SEBHA UNIVERSITY JOURNAL OF PURE & APPLIED SCIENCES VOL.21 NO. 2 2022
DOI: 10.51984/JOPAS.V21I2.1934

جامعة سبها للعلوم البحتة والتطبيقية مجلة
Sebha University Journal of Pure & Applied Sciences

Journal homepage: www.sebhau.edu.ly/journal/index.php/jopas

A robust blind watermarking scheme based on lifting wavelet transform and hessenberg decomposition

Omar Abodena

University of Gharyan, Nahda street, Gharyan, Libya

Keywords:
Lifting wavelet transform
Entropy analysis
Discrete cosine transform
Hessenberg decomposition
Digital watermarking

ABSTRACT

In this paper, a novel robust blind grayscale image digital watermarking scheme is introduced based on lifting wavelet transform (LWT) in combination with discrete cosine transform (DCT), Hessenberg decomposition, and entropy analysis for copyright protection of multimedia information. At first, the two levels of LWT are applied to the host grayscale image to improve the imperceptibility of the watermarking scheme and then the high-frequency sub-band of the 2-level of LWT is decomposed by DCT. Next, the DCT coefficients are divided into 4×4 non-overlapping blocks. After that, Hessenberg decomposition performs on each selected block, whereas the first row, first column element of the upper Hessenberg matrix is utilized to hide the watermark. To evaluate the imperceptibility and robustness of the proposed digital watermarking scheme, the peak signal-to-noise ratio (PSNR), and normalized cross-correlation (NC) are utilized to measure the quality and the ability of the proposed watermarking scheme to robust against signal processing operations and geometric attacks. Experimental and analysis results have demonstrated that the proposed scheme is achieved a very good tradeoff between imperceptibility and robustness. The comparison with other scheme have shown that the proposed digital watermarking schemes have a superior performance in terms of imperceptibility and robustness than other.

طريقة قوية للعلامة المائية العمياء معتمداً على رفع تحويل المويجات وتحليل هيسنبرغ

عمر أبودينة

جامعة غريان، شارع النهضة، غريان، ليبيا

الكلمات المفتاحية:
تحليل الانتروبيا
تحليل هيسنبرغ
تحويل جيب التمام المنفصل
رفع تحويل المويجات
علامة مائية رقمية

الملخص

في هذه الورقة ، تم تقديم طريقة علامة مائية رقمية جديدة لصورة رمادية عمياء على أساس رفع تحويل المويجات مع تحويل جيب التمام المنفصل ، وتحليل هيسنبرغ وتحليل الانتروبيا، لحماية حقوق التأليف والنشر لمعلومات الوسائط المتعددة. في البداية ، يتم تطبيق المستويين رفع تحويل المويجات على صورة مضيفة بتدرج الرمادي لتحسين عدم إدراك طريقة العلامات المائية ثم يتم تحليل النطاق الفرعي عالي التردد للمستوى 2 من رفع تحويل المويجات بواسطة تحويل جيب التمام المنفصل. ثم ، يتم تقسيم معاملات تحويل جيب التمام المنفصل إلى 4 × 4 كتل غير متداخلة. بعد ذلك ، يتم تنفيذ تحليل هيسنبرغ لكل كتلة محددة ، بينما يتم استخدام الصف الأول ، عنصر العمود الأول من مصفوفة هيسنبرغ العليا لإخفاء العلامة المائية. من أجل تقييم عدم إدراك وقوة طريقة العلامة المائية الرقمية المقترحة ، يتم استخدام إشارة الذروة إلى نسبة الضوضاء والارتباط المتبادل الطبيعي لقياس جودة وقدرة طريقة العلامة المائية المقترح على مقاومة عمليات معالجة الإشارات والهجمات الهندسية. أظهرت النتائج التجريبية والتحليلية أن المخطط المقترح قد حقق توازن جيد جدًا بين عدم الإدراك والقوة. أظهرت المقارنات مع المخططات الأخرى أن مخططات العلامات المائية الرقمية المقترحة لها أداء متفوق من حيث عدم الإدراك والقوة من غيرها.

