ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Performance Analysis of Image Watermarking for Different Sub-bands Using LWT and Arnold Map

Sushma Jaiswal[1] and Manoj Kumar Pandey[2]

ABSTRACT

In this paper, blind image watermarking is proposed for grey-scale images using LWT and Arnold maps. A comprehensive analysis of robustness and imperceptibility for different sub-band is analyzed, and a robust sub-band against different attacks is determined for designing a system robust against intentional attacks or combined attacks. The importance of embedding a watermark in several sub-bands has been examined to increase the robustness against various image attacks while retaining a reasonable level of imperceptibility. During the study, robustness is analyzed and watched against the number of attacks such as compression attacks, noisy attacks, de-noising attacks, and geometric attacks. It is moreover seen that higher sub-bands are seen to offer good imperceptibility, and robustness performance depends on the nature of attacks. It has also been noticed that entire attacks affect the watermarked image in a different way. A standard image dataset is used to test the suggested concept, and it is discovered that sub-band 1 performs admirably for strength (robustness) and imperceptibility against different image attacks.

Article information:

Keywords: Arnold Map, Image Attacks, Image Watermarking, Lifting Wavelet Transform, Adaptive Threshold

Article history:
Received: December 10, 2022
Revised: April 2, 2023
Accepted: June 11, 2023
Published: June 24, 2023
(Online)

DOI: 10.37936/ecti-cit.2023172.250954

1. INTRODUCTION

The amount of online digital content is continuously increasing, and this has led to easier and more widespread illicit copying, modification, and distribution. Digital data is easily accessible, which puts content integrity and copyright protection at risk. The literature has made reference to a number of methods for ensuring copyright protection and preventing illicit data copying and modification, including image watermarking, Steganography, and cryptography [1]. Digital image watermarking is a procedure of providing authentication by extracting a watermark from digital media. On the basis of robustness, a watermark is divided into semi-fragile, robust, and fragile. A robust system has the capacity to resist all non-intentional and intentional attacks, whereas a semi-fragile system can tolerate distortion up to some level, and as opposed to semi-fragile, fragile cannot tolerate distortion at all [2]. Specific data can be added into either the spatial domain or frequency domain. Spatial domain methods are more straightforward and uncomplicated to implement than other frequency-domain methods, and frequency-domain-based techniques can tolerate more attacks than spatial domain methods [2]. In contrast, a semi-fragile system can tolerate distortion up to some level, and as opposed to a semi-fragile, a fragile cannot tolerate distortion at all [2]. Blind scheme based watermarking using the transformation domain is explored in this study. In the past various watermarking methods based on discrete cosine transform (DCT) [3-4], discrete Fourier transform (DFT) [5-6], discrete wavelet transform (DWT) [7-9], redundant discrete wavelet transform (RDWT) [10-12], lifting wavelet transform (LWT) [13-15] and singular value decomposition (SVD) [8, 16-17] have been given that utilizes the concept of perception of human and transformed signal in order to achieve the satisfying imperceptibility and enhanced robustness. Various transformation schemes and decomposition methods have been combined to improve the watermarking algorithm's performance [14, 17-19]. Various machine learning algorithm is also applied to strengthen the watermarking algorithms [13, 17, 20-22].

The DCT is a well-known transformationfor image processing and provides good energy compactions; in DCT, all the terms are representedin terms of the

[1,2] The authors are with Department of CSIT, Guru Ghasidas Central University Bilaspur, India., E-mail: jaiswal1302@gmail.com and manojpnd88@gmail.com

cosine function. DWT is also one of the image transformation techniques, and it can represent an image in both spatial and frequency domains simultaneously. However, during the IDWT process, it suffers from the problem of down-sampling, which leads to the development of RDWT. DFT is also one of the candidates among the image transformation techniques, and it represents a signal in terms of the Fourier series. One of the essential properties of DFT is that it is rotational, scaling, and translation (RST) invariant. Apart from these conventional transform methods, SVD is also a numerical tool used for data hiding and image compression. SVD is applied to improve the system's performance in most of the schemes [8, 16-17].

Another similar method for a grey-scale image has been given by Islam et al. [20], and in that, nine image sub-bands are analyzed out of 64 sub-bands with the objective of finding a sub-band that performs better in terms of robustness and imperceptibility. Sub-band 7 shows the best results. SVM is used for binary watermark extraction using RBF kernel.

Zhou et al. [21] have presented an adaptive threshold-based blind image watermarking using a support vector machine and genetic algorithm, in which 50 images out of 2700 images of size 256×256 are utilized, and genetic is used for optimization, and SVM is used for binary watermark extraction. It shows robustness against most of the image attacks except the cropping attack.

Ariatmanto & Ernawan [23] have presented adaptive scaling factor-based image watermarking using DCT transformation. In this, first, a cover image is converted into 8×8 pixels, and then based on the highest variance, the pixel is selected for the embedding process. The adaptive scaling factor is utilized for watermark embedding. Arnold transform is used to strengthen the watermarking process.

Rakhmawati et al. [24] have proposed blind image watermarking for JPEG images using adaptive embedding strength and distribution of quantified coefficients. In this scheme, the embedding strengths and coefficients are adaptively selected from the DCT frequency, and it shows a good balance between imperceptibility and robustness.

An adaptive color image watermarking has been proposed by Qingtang et al. [25] aimed to provide robustness against geometric attacks. Slant transformation is used to calculate the maximum entropy of the pixels blocks, and watermark embedding is done by using adaptive image size, adaptive quantization steps, adaptive watermark encoding, and adaptive embedding position. It shows larger watermark capacity, stronger robustness, and higher security against most of image attacks.

An image watermarking using non-sub-sampled contour-let transform (NSCT) domain, fast generic polar complex exponential transform (FGPCET) magnitudes, and non-symmetric mixtures (NSM) based hidden Markov tree (HMT) has been proposed by Wang et al. [26]. In this, embedding is done using the multiplicative method on NSCT and FGPECT, and extraction is done using the NSM-HMT model and using maximum likelihood criteria.

An adaptive class matrix-based image watermarking has been proposed by Guo et al. [27]. In this method, image watermarking is done using adaptive class matrix selection and modified error diffusion kernel. For watermark embedding, a scheme is proposed based on the correlation analysis and halftone statistics. The result shows that the given methods are good in terms of quality and robustness.

High-capacity QR decomposition-based blind color image watermarking using artificial intelligence has been proposed by Hsu et al. [28]. The watermark bit is embedded based on the pixel difference of two consecutive coefficients of 2*2 blocks, and then the A.I. technique is used to refine the quality of watermark images. It shows good quality watermark image along with good robustness.

During the literature review, it was found that a number of watermarking algorithms and adaptive strategies have been proposed in the wavelet domain, and various sub-bands have been utilized for watermarking. In different levels of transformation, LWT and DWT divided an image into different sub-bands, such as low-low, low-high, high-low, and high-high. A variety of approaches have selected various sub-bands for embedding, like H.L. selected for embedding by Khare & Srivastava [7], as it fulfills the requirements of imperceptibility and robustness. In another study [9], the L.L. sub-band is used for watermark embedding after Q.R. decomposition because embedding in L.L. sub-bands affects the imperceptibility of the watermark. Since embedding in L.H. sub-bands offers a reasonable mix between imperceptibility and robustness, Verma et al. [15], Ramanjaneyulu & Rajarajeswari [22], Song et al. [29], and Verma et al. [30] have adopted L.H. sub-band for watermark embedding. Some schemes have used L.L., L.H., H.L., and H.H. sub-bands in combination to improve the performance, like [31] has used a combination of L.H. and L.L. sub-bands of LWT transform to improve the results.

