A Color Image Watermarking Scheme Based On QR Factorization, Logistic and Lorentz Chaotic Maps

[1]S AROGYA MANOGNA, [2]K.CHAITANYA

[1]Master's degree, Digital Image Processing, [2]Assistant Professor
Department of CSE
Acharya Nagarjuna University, Guntur, Andhra Pradesh

***ABSTRACT*: In this work, a new image watermarking algorithm on color images is proposed. The proposed algorithm divides a cover image into three color bands of red, green and blue. Then the following tasks are done on all three channels separately. First, each color band is divided into patches of small sizes then the entropy of each patch is calculated. At this step a threshold is found based on the average entropy of all patches and following is applied to all patches which have entropy lower than the threshold. A wavelet representation of each patch are given by applying a discrete wavelet transform.(DWT), Then Singular value decomposition (SVD) orthogonal-triangular decomposition and a chirp z-transform (CZT) are used to embed a watermark on the cover image. Several signal processing attacks are applied on watermarked images in order to robustness of the algorithm. The Proposed algorithm is compared with one conventional and two state-of the-art algorithms. Experimental results show superiority of the proposed algorithm compare with other algorithm in the area of image watermarking.**

***Keywords*: digital Image Watermarking, DWT, CZT, Entropy, SVD, QR.**

1. INTRODUCTION

With the widespread use of image processing tools, it becomes increasingly easy for ordinary people to obtain images and modify their contents. Copyright authentication for digital images has therefore become a challenging problem. To address this issue, digital watermarking theory has been proposed in recent decades. Generally speaking, digital watermarking schemes can fall into two broad categories according to different application scenarios: robust watermarking and fragile watermarking.

Robust watermarking techniques can resist most common attacks and consequently are widely used in copyright protection. By contrast, fragile watermarking methods are usually susceptible to any modification and thus are often employed in image tamper detection and restoration. For copyright protection, a robust watermarking scheme should satisfy two basic conditions, namely, robustness and imperceptibility. Here, robustness means that the watermark in a watermarked image can be integrally extracted even when the watermarked image has been distorted by attacks. Imperceptibility means that the quality of the watermarked image cannot be strongly influenced. In other words, no traces of watermark embedding are visible to the naked eyes. According to the working domain, the watermarking techniques can be further split into two categories

One is the watermarking methods performed in the spatial domain, in which the watermarking bits are inserted into carrier image by modifying its pixel values. The second kind of watermarking methods are based on the transform domain. Compared with the former, the watermarking schemes in the transform domain are more robust because the watermark is embedded by modulating the transform coefficients. Because of this property, many robust watermarking methods performed in the transform domain have been proposed for copyright protection. The most widely used transforms are the (DCT) [4], the DWT [5], and the (DFT) [6].

In recent years, (SVD) has received considerable attention in watermarking theory due to its good stability in signal processing. In [7], Liu and Tan introduced a classical SVD-based robust watermarking method. In their method, the watermark is inserted into the carrier image by directly modulating the singular values of the image. However, this method is not secure enough, and the watermark has much influence on the image quality. To resolve this issue, many robust watermarking methods based on hybrid transforms have been proposed, which combine SVD with other transforms, such as DWT and DCT. Lai and Tsai [8] introduced a DWT-SVD-based watermarking algorithm, in which the watermark is inserted by modifying the singular values of high-frequency sub-bands. In [9], another DWT-SVD-based robust watermarking method was proposed by Gupta and Raval. In this scheme, the original image is first decomposed by DWT, and the principal component of the watermark is then superimposed on the singular values of the diagonal high-frequency sub-band (HH). However, experimental results indicate that the extracted watermark has poor image quality when the watermarked image has been attacked. In [10], Singh et al. proposed a hybrid dual watermarking scheme for telemedicine applications.

Two watermarks (image and text) are embedded into a radiological image using a DWT-SVD-based watermarking method. During the embedding and extraction processes of the text watermark, four error correction codes (ECCs) are applied to improve the robustness of the watermark. Based on [10], Singh [11] designed an improved hybrid watermarking method. Unlike reference [10], the carrier image and the watermark image are both decomposed using the DWT, DCT, and SVD. Then, the singular value matrix of the watermark information is embedded into the carrier image using an SVD-based method. However, the quality of the watermarked images is greatly affected in these two methods because two watermarks are embedded in each image.