1.Introduction

In recent years, authentication and copyright protection of multimedia information have become a very hot challenging issue, mainly as a result of the swift advancement in communication technology, telemedicine imaging applications, electronic commerce, internet technology, and a lot of interest in web applications. there is an overwhelming amount of digital multimedia

*Corresponding author:
E-mail addresses: omar.abodena@gu.edu.ly

Article History : Received 14 June 2022 - Received in revised form 29 September 2022 - Accepted 11 September 2022

information on the web. Thus a great number of data can be today easily accessible on the internet for everyone and tampered or modified by utilizing one of the obtainable image processing tools [1]. In the last two decades, an amount of research has been presented on different aspects of digital multimedia data protection such as steganography, encryption, and digital watermarking [2]. In particular, watermarking techniques have been considered an irreplaceable part of digital multimedia data protection and have become a necessary method employed in numerous applications such as authentication or copyright protection-based applications [3]. In addition, a digital watermarking technique can be utilized on various types of digital multimedia information such as video, image, and audio.

The efficient digital watermarking schemes should be fulfilled the following main requirements [4, 5]: (i) Invisibility: the multimedia information quality should not be degraded by inserting the embedded watermark. (ii) Robustness: the ability to extract the watermark from watermarked information after different malicious distortions, including geometrical attacks and signal processing operations. (iii) Security: the watermark information should not be modified, detected, or removed, which generally depends on security keys. (iv) Capacity: the maximum amount of bits that can be hidden into original information without degrading its quality. In addition, the optimal trade-off between invisibility and robustness should be provided.

Digital watermarking embedding techniques can be distinguished into the following groups [6]: a spatial-domain technique and a transform-domain technique. In a spatial-domain technique, the pixels of multimedia information are modified with watermark information. Whilst in a transform-domain technique, the original multimedia information is converted into its magnitude coefficients where the watermark is hidden. Here, several types of transforms like discrete wavelet transform (DWT) [7], discrete cosine transform (DCT) [8], discrete Fourier transform (DFT) [9], discrete-time Fourier transform (DTFT) [10], and matrix decompositions like QR decomposition [11], singular value decomposition (SVD) [12], Hessenberg decomposition [13] and etc. are utilized. Digital watermarking schemes that use transform-domain techniques provide the best invisibility, stability, and robustness than the spatial-domain techniques [2]. Digital watermarking extraction techniques also can be divided into three main groups [14]: (i) Blind: for extracting the watermark, a secure key is only required in this technique. (ii) Semi-blind: this technique is also needed the original multimedia information for extraction the watermark. (iii) Non-blind: host multimedia information and original watermark information are needed for extraction of the watermark.

in this paper, a novel robust blind digital grayscale image watermarking scheme for copyright protection based on lifting wavelet transform (LWT), discrete cosine transform, Hessenberg decomposition, and entropy analysis is presented. Here, the coefficients of a high-frequency subband after carrying out a two-level lifting wavelet transform of the original host image are transformed by discrete cosine transform. Afterward, the coefficients of discrete cosine transform are divided into non-overlapping blocks where Hessenberg decomposition is applied to each non-overlapping block randomly. In this proposed digital watermarking scheme, a new combination of LWT, DCT, and Hessenberg decomposition for digital watermarking is designed to obtain the advantages of hybridization of these transformations for enhancement of invisibility and robustness against attacks, such as LWT provides excellent frequency localization properties [15], DCT provides energy compaction properties [16], and Hessenberg decomposition as a matrix decomposition provides different elements that can be used to embed the watermark information into the biggest energy element of the Hessenberg matrix [17]. For obtaining the optimal trade-off between invisibility and robustness, the entropy analysis is used to obtain the best scaling factor value based on the average entropy of all non-overlapping blocks. To enhance the security of the proposed digital watermarking scheme, a pseudo-random sequence generated by a random permutation function is used to select blocks randomly to embed the watermark bits.

This paper is arranged as follows. The explanations of different terminologies such as LWT, DCT, Hessenberg decomposition, and entropy analysis are given in Section 2. Section 3 discusses the proposed digital watermarking scheme. The experimental results and compared methods are discussed in Section 4 and the conclusion is given in Section 5.