Verma, Jha, and Ojha [30] introduced the adaptive threshold-based scheme, which uses the L.H. sub-band of the third level of decomposition for watermarking. It exhibits good resistance to most image attacks, with the exception of Rotation, salt and pepper noise, and average filtering attacks. Lai & Sai [32] have used both L.L. and L.H. sub-bands for watermarking in the LWT-SVM domain, so after observing several works of literature, it has been found that it is of utmost importance to know the effect of sub-band selection on robustness and imperceptibility in the watermarking system in the adaptive threshold domain.

The novelty of the proposed work is that this paper presents a detailed analysis of watermarking performance for different sub-bands of the image, and this study may help to design robust watermarking against specialized types of image attacks. The proposed work aims to find the effect of robustness and imperceptibility of embedding watermarks in different sub-bands in the LWT domain. The various sub-bands have been selected for watermark embedding for the following concerns-

a) The majority of the information resides in the low-frequency component, but every image is different in terms of the frequency component.
b) Different attacks affect the frequency component of the image differently; for example, jpeg compression attacks eliminate all the components with high frequency.
c) To analyze the deviation in terms of robustness and imperceptibility for different sub-bands.

The contribution of the proposed work is as follows-

- In the proposed work, third-level LWT decomposition has been utilized for watermarking, and analysis has been done to know which sub-bands give good results with respect to robustness and imperceptibility.
- The robustness analysis might be useful to know the nature of the attacks, and one can prepare a system that is robust against a certain attack or set of related attacks.
- The proposed work is simple to implement, and keys and Arnold map used at different levels provide sufficient security.
- The proposed method performs superior to other similar existing methods.

The paper is organized like section 2 contains the watermark insertion and watermark extraction in different sub-bands. Section 3 contains the results and discussion. A comparative study is shown in section 4, and section 5 describes the conclusion and future work.

2. PROPOSED WATERMARKING SCHEME USING LWT AND ARNOLD MAP FOR DIFFERENT SUB-BANDS

This paper presents and examines adaptive threshold-based watermarking for various sub-bands combining the LWT and Arnold map. There are some methods suggested by Verma & Jha [33] and Verma, Jha & Ojha [30] that use the third level of sub-bands (LH3) for the watermark embedding process. However, none of them have demonstrated the effects of watermark embedding on various sub-bands in the adaptive threshold domain. As a result, there is room to examine the effects of using different sub-bands for watermarking. In this paper, all the third-level sub-bands are utilized to know the effects of watermarking on the performance of the system. The adaptive threshold-based approach has been used for extraction as it is one of the simplest and easiest approaches for the watermarking system. The watermark adding and extraction process have been discussed in the later sub-section.

2.1 Sub-bands selection

In this study, all the third-level sub-bands using LWT have been explored and utilized for the embedding of the watermark. Whenever an image is decomposed for the first level using LWT, are generated four sub-bands called LL1, LH1, HL1, and HH1, and when these sub-bands are again decomposed for the second level, each generates four more sub-bands called LL2, LH2, HL2, and HH2 results into total 16 sub-bands and again each sub-bands are again decomposed for third level, then each sub-bands generates four more sub-bands LL3, LH3, HL3, and HH3, leads to total 64 sub-bands generation, so in this way, there are 64 sub-bands obtained an experiment done for the entire 64 sub-bands. However, results and analysis are shown only for 9 bands which cover all the diverse frequency components from higher to lower. The nine subbands (bands) are mentioned as follows.

- band 1: LH3/LL2/LL1
- band 2: LH3/LH2/LL1
- band 3: LH3/HL2/LL1
- band 4: LH3/LH2/LH1
- band 5: LH3/HL2/LH1
- band 6: LH3/LH2/HL1
- band 7: LH3/HL2/HL1
- band 8: LH3/LH2/HH1
- band 9: LH3/HL2/HH1

In the above nine sub-band representation, HH1 represents diagonal details, LL1 represents approximation details, HL1 represent horizontal details, and LH1 represent vertical details of the first LWT partition. Similarly, HH2, LL2, HL2, and LH2, represent diagonal, approximation, horizontal, and vertical details of second-level LWT decomposition. Similarly, LL3, HL3, LH3, and HH3 represent approximation, horizontal, vertical, and diagonal details of third-level LWT decomposition. In the above sub-bands, the sub-band 1: LH3/LL2/LL1 implies the third-level LH3 sub-bands of second-level LL2 sub-bands derived from first-level LL1 sub-band details of the image. In the proposed scheme, the third level of LWT coefficients is rearranged using key 1, and then, the entire shuffled coefficient is grouped to form blocks of size 2x2 with no overlapping. Then, the entire corresponding blocks are rearranged using another key called key 2 to add another level of security. So in this way, there are total 1024 blocks of size 2×2 are obtained, and now, out of 1024 blocks, a total of 512 blocks are selected to embed binary watermark bits of size 512. For embedding the binary bits, the quantization of maximum coefficients is used. In the scheme presented by Verma, Jha & Ojha [30], the experiment is done on sub-band 1, and the embedding threshold T=12 and watermarking strength α=0.7 is utilized, for 15 standard images, including Lena, Peppers, and Mandril, etc. Watermarking strength α shows the strength of the watermark, and it should be between 0 and 1. It is used to get the minimal value of Υ so that the watermark is extracted efficiently.

Fig. 1 shows all 64 sub-bands and all the nine sub-bands are numbers 1-9 and highlighted using colors. In this watermarking scheme, a threshold value (T) is selected, aiming at balancing imperceptibility and robustness, which is one of the challenges of watermarking system. In the proposed scheme, the experiments have been done on different threshold T values, and the variation in the robustness and imperceptibility is exposed in the later section *results and discussion.*

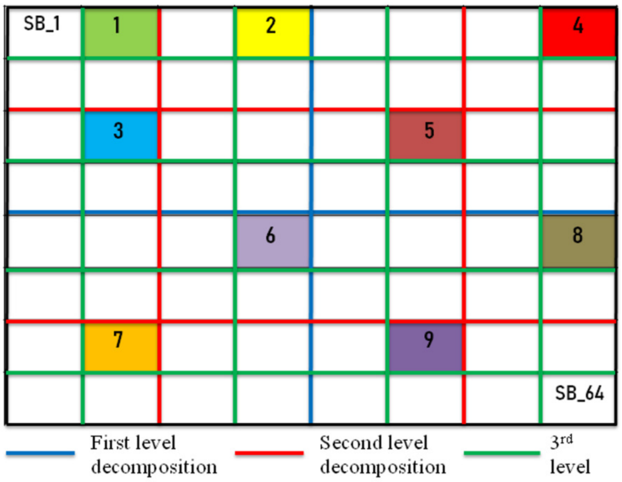


Fig.1: *Third level decomposition and Sub-band 1-9.*

2.2 Block Identification Method (BIM)

Firstly, the cover picture is partitioned into third-level LWT transformation, and the sub-band is further chosen for watermark embedding. The size of all the sub-band is 64×64, which is shuffled by applying a secret seed key (key1). Then the entire non-overlapping coefficients are arranged to form blocks of size 2×2. Then a different seed key (key 2) is used to arbitrarily shuffle these blocks as well. For every single block, calculate the CDmin (minimum coefficient difference) and CDmax (maximum coefficient difference) using the following formula.

$$CDmin = x(2) - x(1); \qquad (1)$$

$$CDmin = x(n) - x(n-1); \qquad (2)$$

Where a block contains four coefficients in order $x(1) < x(2) < x(n-1) < x(n)$ and CD_{max} is used for watermark embedding, and blocks for watermark embedding are selected using CD_{min}. The selection criterion for I.R. (important region) and NIR (non-important region) is as follows:

$$if\ \mathrm{CD}^{\mathrm{i}}\,\mathrm{min} <= T, \mathrm{i}^{\mathrm{th}} block\ belongs\ to\ IR. \qquad (3)$$

$$if\ \mathrm{CD}^{\mathrm{i}}\,\mathrm{min} > T, \mathrm{i}^{\mathrm{th}} block\ belongs\ to\ NIR. \qquad (4)$$

Where T = embedding threshold value.