In [12], Singh et al. designed another hybrid watermarking method performed in DWT-DCT-SVD domain. The carrier image is firstly decomposed by DWT transform, then the low frequency sub-band (LL) and the watermark image are both transformed by DCT transform. The singular values of the DCT coefficients in watermark image are embedded into the singular values of the DCT coefficients in LL sub-band. To select an appropriate wavelet basis for DWT-DCT-SVD-based robust watermarking, Singh and Tayal [13] studied different wavelet families in DWT transform and analyzed their effects on the performance of hybrid watermarking. The comparison experiments indicate that different wavelets have different impacts on the watermarking scheme, and "the best wavelet" choice is dependent on several factors. To protect the copyright of color images, Roy and Pal [14] proposed a hybrid robust watermarking scheme that combines SVD with the redundant discrete wavelet transform (RDWT).

In [15], Laur et al. proposed a robust color image watermarking based on entropy and QR decomposition. The entropy is used to select the image blocks for watermark embedding. After chirp Z-transform, DWT transform, QR decomposition, and SVD transform, the watermark information is finally embedded into the singular values of carrier image. It is generally known that the scaling factor has a significant effect on SVD-based watermarking algorithms. To select an optimal scaling factor for SVD-based watermarking, Mishra et al. [16] analyzed the effect of different scaling factors on watermark imperceptibility and robustness. Based on the analysis, they proposed an optimized SVD-based watermarking method, in which an optimal scaling factor is identified using an optimization algorithm called the firefly algorithm (FA) [17].

Although this scheme achieves a good balance between robustness and imperceptibility, it can also lead to false-positive problem during the watermark extraction process [18]. To solve this problem, Makbol and Khoo [19] presented a false-positive-free watermarking scheme that combines SVD with the integer wavelet transform (IWT). To prevent false-positive problem, a signature generated from two orthogonal matrices U and V is inserted into the carrier image along with the watermark. During watermark detection, this signature is firstly extracted, and a certification process is then performed before watermark extraction. To further improve watermark robustness and imperceptibility, Ansari et al. [20] presented an improved robust watermarking algorithm based on [19], in which an optimal scaling factor is selected through artificial bee colony (ABC) optimization.

Compared with the previous method, this method achieves promising performance. A blind and robust watermarking method executed in the DWT, SVD, and DCT domains has been proposed in [21]. On the receiving end, the two identical watermarks are extracted from LH and HL sub-bands respectively, and a watermark correction process is applied to further improve the quality of the extracted watermark. The remainder of this article is organized as follows. In Section 2, APDCBT and SVD transforms are briefly described. The proposed method, including watermark insertion and watermark extraction, is developed in Section 3. Section 4 presents the experimental results and performance analysis. The conclusions and an outlook on possible future work are presented in Section 5.

2. PERELIMINARY

2.1 APDCBT

It is widely shared that the DCT has good properties of energy concentration. For this reason, it has been broadly applied in image compression and watermarking techniques. However, as research continues, some negative effects have been revealed that the image compressed by DCT has serious block artifacts at low bit rates. To solve this problem, a new transform called APDCBT was presented in Compared with the conventional DCT transform, the APDCBT transform shows outstanding performance in high-frequency attenuation and low-frequency aggregation. Thanks to these features, the APDCBT gets extensive usage in image processing and watermarking techniques .In, the APDCBT was first introduced into the field of information hiding, in which the APDCBT was just adopted to replace the DCT in conventional DCT-based robust watermarking method. To make better use of APDCBT, in this article, we introduce a hybrid watermarking method by combining APDCBT with DWT and SVD. In APDCBT transform, a transformation matrix B with dimensions of N × N is defined as

$$B(m,n)=\begin{cases}\frac{N-m}{N^2}, & m=0,1,2,\dots,N-1,n=0\\ \frac{1}{N^2}\left[(N-m)\cos\frac{mn\pi}{N}-csc\frac{n\pi}{N}\sin\frac{mn\pi}{N}\right], & m=0,1,2,\dots,N-1,n=1,2,\dots,N-1\end{cases} \quad (1)$$

For an image block X with dimensions of N×N, the APDCBT can be expressed as follows

$$Y=BXB^T \quad (2)$$

Where Y denotes the transform coefficient matrix after APDCBT.