Preliminaries

1. Lifting wavelet transform

The lifting wavelet transform proposed by Sweldens [18], has been utilized in many applications such as pattern recognition, image compression, and image processing [19] as a powerful scheme. LWT is presented for reducing memory requirement and computation time as the lifting method allows a fully in-place implementation of wavelet transform[4]. As compared to traditional discrete wavelet transform, LWT requires a half number of calculations and permits us to perform reversible integer wavelet transform [20]. The lifting wavelet transform includes three steps as follows [20]:

1) Splitting: In this step, the primary signal s(k) is divided into odd and even non-overlapping samples: So(k) and Se(k).

$$So(k) = s(2k+1), Se(k) = s(2k) \quad (1)$$

2) Prediction: In this step, using even signal samples to predict odd signal samples and the two divided signals should be closely correlated. This step can be viewed as a high pass filter processing. The difference can be given as follows:

$$D(k) = So(k) - P(Se(k)) \quad (2)$$

where P[.] denotes the predict operator, while D(k) denotes a detail signal. The D(k) indicates the high-frequency component of the input signal s(k).

3) Updating: In this step, introducing the operator of updating U[.], and utilizing the detail signal D(k) for updating even samples Se(k). This step can be viewed as a low pass filter processing. The approximate signal C(k) can be given as follows:

$$C(k) = Se(k) + U(D(k)) \quad (3)$$

where the C(k) indicates the low frequency component of the input signal s(k).

2. Discrete cosine transform

Discrete cosine transform is commonly utilized in the transformation domain techniques. DCT provides a robust scheme at a high level due to introducing the signal transformation operation of the frequency domain [21]. The original signal is transformed into three sub-bands: low-frequency, middle-frequency, and high-frequency sub-bands. The energy compaction property is the main characteristic of discrete cosine transform, where the main parts of the input signal are comprised in low-frequency sub-bands and the high-frequency sub-bands are more robust to signal processing attacks [22].

3. Hessenberg decomposition

The Hessenberg decomposition is the decomposition of a special type of square matrix A and the Hessenberg decompositions have been utilized as good useful decomposition in specific control theory applications [23]. A matrix A is decomposed by the Hessenberg decomposition utilizing orthogonal similarity transformations for reduction of the real matrix A to the upper Hessenberg form into its factors H and Q, that its form can be presented as follows:

$$A = QHQ^T \quad (4)$$

where Q is an orthogonal matrix, whilst H is an upper Hessenberg matrix, whereas hij = 0 whenever i > j+1.

4. Entropy analysis

The entropy can be utilized for enumeration to how much data content is presented in the image. It depicts the number of randomness and uncertainty contained in the image. The more contained image information indicates better its quality. Also, entropy can be named Shannon's entropy and the entropy of information calculates the uncertainty of a data source. The entropy of Shannon can be defined as follows [24, 25]:

$$E(x) = -\sum p(x) \log p(x) \quad (5)$$

Proposed method

A novel blind digital grayscale image watermarking scheme is proposed to hide the watermark information into a grayscale image based on lifting wavelet transform in combination with Hessenberg decomposition, discrete cosine transform, and entropy analysis. There are two processes in the proposed method: the watermark embedding process and the watermark extraction process where figures 1 and 2 show the block diagrams of these processes.

1. Watermark embedding process

The involved steps of the watermark embedding process can be presented below:

Step 1: Applying two-level lifting wavelet transform to host image of size $N \times N$ to decompose it. For having cA_1, cH_1, cV_1, and cD_1 of the 1-level then having cA_2, cH_2, cV_2, and cD_2 of the cD_1 of the 2-level. Here, cA_1 and cA_2 are diagonal details of the first and second levels of lifting wavelet transform respectively. cH_1 and cH_2 are vertical details of the first and second levels of lifting wavelet transform respectively. cV_1 and cV_2 are horizontal details of the first and second levels of lifting wavelet transform respectively. cD_1 and cD_2 are lower resolution approximation components of the first and second levels of lifting wavelet transform respectively.