2.3 Block Identification Method (BIM)

One of the challenges of image watermarking is to maintain the balance between imperceptibility and robustness, and therefore the selection of optimal threshold value is very important, therefore instead of selecting the threshold randomly, the selection is made by performing an experiment of Mandril standard image for different threshold values for T=11, 15, 25, 35 and 40. The imperceptibility (PSNR) for different thresholds is shown using Fig. 2, and Fig. 3 shows the robustness (N.C.) of the different thresholds for the Mandril image.

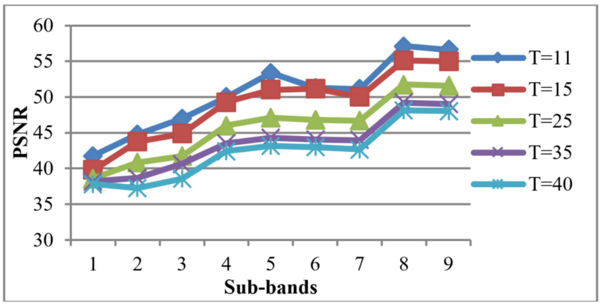


Fig.2: *PSNR value for different thresholds on Mandril.*

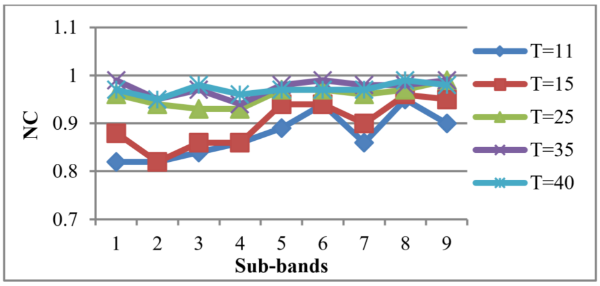


Fig.3: *N.C. value for different thresholds on Mandril.*

The experimental results depicted using Fig. 2 and Fig. 3 on different threshold value shows that by increasing the threshold value and keeping watermarking strength constant at α=0.7, the robustness (N.C. value) increases, but the imperceptibility (PSNR value) decreases. It has been understood from the results that T= 35 gives a balanced output in terms of PSNR and N.C. Therefore, all the results and analysis have been shown for T=35 and α=0.7.

2.4 Watermark adding procedure

This section contains the proposed watermark-adding procedure, and the mathematical formula for adding the watermark is as follows.

For each and every watermark, bit 1 or 0, quantize the largest coefficient of the corresponding blocks in I.R. using equations (5) and (6).
If watermark bit is =1,

$$x(n)_i = x(n)_i + T, \text{ifCD}^{\text{i}}\max < \max(\sigma, T); \quad x(n)_i, \quad \text{Ohtherwise} \tag{5}$$

And, if the watermark bit is =0,

$$x(n)_i = x(n)_i - \text{CD}^{\text{i}}\max \tag{6}$$

Where T represents the threshold, and CD^{i} max is the variation between two maximum coefficients for the consequent i^{th} block. The average variation (difference) value of the coefficient for entire N_b blocks is given by:

$$\sigma = \frac{\sum_{i=1}^{N_b} \text{CD}^i\max}{N_b} \tag{7}$$

Fig. 4 depicts the steps for the watermark embedding and extraction procedure.

2.5 Steps involved for watermark adding.

The following are the steps for inserting a watermark:

Step 1 Third-level LWT partitioning is used to divide the cover image, and **shuffle** (S.B.; Key1; S.B.') is used to randomly rearrange selected sub-band coefficients.

Step 2 Successive non-overlapping coefficients of selected bands are arranged to make blocks of size (2×2), and all the related blocks are randomly rearranged using shuffle (SBL, Key2; SBL').

Step 3 Blocks (which are randomly rearranged) are partitioned using BIM to get I.R. and NIR (Non-important region) subsequently.

Step 4 The average of all coefficient variation for all Nb blocks present in I.R. is found out using eq. (7).

Step 5 The watermark(W) is scrambled using an Arnold map and then converted to a 1-D array of length Nw.

Step 6 For every Nw bit (watermark bit), do the following:

6.1 Randomly select 512 blocks from the I.R. (where $Nw < Nb$), and find the two largest coefficient values $x(n)$ and $x(n-1)$ for given blocks.

6.1 If the watermark bit is equal to 1, modify $x(n)$ using (5).

6.1 If the watermark bit is equal to 0, modify $x(n)$ using (6).

Step 7 All updated and leftover blocks of I.R. and NIR are combined into the novel place positions.

Step 8 Entire updated coefficients and blocks of elected sub-band are shuffled in inverse order using the same keys.

2.6 The decoder design

The given watermarking method is blind; therefore, it doesn't need a cover image and original watermark image for extraction of the watermark. Here the adaptive-threshold-based idea is used for the extraction of the watermark. Here adaptive threshold Υ is determined as

$$\Upsilon = \frac{\sum_{i=1}^{Nw \times \alpha} \Phi' i}{Nw \times \alpha} \tag{8}$$

Here Φ'i is a set of {CD'$_{\max 1}$,CD'$_{\max 2}$,. . .,CD'$_{\max i}$, for i=1,2,. . .,Nw. Here all the maximum coefficient difference is set increasingly. Here factor α is applied to ensure the minimum Υ for watermark extraction, where $0 < \alpha \leq 1$.
The bits of watermark is extracted using the following rules:

$$watermark_{bit} = 1, \quad if(\text{CD}'_{\max \text{i}} \geq \min(\Upsilon, T) \quad 0, \quad \text{Ohtherwise} \tag{9}$$

2.7 Watermark extraction steps

The step for extraction of the watermark is as follows:

Step 1 The coefficients of a watermarked image are extracted, similar to an embedding-like process.

Step 2 With the help of identical keys, i.e., Key1 and Key2, the values and consequent blocks of the HL3 sub-band are shuffled at random.

Step 3 Determine which blocks' positions include the watermark bits.