2.2 SVD

SVD is a common transform that is often used in numerical analysis and principal component analysis (PCA). Through SVD, a matrix M can be decomposed into three parts denoted by U, S, a 9nd V:

$$M=USV^T \quad (3)$$

Where U and V are two orthogonal matrices and S is a diagonal matrix. The elements in matrix S, which are also called singular values, have good stability in signal processing and can resist common attacks to a certain extent. In addition, SVD can be performed on any matrices with no limitation. The top few singular values contain the majority of the image information. Because of these properties, SVD has been widely used in watermarking schemes for copyright authentication.

2.3 DWT

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2scale wavelet transform shown in below Figure1.

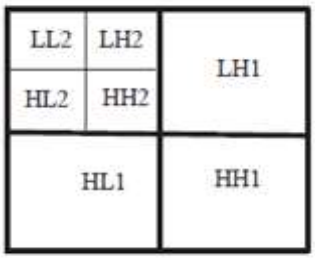

Fig 1.Frequency decomposition in DWT.

3. THE PROPOSED SCHEME

We present the proposed method based on DWT, APDCBT, and SVD in this section. It involves two stages: watermark insertion and watermark extraction. To concrete steps are introduced in the following subsections.

3.1 WATERMARK INSERTION

Figure 2 depicts the process of watermark insertion, and the detailed steps are presented below:

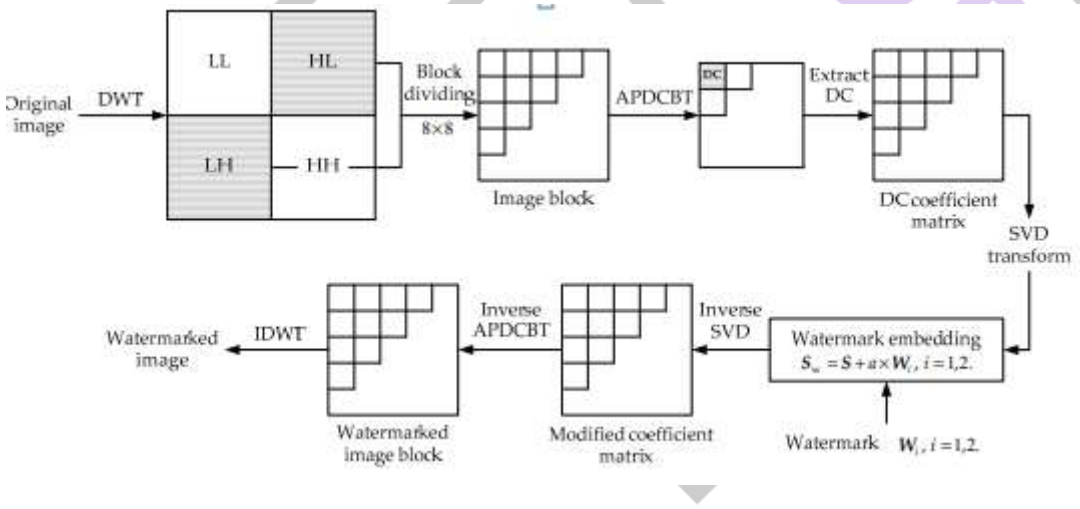

Fig 2 Watermark insertion

Step 1: One-level DWT decomposition with "HAAR" wavelet is first performed on the carrier image, yielding four sub-bands: three high-frequency sub-bands (LH, HL, and HH) and a low-frequency sub-band (LL).

Step 2: To reduce the influence of watermark insertion, two high-frequency sub-bands, LH and HL, are for the insertion of two identical watermarks. Using the HL, sub-band as an example, the blocks-based APDCBT is applied to each sub-block obtained by dividing the image into 8×8 blocks.

Step 3: The DC coefficient of each sub-block is used to generate a new coefficient matrix denoted by M. Then, SVD is applied to this coefficient matrix, and the singular value matrix S value M is computed.

Step 4: The first watermark W_1 is inserted into the coefficient matrix, which is shown as follows

$S_W = S + a \times w_1$ and $S_W = U_{sw1} V \frac{T}{W_1}$ (4)

where a is the watermark embedding intensity, S_W is a matrix containing the watermark information, Uw and Vw are newly generated orthogonal matrices, and Sw1 is the modified singular value matrix after watermark insertion.