Step 2: Applying DCT to cD_2 high-frequency sub-band for having DCT coefficients.

Step 3: DCT coefficients are divided to obtain non-overlapping blocks of size 4 × 4. In which the blocks' number is 64^2.

Step 4: Computing the entropy of each block to obtain the average of blocks' entropy for utilizing it as quantization stage α.

Step 5: Generation of the pseudo-random sequences utilizing randperm-function based on the key_1 and key_2 for having two random numbers which indicate the column and row. Where the key_1 and key_2 are 12 and 8, respectively.

Step 6: Each selected 4 × 4 blocks based on the pseudo-random sequences is applied by the Hessenberg decomposition as mentioned in Eq. (4) to get the matrices H and Q.

Step 7: The magnitudes M_1 and M_2 are modified depending on the binary watermark data w, as below:

$$if\ w(i,j) = 1, \begin{cases} M_1 = 0.25\alpha \\ M_2 = -0.95\alpha \end{cases} \quad (6)$$

$$if\ w(i,j) = 0, \begin{cases} M_1 = -0.25\alpha \\ M_2 = 0.95\alpha \end{cases} \quad (7)$$

here (1≤i, j≤N), and α indicates the quantization stage. Where 0.25 and 0.95 are chosen to obtain good results in both robustness and imperceptibility.

Step 8: The potential quantization outcomes T_1 and T_2 are computed by the modified magnitudes M_1 and M_2.

$$T_1 = 2k\alpha + M_1 \quad (8)$$

$$T_2 = 2k\alpha + M_2 \quad (9)$$

here $k = floor(ceil(h_{1,1}/\alpha)/2)$, $ceil(.)$ and $floor(.)$ indicate as the largest nearest integer and the least nearest integer, respectively.

Step 9: The first-column, first-row component $h_{1,1}$ of upper Hessenberg decomposition matrix H is selected to hide the binary watermark as shown:

$$h'_{1,1} = \begin{cases} T_2\ if\ abs(h_{1,1} - T_2) < abs\ (h_{1,1} - T_1) \\ T_1\ else \end{cases} \quad (10)$$

here $abs(.)$ indicates the absolute value.

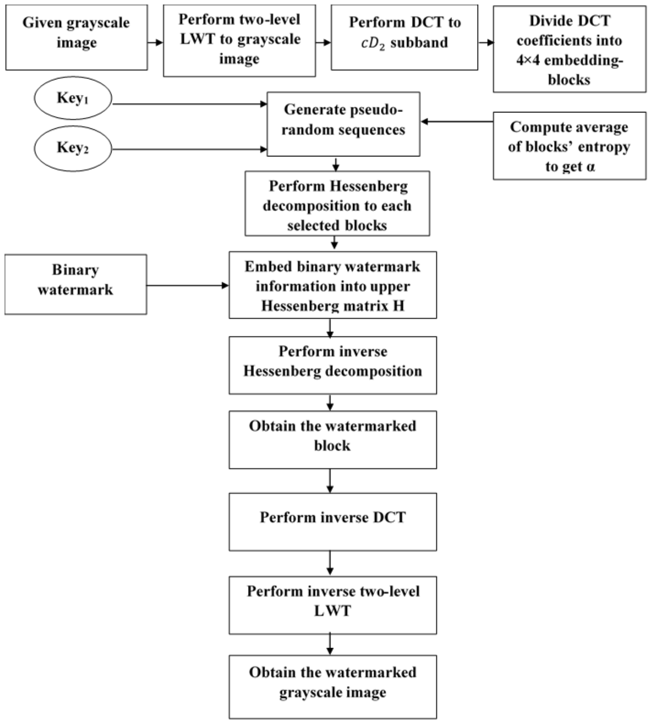

Fig. 1: The proposed grayscale watermarking embedding process

Step 10: The $h_{1,1}$ with $h'_{1,1}$ is replaced and after that perform the inverse Hessenberg decomposition for obtaining the A' watermarked block.

$$A' = QH'Q^T \quad (11)$$

Step 11: The embedding steps 6–10 are repeated for hiding all watermark data.