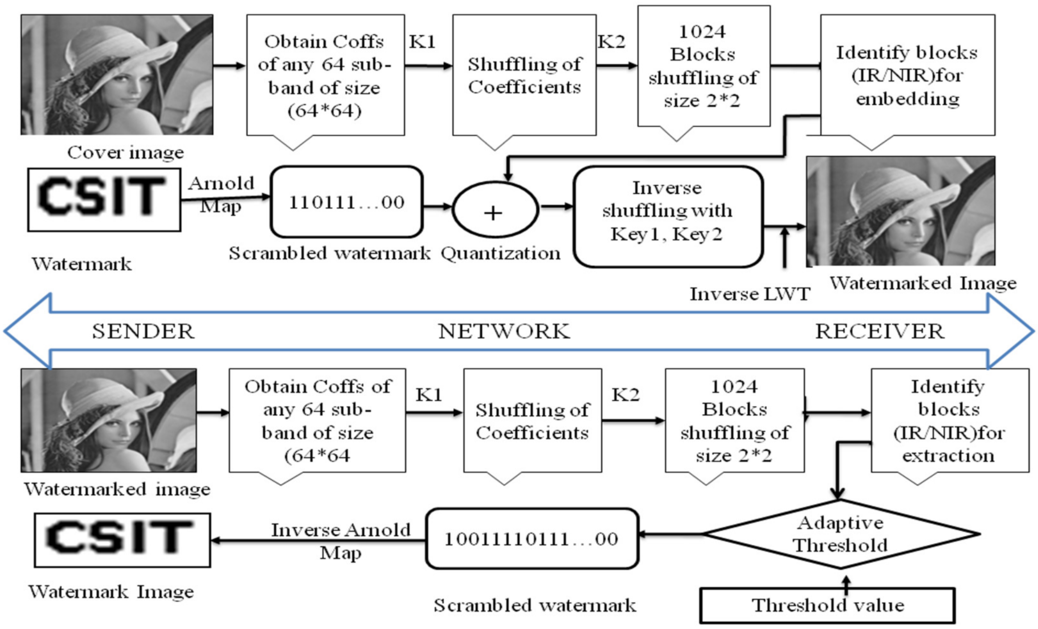

Cover image
Obtain Coffs of any 64 sub-band of size (64*64)
K1
Shuffling of Coefficients
K2
1024 Blocks shuffling of size 2*2
Identify blocks (IR/NIR)for embedding
CSIT
Watermark
Arnold Map
110111...00
Scrambled watermark
+
Quantization
Inverse shuffling with Key1, Key2
Inverse LWT
Watermarked Image
SENDER
NETWORK
RECEIVER
Watermarked image
Obtain Coffs of any 64 sub-band of size (64*64
K1
Shuffling of Coefficients
K2
1024 Blocks shuffling of size 2*2
Identify blocks (IR/NIR)for extraction
CSIT
Watermark Image
Inverse Arnold Map
10011110111...00
Scrambled watermark
Adaptive Threshold
Threshold value

Fig.4: *Watermark embedding and extraction process for all sub-bands.*

Step 4 Do the following for all the Nw blocks:

4.1 Obtain two maximum coefficients $x(n)$', $x(n-1)$' for each block, and get CD'$_{\text{max}}$i

4.1 The watermark bits are obtained utilizing eq. (9)

Step 5 The obtained values are saved in 1-D array W' having length Nw, and then, inversely, shuffled the obtained scrambled watermark is using the Arnold map.

Step 6 Change the shape of extracted watermarks to the size of the novel watermark.

3. RESULTS AND DISCUSSION

The adaptive threshold-based watermark scheme is tested on 15 gray-scale images of size (512×512) and a binary watermark of size (16×32). For the experiment and analysis, various images such as Lena, Peppers, Mandril, Cameraman, Lake, Jetplane, House, Livingroom, Walkbridge, Man, Boat, Satellite, Woman, Galaxy, and Chest X-ray are considered, but for briefness result of only five images are shown. The entire image used for the experiments are standard gray-scale images having 512×512 dimensions, and one binary image (created by my own) of dimension 16×32 is utilized in the proposed research. These image data are collected from the standard image dataset available in [34]. The experiment was carried out using Windows 10 and MATLAB (R2016a). A Lenovo laptop with an Intel i5 processor and 16 G.B. of RAM was used for the experiment. Fig. 5 represents the sample of 15 standard images. For the sake of concision, Fig. 6 illustrates the conventional Mandril image of size 512×512 and watermarked image under no attack circumstance while the embedding is carried out on sub-band 1.

Imperceptibility is measured using the peak signal-to-noise ratio (PSNR), and robustness is evaluated using normalized correlation coefficient (N.C.) and bit error rate (BER). The performance of the system is examined and assessed using PSNR, NC, and BER in the suggested work. PSNR is used to compare the original cover image to the watermarked version, and N.C. and BER are used to compare the extracted watermark to the original watermark.

The mean square error (MSE) between the original CI (cover image) and W.I. (watermarked image) is obtained using.

$$\mathrm{MSE} = \frac{1}{\mathrm{M{*}N}} \sum_{\mathrm{ij=0}}^{\mathrm{MN}} \mathrm{CI(i,j)} - \mathrm{WI(i,j)} \tag{10}$$

Where M*N shows the dimension of the images and CI(i, j) and W.I. (i, j) represent the grey value at position (i, j). The PSNR can be represented as:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}} \tag{11}$$

N.C. value and BER value can be calculated as follows:

$$\mathrm{NC} = \frac{\sum_i W_{ij} \sum_j W'_{ij}}{\mathrm{h \times w}} \tag{12}$$

W_{ij} and W'_{ij} are valued at (i,j) of cover and watermarked image, and it is set as 1 if it is a watermark bit 1; Otherwise, it is set as -1; h and w are watermark image dimensions, respectively.

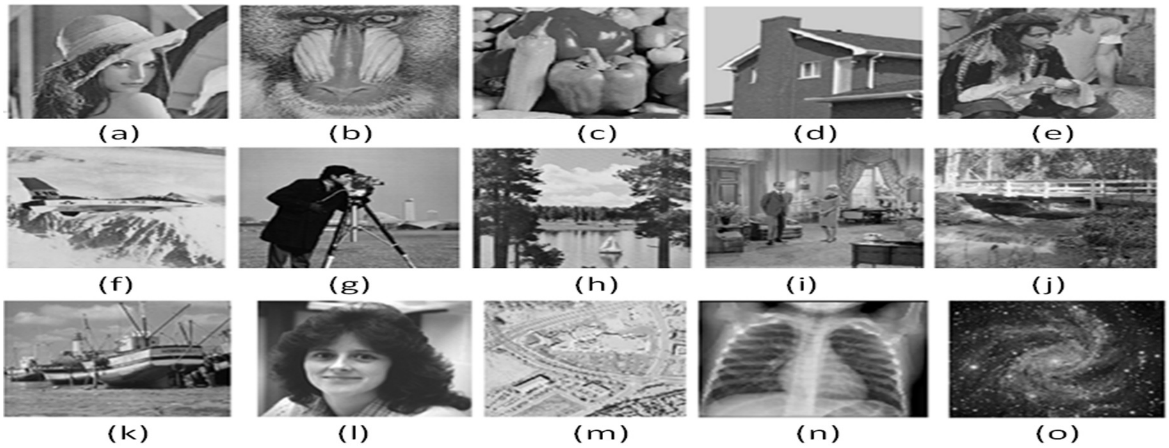


Fig.5: *Standard test image (a) Lena, (b) Mandril, (c) Peppers, (d) House, (e) Man, (f) Jetplane, (g) Cameraman, (h) Lake, (i) Livingroom, (j) Walkbridge, (k) Boat, (l) Woman, (m) Satellite, (n) Chest X-ray, and (o) Galaxy.*

$$\mathrm{BER} = \frac{\mathrm{B}}{\mathrm{h} \times \mathrm{w}} \tag{13}$$

Where B is equal to the wrongly detected bit, and h*w is the dimension.

3.1 Imperceptibility study

In this section, the imperceptibility of the proposed algorithm on different images for dissimilar sub-bands is discussed.

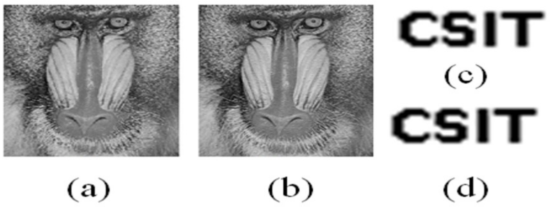


Fig.6: *(a) Cover image of size (512×512), (b) watermarked Mandril image having PSNR=38.19, (c) watermark image of size (16×32), (d) obtained watermark on sub-band 1 with NC=1 and BER=0.*

In this study, imperceptibility and robustness are monitored for different threshold values, and for lower values of T, imperceptibility increases and robustness drops. It has been noticed during the study that embedding watermarks on L.L. sub-bands affects the imperceptibility, and embedding on L.H. or H.L. sub-bands improves the robustness.

It has been noticed that different images have different color combinations and different illumination; therefore, all the images do not perform equally in terms of robustness and imperceptibility. Fig. 7 shows the PSNR value for five standard images, i.e., Lena, Mandril, Peppers, Cameraman, and Lake, for T=35 and embedding strength=0.7. Table 1 shows the extracted watermark and N.C. value against various image attacks for sub-band 1 to 9 for standard image Lena.