Step 5: The inverse SVD is applied to Sw1, and then we get a modified coefficient matrix M0. After the inverse APDCBT, the HL sub-band embedded by watermark W1 is obtained.

Step 6: To embed the second watermark W2, the same process is performed on the LH sub-band.

Step 7: The inverse DWT (IDWT) is applied to obtain the watermarked carrier image.

3.2 WATERMARK EXTRACTION

The flow diagram of watermark extraction is shown in Figure 2. The extraction process consists of the following steps:

Step 1: The received image, which might have been distorted by various attacks, is transformed by one-level DWT with "HAAR" wavelet. Then, the high-frequency sub-bands, LHW and HLW, are obtained.

Step 2: To extract the watermark W∗ 1 in HLW sub-band, the sub-band image is first divided into 8 × 8 non-overlapping sub-blocks. Then, the APDCBT is performed on each sub-block. Subsequently, the DC coefficients in the APDCBT coefficient matrices are used to produce a new matrix M∗.

Step 3: The newly generated matrix M∗ is transformed by SVD to obtain three new matrices, U∗, S∗, and V∗, as given in Equation (5):

$$M^*=U^*S^*(V^*)^T \quad (5)$$

Step 4: The watermark W∗ 1 is computed by applying the inverse process of Step 4 in watermark embedding procedure, which can be expressed as follows:

$$S_w^*=U_w S^* V_w^T W_1^*= (S_w^*-S)/a. \quad (6)$$

To obtain another watermark, W∗ 2, the same process is applied to the LHw sub-band. Finally, the watermark W is computed by averaging these two watermarks, i.e., W = (W∗ 1 + W∗ 2) /2. To further improve the quality of the extracted watermark, a sign function used in is employed to correct the watermark:

$$W^*(i,j)=\{1,W(i,j)\geq T \quad (7)$$

Where T is a threshold between 0 and 1, W∗ is the extracted watermark after correction, and (i, j) represents the coordinates of a pixel in watermark image. In the experiments reported below, T is set to 0.5.

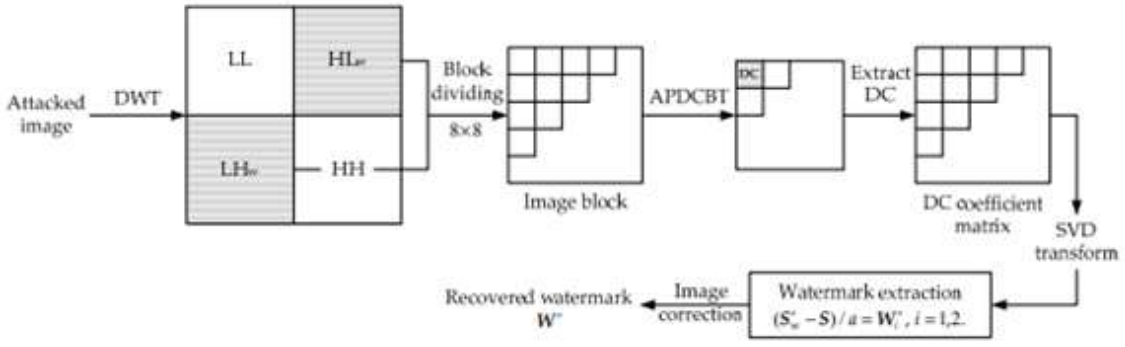

Fig3. Watermark extraction

To better understand the proposed watermarking scheme, the pseudo code forms of the watermark insertion and extraction processes are presented in Algorithms1 and 2, respectively:

4. PERFORMANCE ANALYSIS

In this section, several experiments are conducted to evaluate the imperceptibility and robustness of the proposed watermarking method. Since the proposed method is implemented in the frequency domain, the watermark information is distributed on the whole image. In this paper, we use the standard test images with size of 512 × 512 as the example to show the algorithm performance. The gray-scale image Lena with dimensions of 512 × 512 is adopted as the carrier image. A binary logo image (SDUW, the abbreviation

for Shandong University at Weihai) with dimensions of 32 × 32 is used as the watermark. In watermarking schemes based on SVD, the watermarking intensity plays an important role for the performance of the algorithm. To make better experimental comparisons, the embedding intensity used in these experiments is the same as that used in reference, which is equal to 0.05.

