineering Department, UTP. She has been in the department for more than ten years. She has 17 years of experience doing research in medical image processing and analysis. This has cultivated her interest in intelligent signal and imaging research for medical/health application. Her work has been published in various journal and presented at various biomedical conferences namely the IEEE Engineering in Medicine and Biology Society and the European Conference of the International Federation for Medical and Biological Engineering.

IRRAIVAN ELAMVAZUTHI (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electrical engineering from the University of Technology Malaysia (UTM), in 1989, and the Ph.D. degree from the Department of Automatic Control and Systems Engineering, The University of Sheffield, U.K., in 2002. He is currently an Associate Professor at the Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS (UTP), Malaysia. At UTP, he is attached to the Health Analytics Institute, where he is actively involved in robotics and automation-related research. Before joining UTP, he worked at the University Kuala Lumpur-Malaysia France Institute, Standards and Industrial Research Institute of Malaysia (SIRIM), and UMW Industrial Power. His membership in national and international professional bodies include the Board of Engineers Malaysia (BEM), the Institution of Engineers Malaysia (IEM), the Institution of Electrical and Electronic Engineering (IEEE), the American Association for the Advancement of Science, the IEEE Robotics and Automation Society, the IEEE Control Systems Society, the International Federation of Automatic Control (IFAC), and the Institute of Measurement and Control (InstMC, U.K.).

ALAKNANDA ASHOK received the Ph.D. degree in digital image processing from the Indian Institute of Technology (IIT), Roorkee. She had experience in various capacities like Nodal Officer of G. B. Pant University of Agriculture and Technology, Pantnagar, twice the Controller of Examination of UTU, Dehradun, a Senior Principal Scientist at CSIR, HQs Delhi, the Director of the Women Institute of Technology, Dehradun, a Committee Member of Ph.D., Academics, Administrative Council, and the Admission Committee of Uttarakhand Technical University (UTU), Dehradun. She has been working as the Dean of the College of Technology, G. B. Pant University of Agriculture and Technology, since February 2020. She has organized several national/international conferences, symposiums, workshops, webinars, and training programs. Several MOUs have been signed under her leadership. She has over 24 years of professional experience. Her work is in digital image processing application of renewable energy and application of the Internet of Things (IoT), wireless sensor networks, smart GIS-based water info systems, and e-health application. She is a member of various academic societies. She had chaired and was the keynote speaker in several conferences.

SUMIT AOLE received the B.E. degree in instrumentation engineering from RTM Nagpur University, in 2012, and the M.E. degree in instrumentation and control engineering from Mumbai University, in 2015. He is currently pursuing the Ph.D. degree with the Department of Instrumentation Engineering, SGGSIE & T, SRTM University, and attached to Universiti Teknologi PETRONAS, Bandar Seri Iskandar, Malaysia, for his research work. He also works as a Project Associate with the CSIR-CSIO, Department of Biomedical Applications, Chandigarh. His research interests include biomedical signal processing, wearable sensor technology, gait analysis, control systems, and rehabilitation robotic devices.

NAVEEN SHARMA is currently working as a Scientist with the Biomedical Division, CSIR-Central Scientific Instruments Organization, Chandigarh. He has ten years' experience in research and development. His research interests include biomedical image processing, computer vision, affective computing, machine learning, and cyber forensics and security. He is a Life Member of the Indian Science Congress.