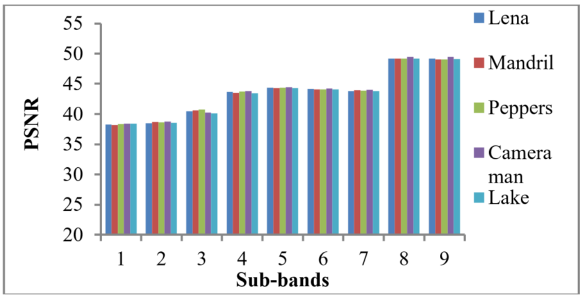


Fig.7: *PSNR variation of 5 standard images.*

3.2 Robustness analysis

In this study, N.C. and BER values are used to measure the robustness of the extracted watermark. The robustness of the proposed scheme has been tested on sub-band 1 to sub-band 9, which covers sub-bands of high-frequency to sub-bands of low-frequency on 5 standard images. The attacks considered for the study purpose are the compression attack, geometric attack, image processing attack, noisy attack, and de-noising attacks, respectively.

It is very clear from Table 1 that sub-band 1 is performing well in terms of robustness and imperceptibility. Table 2 shows the average robustness performance in terms of N.C. value for 15 standard images (average) for different sub-bands. The paper's later section discusses the robustness analysis of several attack categories.

3.2.1 Strength against geometric attacks

The robustness against geometric attacks, i.e., scaling and cropping attacks, has been considered for the study purpose, and evaluation has been done on

Table 1: *Extracted watermark and N.C. of extracted watermark under different attacks.*

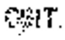
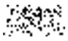
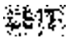
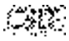
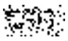
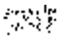
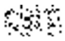
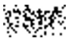
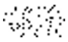
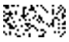
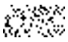
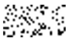
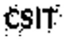
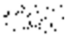
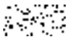
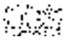
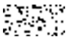
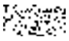
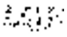
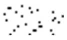
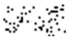
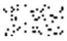
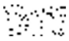
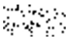
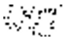
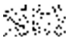
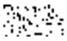
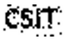
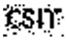
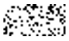
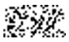
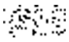
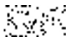
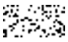
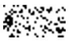
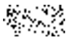
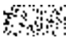
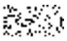
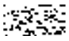
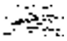
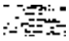
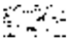
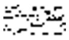
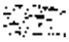
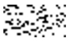
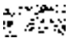
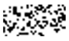
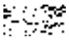
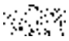
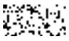
Attacks	Sub-band 1	Sub-band 2	Sub-band 3	Sub-band 4	Sub-band 5	Sub-band 6	Sub-band 7	Sub-band 8	Sub-band 9
SLP(0.01)									
NC Value	0.9844	0.8047	0.8203	0.5664	0.6601	0.6133	0.5781	0.3711	0.1641
SPLN(0.01)									
NC Value	0.8867	0.8515	0.6406	0.4609	0.625	0.6054	0.4218	0.1601	0.3281
GN(0.01)									
NC Value	0.9297	0.5934	0.4766	0.4961	0.3125	0.3242	0.3594	0.2891	0.2304
HE									
NC Value	0.9844	0.8789	0.9023	0.8867	0.9218	0.8477	0.9179	0.9290	0.8594
SCL(0.5)									
NC Value	0.9140	0.986	0.7227	0.4882	0.4140	0.3867	0.2968	0.3047	0.2969
MF(2x2)									
NC Value	0.9727	0.8516	0.9375	0.6367	0.4648	0.3984	0.6289	0.3555	0.4101
MF(3x3)									
NC Value	0.9609	0.9492	0.9296	0.3203	0.4727	0.5117	0.6132	0.3320	0.3359
CR (10%)									
NC Value	0.8594	0.8516	0.2539	0.8007	0.2656	0.2929	0.3085	0.3307	0.2070
CR (25%)									
NC Value	0.6679	0.6289	0.2851	0.6172	0.4218	0.4179	0.2578	0.3320	0.1016
RT(0.1)									
NC Value	0.7266	0.6563	0.7617	0.4297	0.3046	0.3867	0.3594	0.6562	0.3710
JPEG (20)									
NC Value	0.7578	0.7109	0.6914	0.7575	0.3086	0.3437	0.6601	0.0965	0.2070
JPEG (30)									
NC Value	0.9882	0.8710	0.8047	0.7773	0.1367	0.3906	0.7813	0.2188	0.3086
JPEG (40)									
NC Value	0.9787	0.8750	0.9414	0.8086	0.3906	0.2929	0.8007	0.3633	0.0585
JPEG (50)									
NC Value	0.9258	0.8477	0.8984	0.7969	0.2929	0.8906	0.9258	0.1875	0.2773
JPEG (60)									
NC Value	1.0	0.9101	0.8164	0.9687	0.3867	0.9296	0.9336	0.2382	0.1875
Avg. NC Value	**0.9024**	**0.8179**	**0.7255**	**0.6541**	**0.5208**	**0.5088**	**0.5898**	**0.3443**	**0.2896**

Table 2: *Robustness measure (over 15 images) of extracted watermark for various attacks.*

Attacks	S_band 1	S_band 2	S_band 3	S_band 4	S_band 5	S_band 6	S_band 7	S_band 8	S_band 9
SLP (0.01)	0.86	0.72	0.74	0.46	0.51	0.55	0.53	0.35	0.34
SPLN(0.01)	0.83	0.67	0.65	0.50	0.45	0.58	0.49	0.23	0.34
GN (0.01)	0.85	0.60	0.51	0.32	0.37	0.40	0.32	0.27	0.20
HE	0.93	0.91	0.91	0.89	0.88	0.87	0.88	0.85	0.85
SCL(0.5)	0.93	0.84	0.75	0.32	0.43	0.36	0.4	0.28	0.29
MF (2×2)	0.83	0.71	0.87	0.58	0.21	0.25	0.61	0.32	0.28
MF (3×3)	0.91	0.83	0.87	0.43	0.45	0.43	0.67	0.40	0.36
CR (10%)	0.75	0.68	0.41	0.62	0.34	0.29	0.22	0.27	0.29
CR (25%)	0.59	0.53	0.40	0.42	0.40	0.40	0.25	0.39	0.24
RT (0.1)	0.71	0.68	0.58	0.31	0.38	0.34	0.33	0.65	0.46
JPEG (40)	0.79	0.80	0.72	0.76	0.30	0.29	0.84	0.25	0.27
JPEG (60)	0.99	0.91	0.74	0.86	0.41	0.94	0.85	0.31	0.26

five standard images. Fig. 8, Fig. 9, and Fig. 10 show the N.C. value of different images under scaling (SCL 0.5), cropping (C.R. 10%) attack, and rotation (RT 0.1), respectively.

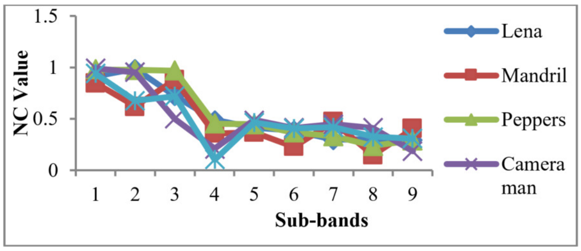


Fig.8: *N.C. variations scaling (0.5) attack.*

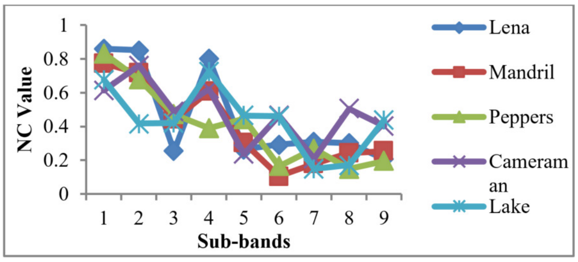


Fig.9: *N.C. variations against cropping (10%) attack.*

The proposed scheme gives good robustness against the cropping attacks; one can observe from Fig. 8 that lower sub-bands perform better against cropping attacks in terms of N.C. value; this may be due to lower sub-bands remaining less affected than the higher frequency sub-bands. Fig. 11 shows the performance against the Rotation (0.1) attack for sub-band 1 to 9, and one can observe that the lower sub-bands perform better than higher sub-bands, and this may be because lower sub-bands are less affected by rotation attack than the higher sub-bands. Sub-band 8 is also performing well against rotation attacks. Sub-band 1 provides an average N.C. value of 0.93 for the SCL (0.5) attack, 0.75 for the Crop (10%) attack, and 0.71 for the Rotation (0.1) attack.