4.1 IMPERCEPTIBILITY

The peak signal-to-noise ratio (PSNR) is a common image quality evaluation index used in the field of image processing. For an image with dimensions of 512 × 512, the PSNR is defined as:

$$\text{PSNR} = 10\lg\left[\frac{512\times512\times max[I(i,j)]2}{\sum_{i=1}^{512}\sum_{j=1}^{512}[I(i,j)-Iw(i,j)]2}\right] \quad (8)$$

Generally, a higher PSNR implies that the watermark in the watermarked image has better imperceptibility. To evaluate the quality of an extracted watermark, the similarity between the original watermark W1 and the extracted watermark $W*$ is calculated as the normalized correlation coefficient (NCC). For the experiments reported in this paper, the NCC can be represented as follows:

$$\text{NCC} = \frac{\sum_{i=1}^{32}\sum_{j=1}^{32}W1(i,j)\times W*(\text{i,j})}{\sum_{i=1}^{32}\sum_{j=1}^{32}W1(i,j)\times W1(\text{i,j})} \quad (9)$$

Figure 3 shows the carrier images and watermarks without performing any attack. It can be observed that there is no subjective visual difference between the original image and its watermarked counterpart. To compare with other watermarking algorithms, Table 1 lists the watermark capacity, PSNR, and NCC of two robust watermarking methods (.By using this equation (9). It should be noted that for comparison, the watermark in [7] is embedded into the top left corner of carrier image. From Table 1, it can be observed that the proposed scheme and the method in reference [22] have higher PSNR values than the method proposed by Liu and Tan [7]. The NCC value of the proposed scheme is slightly lower than reference [7], but it is higher than the recently proposed method in reference [22].

(a) (b) (c)

Fig4. The carrier images and watermarks without performing any attack: (a) original Lena image; (b) binary water mark; (c) water marked Lena image; (d) extracted watermark

Table1. Comparisons among different robust watermarking methods in terms of watermark capacity, peak signal-to-noise ratio (PSNR) and normalized correlation coefficient (NCC).

Items	Liu and Tan [7]	Fazli and Moeini [22]	Proposed
Watermark image	gray	binary	binary
Capacity	32 × 32	32 × 32 × 4	32 × 32 × 2
PSNR (dB)	53.83	101.97	101.97
NCC	1	0.9603	0.9724

4.2 ROBUSTNESS

To test the robustness of the proposed algorithm, various common signal processing attacks are applied to the watermarked images, such as salt and pepper noise, Gaussian noise, and JPEG compression. Figure 4 shows the attacked images and their corresponding watermarks extracted from them. The results demonstrate that the extracted watermarks obtained using the presented method show good robustness to various attacks. To objectively evaluate the robustness of the proposed method, Table 2 lists the NCC values of the extracted watermarks under different attacks. In addition, we compare the proposed method with a conventional SVD-based watermarking method [7] and a hybrid watermarking method presented in [22]. Considering the randomness of the noise, the NCC values of the extracted watermarks after noise attacks are the average values from multiple experiments. From Table 2, we can see that the NCC values obtained using the proposed method are approximately equal to or even greater than those achieved by other

methods under the same attacks. Furthermore, the NCC results are extremely stable under different attack intensities. These results suggest that the proposed method is highly robust compared with the scheme proposed in reference [22].

Fig 5 CONT

Fig 6 Attacked images and the corresponding watermarks extracted from them. (a) salt and pepper noise (0.005); (b) Gaussian noise (0,001); (c) modern filtering(5×5); (d) average filtering(3×3); (e) rotation(15); (f) JPEG compressions with quality factor (QF) equal to 20; (g) cropping(25%); (h) scaling (2,05); (i) contrast enhancement (1,5); (j) brightness adjustment (+50).