Step 12: All watermarked blocks are combined.

Step 13: The inverse of discrete cosine transform is applied to the combined watermarked blocks for obtaining the modified high-frequency sub-band cD^w, in which cD^w indicates the watermarked estimated high-frequency sub-band.

Step 14: The inverse of the two-level lifting wavelet transform is applied based on the changed high-frequency sub-band cD^w instead of cD_2 for obtaining the watermarked grayscale image.

2. Watermark extraction process

The involved steps of the watermark extraction process can be given below:

Step 1: Applying two-level lifting wavelet transform to the watermarked image of size $N \times N$ to decompose it. For having cA_1, cH_1, cV_1, and cD_1 of the 1-level then having cA_2, cH_2, cV_2, and cD_2 of the cD_1 of the 2-level.

Step 2: Applying DCT to cD_2 high-frequency sub-band for having DCT coefficients.

Step 3: DCT coefficients are divided to obtain non-overlapping blocks of size 4 × 4. In which the blocks' number is 64^2.

Step 4: Computing the entropy of each block to obtain the average of blocks' entropy for utilizing it as quantization stage α.

Step 5: Generation of the pseudo-random sequences utilizing randperm-function based on the key_1 and key_2 for having two random numbers which indicate the column and row.

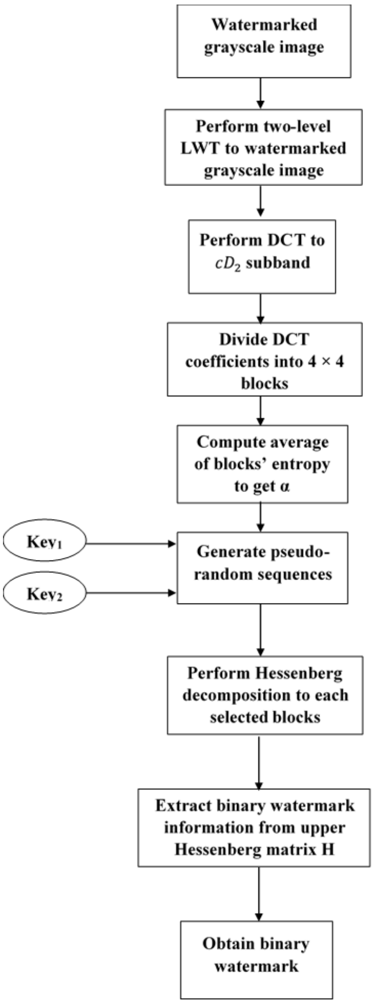

Fig. 2: The proposed grayscale watermarking extraction process

Step 6: Each selected 4 × 4 blocks based on the pseudo-random sequences is applied by the Hessenberg decomposition as mentioned in Eq. (4) to get the matrices $H^{`}$ and $Q^{`}$.

Step 7: The first column, first row component $h'_{1,1}$of matrix's upper Hessenberg H' is utilized for extraction of the binary watermark as shown:

$$w'_{i,j} = mod\ (\ ceil\left(\frac{h'_{1,1}}{\alpha}\right), 2) \qquad (12)$$

here (1≤*i*, *j*≤N) and $mod(.)$ indicates the modulo operation.

Step 8: The detecting steps 6–7 are repeated for detecting all watermark information and then obtaining the extracted binary watermark.

Experimental results and discussion

Several experimental results are performed to present the effectiveness of the proposed digital grayscale image watermarking scheme in terms of imperceptibility and ability to be robust against attacks. All experiment results were performed utilizing MATLAB R2017b on a laptop computer that its classifications are windows 10 environment, Intel Core i3 2.00 GHz CPU, and 4.00 GB RAM. The proposed grayscale image watermarking scheme is applied to common test grayscale images. Five test grayscale images from USC-SIPI database [26] are utilized in the proposed grayscale image watermarking scheme, these images are 1024 × 1024 as shown in fig. 3 as referred to "Lena", "Sailboat", "Peppers", "Baboon", and "Airplane, respectively. The watermarks utilized in this scheme of size 64×64 is shown in fig. 4.