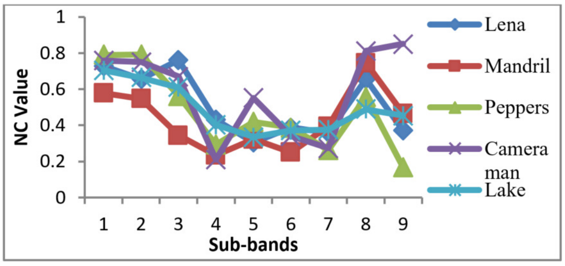


Fig.10: *N.C. variations against rotation (0.1) attack.*

3.2.2 Robustness against noisy and de-noising attacks

The robustness of the scheme has been tested against the noising attacks, i.e., salt and pepper (SLP) noise with intensity 0.01, speckle noise (SPLN) with intensity 0.01, de-noising attack, i.e., histogram equalization (HE) and the median filter (3×3). It is analyzed from Fig. 11 and Fig. 12 that the proposed scheme provides sufficient robustness against SLP and SPLN attacks, especially for lower-level sub-bands (sub-band 1 – 3). The lower level sub-bands may be less affected by SLP and SPLN attacks; therefore, they perform well.

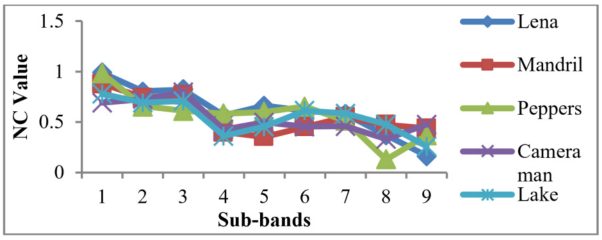


Fig.11: *N.C. variations against SLP (0.01) attack.*

It is clear from Fig. 13 that in the case of the G.N. attack, the lower sub-band gives sufficient robustness compared to higher sub-bands; this may be

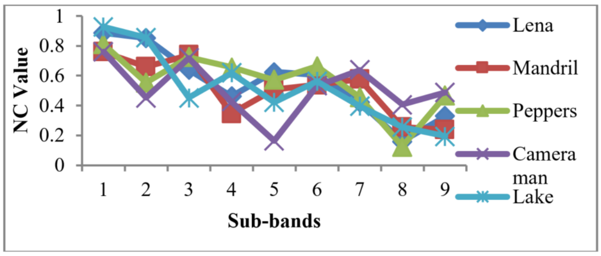


Fig.12: *N.C. variations against SPLN (0.01) attack.*

due to the Gaussian noise attack affecting more to higher frequency component. It is observed from Fig. 14 that for de-noising attacks like HE, it gives adequate robustness for all the sub-bands. It is obvious from Fig. 15 that lower-level sub-bands perform well against the median filter attack.

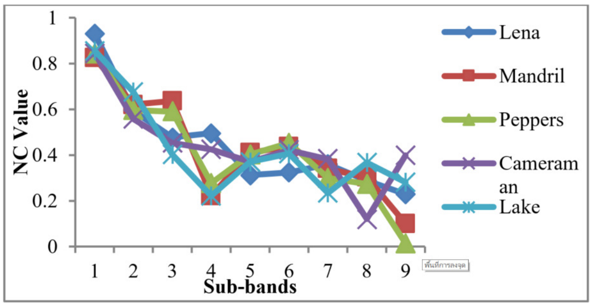


Fig.13: *N.C. variations against G.N. (0.01) attack.*

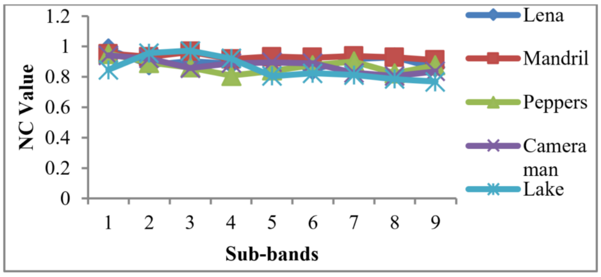


Fig.14: *N.C. variations against HE attack.*

It is observed that for noisy and de-noisy attacks, the proposed scheme gives average robustness of 0.86 for SLP (0.01) attack, 0.83 for SPLN (0.01), 0.85 for G.N. (0.01), 0.93 for Histogram Equalization (HE), 0.91 for M.D. (3×3) filter attack for sub-band 1.

3.2.3 Robustness against compression attacks

The system's robustness has been tested against lossy compression attacks, i.e., joint picture expert group (JPEG) for different compression factors of 40 and 60 on five standard images. The NC variation for JPEG (40%) and JPEG (60%) has been shown using Fig. 17 and Fig. 18.

One can observe from Fig. 16 that against JPEG (40%) attack, lower frequency sub-bands are performing well, and sub-band 7 is also giving good robustness as compared to other sub-bands. It is clear from Fig. 17 that for JPEG (60%) attack, lower frequency sub-bands, sub-band 6, and sub-band 7 are performing well in terms of N.C. value. The L.L. and L.H. sub-band provides excellent robustness against lossy compression attacks. It is observed that the proposed watermarking scheme gives an average robustness of 0.79 for JPEG (40%), 0.99 for JPEG (60%) attack on sub-band 1.

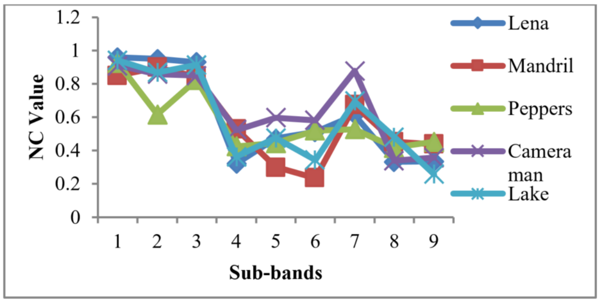


Fig.15: *N.C. variations against M.D. (3×3) attack.*

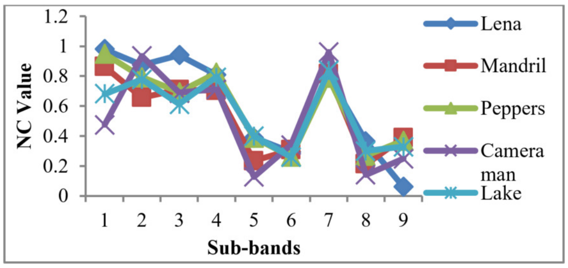


Fig.16: *N.C. variations against JPEG (40%) attack.*

4. COMPARATIVE PERFORMANCE ANALYSIS

The LWT and adaptive threshold-based watermarking for different sub-bands is presented, and the experiments are done to uncover the effect on the robustness and imperceptibility of the image. In this section, the performance of the proposed idea has been compared with other watermarking schemes. Fig. 7 shows that the PSNR value increases for each sub-band, ranging from approximately 39 dB to