Table2. NCC values of the extracted watermarks under different attacks

Attack	Liu and Tan [7]	Fazli and Moeini [22]	Proposed
Embedding intensity	0.05	0.05	0.05
Salt and pepper noise (0.005)	09628	0.9993	0.9988
Salt and pepper noise (0.01)	0.9158	1	0.9985
Gaussian noise (0, 0.005)	0.8606	1	0.9986
Gaussian noise (0, 0.01)	0.8235	1	0.9993
Scaling (2, 0.5)	0.9838	0.9621	0.9638
Scaling (0.5, 2)	0.9123	0.9603	0.9672
Median filtering (3 × 3)	0.9321	0.9638	0.9793
Median filtering (5 × 5)	0.8510	0.9621	0.9724
Average filtering (3 × 3)	0.8987	0.9793	0.9741
Average filtering (5 × 5)	0.8153	0.9586	0.9690
Rotation (5°)	0.8223	1	0.9897
Rotation (15°)	–	0.9948	1
Contrast enhancement (1.2)	0.9889	1	1
Contrast enhancement (1.5)	0.9844	1	1
Brightness adjustment (+50)	1	0.9672	0.9741
Brightness adjustment (+100)	0.7598	0.9603	0.9707

4.3 JPEG COMPRESSION

JPEG compression is widely adopted in image transmission and storage. To test the properties of the proposed algorithm under JPEG compression, the watermarked images are compressed by JPEG compression with different QFs. Figure 5 presents the curves of the NCC values under JPEG compression with different QFs. The experimental results show that the proposed scheme has higher NCC values than the other two methods. Besides, it can also be noticed from the figure that the NCC values obtained by the proposed scheme and reference [22] are more stable than those of Liu and Tan's method [7]. The reason is that the reference [7] is a pure SVD-based watermarking scheme, while the proposed scheme and reference [22] are based on hybrid transforms. Compared to the former, the hybrid transform based watermarking schemes have better robustness for JPEG compression with different QFs. When the watermarked images in [7] are highly compressed by JPEG compression (with low QFs), the watermark information will be destroyed more easily than the other two methods. In conclusion, the data in Fig 5 prove that our proposed algorithm exhibits better robustness against JPEG compression than the other methods.

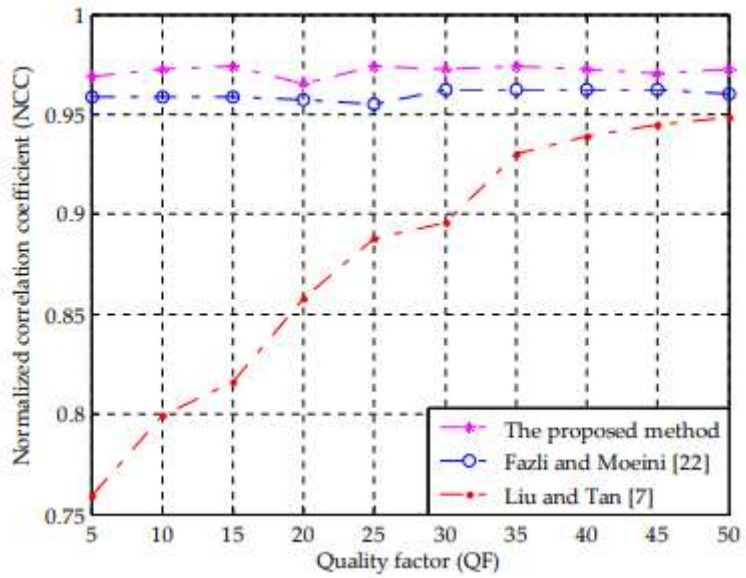

Fig7. NCC values under JPEG compression with different QFs

However, in practical applications, images are always vulnerable to more than one kind of attack. Moreover, digital images need to be preprocessed to reduce the bandwidth and memory required for the transmission and storage. To test the robustness of the proposed method under hybrid attacks, Figure 6 shows watermarked images subjected to hybrid signal processing attacks and their corresponding extracted watermarks. Table 3 gives the NCC values of the watermarks extracted under different conditions. It is observed that our proposed scheme achieves promising results compared with those of Fazli and Moeini's method [22]. The watermarks could be extracted without much degradation. Based on the above comparisons and analysis, we conclude that the proposed watermarking algorithm shows superior robustness in resisting various signal processing attacks.