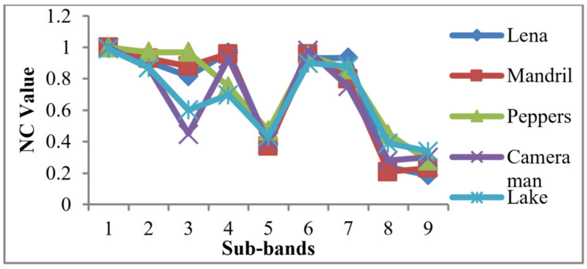


Fig.17: *N.C. variations against JPEG (60%) attack.*

Table 3: *Comparison of results with [15, 30, and 35] for various attacks in terms of N.C.*

Attacks	Lena				Peppers			Mandril		
	[15]	[30]	[35]	Proposed	[15]	[30]	Proposed	[15]	[30]	Proposed
SLP(0.01)	0.914	0.753	0.731	**0.984**	0.91	0.785	0.980	0.929	0.843	0.878
SPLN(0.01)	0.910	0.746	0.738	0.887	0.89	0.80	0.808	0.914	0.800	0.757
MD (3×3)	0.92	0.95	0.549	**0.96**	0.918	0.91	**0.925**	0.898	X	**0.898**
HE	0.933	0.92	0.98	**0.984**	0.937	0.88	**0.953**	0.895	X	**0.953**
CR (25%)	X	0.933	X	0.667	X	0.910	0.632	X	0.92	0.589
CR (10%)	0.99	X	0.917	0.859	0.972	X	0.832	0.96	X	0.773
SCL(0.5)	0.94	0.984	0.647	0.914	0.941	0.97	**0.98**	0.953	0.964	0.847
JPEG(30)	0.96	0.99	0.945	**0.99**	0.945	0.99	0.935	0.953	X	0.863
JPEG(40)	0.968	1.0	0.976	**0.978**	0.968	0.99	0.94	0.96	X	0.868
JPEG(50)	0.98	1.0	0.988	0.925	0.984	1.0	**1.0**	0.976	X	**1.0**
JPEG(60)	1.0	1.0	0.991	**1.0**	1.0	1.0	**1.0**	1.0	X	**1.0**

Table 4: *Comparison of results with [15, 30, and 35] for various attacks in terms of BER.*

Attacks	Lena				Mandril			
	[15]	[30]	[35]	Proposed	[15]	[30]	[35]	Proposed
SLP(0.01)	0.043	0.048	0.125	**0.007**	0.0352	0.0488	0.1465	0.084
HE	0.0332	0.0156	0.002	**0.007**	0.0257	0.0254	0.0020	0.023
SCL(0.5)	0.0273	X	X	**0.042**	0.0234	X	X	0.067
JPEG(30)	0.0195	0.0098	0.025	**0.005**	0.0234	0.0332	0.052	0.069
JPEG(40)	0.0156	0.0117	0.009	0.011	0.0195	0.0410	0.007	0.068

49 dB for different images. The watermark scheme must be robust against most image attacks, but it is also true that no watermark algorithm can be robust against all image attacks; therefore, the watermarking algorithm must be robust against most image attacks. Table 1 shows the extracted watermark and corresponding N.C. value on Lena's watermarked image against different attacks for different sub-bands, and one can observe that sub-band 1 provides the most optimal results. It exhibits a fair compromise between imperceptibility and robustness with an average N.C. value of 0.9024 and the PSNR value of approx 39 dB, which is adequate.

It can be said that sub-band 1 provides good optimal results; therefore, the performance of sub-band 1 is compared in terms of N.C. with the schemes such as Verma et al. [15], Verma et al. [30], and Islam et al. [35] and shown using Table 3. Fig. 18 shows the performance comparison with Verma et al. [30] on the Lena image, and it shows that except for the G.N. (0.01), C.R. (25%), SCL(0.5), and JPEG(50) attack, the proposed scheme performs well against most of the image attacks.

Table 4 shows the BER comparison with other schemes, such as Verma et al. [15], Ariatmanto & Ernawan [23], Verma et al. [30], and Islam et al. [35], and it shows that the proposed scheme performs well against most of the image attacks for Lena.

In Table 3 and Table 4, bold values show that the proposed scheme performs well or equally over another existing scheme for different image attacks, and the sign of X shows missing data.

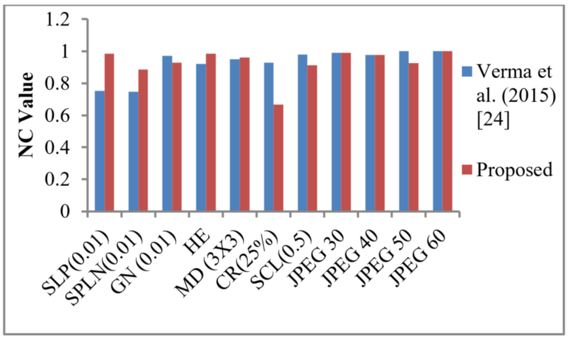


Fig.18: *N.C. Comparison with Verma et al. [24].*

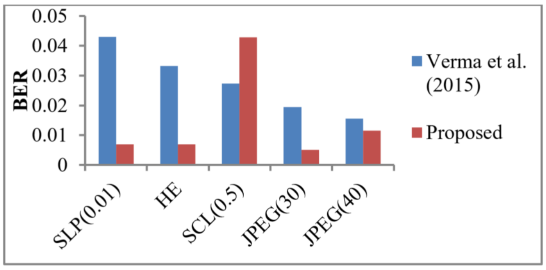


Fig.19: *BER Comparison with Verma et al. [15] against different attacks on Lena.*

Fig. 19 shows the comparison using BER with Verma et al. (2105) [15] for standard image Lena, and it shows that the proposed scheme performs well except for the SCL(0.5) attack. Fig. 20 shows the comparison of N.C. value under various compression attacks with Islam et al. (2020) [20], and it shows that the proposed scheme performs well against all compression attacks. N.C. comparison with Ariatmanto

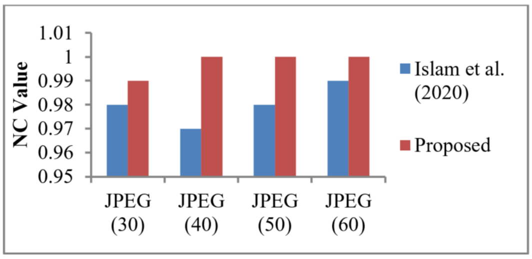


Fig.20: *N.C. compression with Islam et al. [20] for compression attacks on Lena.*

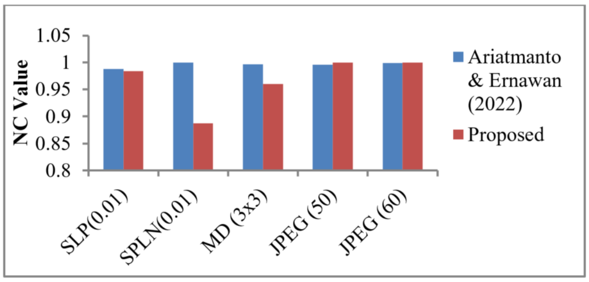


Fig.21: *N.C. Comparison with Ariatmanto & Ernawan [23] against various image attacks on Lena.*

& Ernawan (2022) [23] is shown using Fig. 21, and it shows that except for the SLP(0.01), SPLN(0.01), and M.D. (3×3) attacks, the proposed scheme performs well.

It is observed using comparative analysis that the proposed scheme performs well against the most common image attacks. It is noted from the comparative study that proposed LWT and Adaptive threshold-based watermarking for different sub-band gives better results irrespective of different attacks on different standard images.

5. CONCLUSION AND FUTURE WORK

This paper presents the LWT and adaptive threshold-based image watermarking performance for different sub-bands to find the effects on the imperceptibility and robustness of watermarked images. The different attack affects the robustness and imperceptibility of the system differently like the noise attack affects the N.C. and PSNR value differently than the geometric attack. The watermark embedding in all sub-bands except higher level sub-bands provides sufficient robustness against SLP and SPLN noise attacks. In the case of scaling and cropping attacks, the lower sub-bands provide good robustness, whereas the sub-band 7 and lower sub-band gives good robustness against compression attack. The H.H. sub-bands perform very poorly in terms of robustness for compression attacks, whereas the L.L. and L.H. sub-bands give optimal performance against compression attacks. Overall observation shows that, by means of averaging, sub-band 1 gives the most optimal performance for the strength and robustness of the watermark. The strength of the proposed scheme is that it is simple and efficient, but for some attacks, it needs further improvement. In the future, the proposed idea can be extended to use some machine or deep learning algorithm in order to improve the results.

ACKNOWLEDGMENT

The authors would like to thank the editor and the anonymous reviewers for their valuable comments and suggestions to improve the quality of this paper. This research received no specific grant from any funding agency.

References

[1] C. J. Biermann, *Handbook of Pulping and Papermaking*, 2nd ed. San Diego, California, USA, Academic Press, 1996.

[2] S. Kumar, B. K. Singh and M. Yadav, "A Recent Survey on Multimedia and Database Watermarking," *Multimedia Tools and Applications*, vol. 79, pp. 20149–20197, 2020.

[3] S. Liu, Z. Pan and H. Song, "Digital Image Watermarking Method Based on DCT and Fractal Encoding," *IET Image Process*, vol. 11, pp. 815–821, 2017.

[4] B. Lutovac, M. Daković, S. Stanković and I. Orović, "An algorithm for robust image watermarking based on the DCT and Zernike moments," *Multimedia Tools Application*, vol. 76, pp.23333-23352, 2017.

[5] D.G. Savakar and A. Ghuli, "Non-Blind Digital Watermarking with Enhanced Image Embedding Capacity Using Meyer Wavelet Decomposition, SVD, and DFT," *Pattern Recognition and Image Analysis*, vol. 27, pp. 511–517, 2017.

[6] V. Solachidis and I. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," in *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753, 2001.

[7] P. Khare and V. K. Srivastava, "A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT," *Journal of Intelligent Systems*, vol. 30, pp. 297–311, 2021.

[8] Singh D, Singh SK (2016) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl 76(11):13001–13024

[9] S. Jia, Q. Zhou and H. Zhou, "A Novel Color Image Watermarking Scheme Based on DWT and Q.R. Decomposition," *Journal of Applied Science and Engineering*, vol. 20, pp. 193–200, 2017.

[10] S. Singh, V. S. Rathore, R. Singh and M. K. Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain," *Multimedia Tools Application*, vol. 76, pp. 19113–19137, 2017.

[11] R. Thanki, A. Kothari and S. Borra, "Hybrid, blind and robust image watermark-

ing: RDWT–NSCT based secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, pp. 27593-27613, 2021.

[12] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *The Visual Computer*, vol. 36, pp. 19-37, 2020.

[13] R. Mehta, K. Gupta and A. K. Yadav, "An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain," *Multimedia Tools and Applications*, vol. 79, pp. 18657–18678, 2020.

[14] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimedia Tools and Applications*, vol. 78, pp. 30523–30533, 2019.

[15] V. S. Verma, R.K. Jha and A. Ojha, "Digital watermark extraction using support vector machine with principal component analysis-based feature reduction," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 75–85, 2015

[16] S. B. B. 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," *The Visual Computer*, vol. 37, pp. 385-409, 2021.

[17] A. Zear and P. K. Singh, "Secure and robust color image dual watermarking based on LWT-DCT-SVD," *Multimedia Applications and Services*, vol. 81, pp. 26721-26738, 2022.

[18] S. Roy and A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling," *Multimedia Tools and Applications*, vol. 76, pp. 3577–3616, 2017.

[19] A. K. Abdulrahman and S. Ozturk, "A Novel Hybrid DCT and DWT-Based Robust Watermarking Algorithm for Color Images," *Multimedia Tools and Applications*, vol. 78, pp. 17027–17049, 2019.

[20] M. Islam, A. Roy and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Computing and Applications*, vol. 32, pp. 1379–1403, 2020.

[21] X. Zhou, C. Cao, J. Ma and L. Wang, "Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm," *Hindawi, Mathematical Problems in Engineering*, Article ID 2685739, 9 pages, 2018.

[22] K. Ramanjaneyulu and K. Rajarajeswari, "Wavelet-based oblivious image watermarking scheme using genetic algorithm," *IET Image Processing*, vol. 6, no. 4, pp. 364-373, 2012.

[23] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 3, 605-614, 2022.

[24] L. Rakhmawati, W. Wirawan, S. Suwadi, C. Delpha and P. Duhamel, "Blind robust image watermarking based on adaptive embedding strength and distribution of quantified coefficients," *Expert Systems with Applications*, vol. 187, 115906, 2022

[25] S. Qingtang, D. Liu and Y. Sun, "A robust adaptive blind color image is watermarking for resisting geometric attacks," *Information Sciences*, vol. 606, pp. 194-212, 2022.

[26] X. Wang, F. Peng, P. Niu and H. Yang, "Statistical image watermark decoder using NSM-HMT in NSCT-FGPCET magnitude domain," *Journal of Information Security and Applications*, vol. 69, 103312, 2022.

[27] J.-M. Guo and S. Seshathiri, "Watermarking in dot-diffusion halftones using adaptive class-matrix and error diffusion," *ECTI-CIT Transactions*, vol. 13, no. 1, pp. 1–8, Jun. 2019.

[28] L. Y. Hsu, H. T. Hu and H. H. Chou, "A high-capacity QRD-based blind color image watermarking algorithm incorporated with A.I. technologies," *Expert Systems with Applications*, vol. 199, 117134, 2022.

[29] C. Song, S. Sudirman and M. Merabti, "A robust region-adaptive dual image watermarking technique," *Journal of Visual Communication and Image Representation* vol. 23, no. 3, pp. 549–568, 2012.

[30] V. S. Verma, R. K.Jha and A. Ojha, "Significant region-based robust watermarking scheme in lifting wavelet transform domain," *Expert Systems with Application*, vol. 42, no. 21, pp. 8184–8197, 2015.

[31] M. Talbi and M. S. Bouhlel, "Secure Image Watermarking Based on LWT and SVD," *International Journal of Image and Graphics*, vol. 18, no. 4, 1850021, 25 pages, 2018.

[32] C. -C. Lai and C. -C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060-3063, Nov. 2010.

[33] V. S. Verma and R.K. Jha, "Improved watermarking technique based on significant difference of lifting wavelet coefficients," *Signal, Image and Video Processing*, vol. 9, pp. 1443–1450, 2015.

[34] `http://www.imageprocessingplace.com/root_files_V3/image_databases.htm` (accessed Dec, 2021).

[35] M. Islam and R.H.Laskar, "Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark ex-

traction using SVM," *Multimedia Tools Application* vol. 77, pp. 14407–14434, 2018.

Sushma Jaiswal is an Assistant Professor in the Department of CSIT of Guru Ghasidas Central University, Bilaspur (C.G.). She has completed her Ph.D. in the field of image processing, and her fields of interest are computer graphics, machine vision, and image processing. She has teaching experience of 16 years, and she has published many papers in various national and international journals.

Manoj Kumar Pandey is a Ph.D. research scholar at Guru Ghasidas Central University, Bilaspur (C.G.), India. He has done M. Tech. (CSE) and MCA from CSVTU, Bhilai. He is also NET, and His field of interest is machine vision, digital image security, network security, and cryptography. He has research experience of 5 years and teaching experience of 9 years and published various papers in information security.