)

Fig 8.Images subjected to hybrid attacks and their corresponding watermarks: (a) Gaussian noise [0,0.01] + median filtering(3×3); (b) Gaussian noise(0,0.01)+average filtering(3×3); (c) Salt and pepper noise (0,01)+ median filtering(3×3); (d) salt and pepper noise(0,01) +average filtering(3×3); (e) scaling (2,0.5) +JPEG compression (QF=50); (f) scaling(0,5.2)+JPEG compressions(QF=50);(g) JPEG compression(QF=50)+ cropping(25); (h) median filtering(3×3)+JPEG compression(QF=50);(i) average filtering (3×3)+JPEG compression(QF=50);(j) salt and pepper noise(0,01)+Gaussian noise(0,0.01).

Table3. NCC values of the watermarks extracted after hybrid attacks

Attack	Liu and Tan [7]	Fazli and Moeini [22]	Proposed
Gaussian noise (0, 0.01) + median filtering (3 × 3)	0.9401	0.9995	0.9971
Gaussian noise (0, 0.01) + average filtering (3 × 3)	0.9716	1	0.9964
Salt and pepper noise (0.01) + median filtering (3 × 3)	0.9332	0.9631	0.9793
Salt and pepper noise (0.01) + average filtering (3 × 3)	0.9647	0.9993	0.9867
Scaling (2, 0.5) + JPEG compression (QF = 50)	0.9462	0.9621	0.9707
Scaling (0.5, 2) + JPEG compression (QF = 50)	0.8942	0.9621	0.9724
JPEG compression (QF=50) + cropping (25%)	0.9485	0.8086	0.8569
Median filtering (3 × 3) + JPEG compression (QF = 50)	0.9455	0.9569	0.9707
Average filtering (3 × 3) + JPEG compression (QF = 50)	0.8885	0.9707	0.9759

5. CONCLUSION:

In this work, a novel watermarking algorithm is proposed for colored images. The algorithm embeds a watermark into singular values of all three color channel of cover image. At the First step, the cover image is branched into three color channels of R, G, and B, and then each channel is divided into patches. Then a proper patch which has low entropy is found in order to watermark embedding. Then these patches are decomposed into frequency channels by using DWT and further decomposed using CZT. Then orthogonal-triangular decomposition and Singular value decomposition are used to embed a watermark on the cover image.

References:

[1] V. Solachidis, E. Maiorana, P. Campisi, and F. Banterle, "HDR image watermarking based on bracketing decomposition," in Digital Signal Processing (DSP), 2013 18th International Conference on, pp. 1–6, IEEE, 2013.

[2] F. Guerrini, M. Okuda, N. Adami, and R. Leonardi, "High dynamic range image watermarking robust against tone-mapping operators," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 2, pp. 283–295, 2011.

[3] X. Xue, M. Okuda, and S. Goto, "μ-law based watermarking for HDR image robust to tone mapping," 2011.

[4] H. Park, S. H. Lee, and Y. S. Moon, "Adaptive video watermarking utilizing video characteristics in 3d-dct domain," in Digital Watermarking, pp. 397–406, Springer, 2006.

[5] K. Zebbiche and F. Khelifi, "Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking," IET Image Processing, vol. 8, no. 1, pp. 23–32, 2014.

[6] L. Laur, M. Daneshmand, M. Agoyi, and G. Anbarjafari, "Robust grayscale watermarking technique based on face detection," in Signal Processing and Communications Applications Conference (SIU), 2015 23th, pp. 471–475, IEEE, 2015.

[7] P. A. Hernandez-Avalos, C. Feregrino-Uribe, and R. Cumplido, "Watermarking using similarities based on fractal codification," Digital Signal Processing, vol. 22, no. 2, pp. 324–336, 2012.

[8] P. Rasti, S. Samiei, M. Agoyi, S. Escalera, and G. Anbarjafari, "Robust non-blind color video watermarking using qr decomposition and entropy analysis," Journal of Visual Communication and Image Representation, vol. 38, pp. 838–847, 2016.

[9] E. Elbas¸i, "Robust multimedia watermarking: Hidden markov model approach for video sequences," Turkish Journal of Electrical Engineering & Computer Sciences, vol. 18, no. 2, pp. 159–170, 2010.

[10] M. Agoyi, E. C¸ elebi, and G. Anbarjafari, "A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition," Signal, Image and Video Processing, vol. 9, no. 3, pp. 735–745, 2015.