The attacks used in the proposed scheme are explained as follows:

- Sharpening: The watermarked grayscale images are sharpened with 1 amount value.
- Gamma correction: The Gamma correction is applied to the watermarked grayscale images by 1 Gamma value, whereas Gamma value 1 is used for a linear mapping between intensity values in the watermarked image.
- Blurring: The watermarked grayscale images are blurred with 1 blurring value.
- Salt & pepper noise: The salt and pepper noise is added to the watermarked grayscale images with 0.001 noising value.
- Gaussian noise: The Gaussian noise is added to the watermarked grayscale images with a mean value 0 and 0.001 variance value.
- Median filter: The median filter is applied to the watermarked grayscale images with 3×3 window size.
- Scaling: The watermarked grayscale images are scaled to 7 times.
- Cropping: The watermarked grayscale images are cropped from the top to 75% value.
- JPEG 2000 compression: The JPEG 2000 compression is applied to the watermarked grayscale images with 5 compression ratio.

After that, a comparison of the results obtained from the proposed scheme with the results from transform domain-based grayscale image watermarking schemes.

To evaluate the imperceptibility and robustness of the proposed digital watermarking scheme, the peak signal to noise ratio (PSNR), and normalized cross-correlation (NC) are utilized to measure the quality of the proposed watermarking scheme and the ability of the proposed watermarking scheme to robust against signal processing operations and geometric attacks.

Peak signal to noise ratio is defined as an engineering phrase to compute the ratio between the highest potential power of a signal and the power of distorting noise which impacts the fidelity of the signal's representation [27]. Its formula can be given as follows:

$$PSNR = 10\ \log\frac{255^2}{MSE}dB \qquad (13)$$

here MSE indicates the mean square error between the cover signal and distorted signal which is given as follows:

$$MSE = \frac{1}{MN}\sum_{l=1}^{M}\sum_{k=1}^{N}(C(l,k) - C'(l,k))^2 \qquad (14)$$

here *C(l,k)* and *C`(l,k)* indicate the $(l,k)^{th}$ pixel value in the cover signal and watermarked signal, respectively.

Normalized cross-correlation is defined as a well-known metric utilized for measuring the similarity degree between two compared signals [28]. Its formula can be given as follows:

$$NC = \frac{\sum_{l=1}^{M}\sum_{k=1}^{N} W(l,k)\times W'(l,k)}{\sqrt{\sum_{l=1}^{M}\sum_{k=1}^{N} W^2(l,k)} \times \sqrt{\sum_{l=1}^{M}\sum_{k=1}^{N} W'^2(l,k)}} \qquad (15)$$

here *W* and *W`* indicate the original watermark signal and the extracted watermark signal after being attacked, respectively; *N* and *M* indicate the watermark signal size. Table 1 and 2 list the PSNR and NC values of the watermarked grayscale images with a watermark image under no attacks.

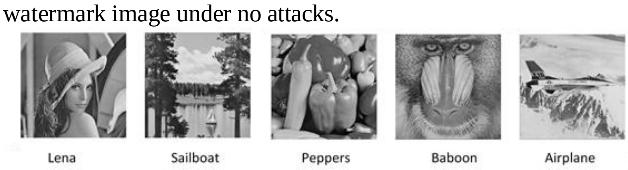

Fig. 3: The grayscale host images

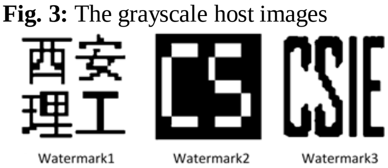

Fig. 4: The watermark images

In general, maximal PSNR values refer to that the proposed scheme offers superior performance in terms of imperceptibility, while maximal NC values refer to that the proposed scheme offers superior performance in terms of robustness. The PSNR values of the proposed grayscale image watermarking scheme are more than 37.481 dB whilst the NC values are 1.000.

Table 1: The PSNR values with no attacks

Cover image	Watermark1	Watermark2	Watermark3
Lena	44.880	44.882	44.880
Sailboat	41.854	41.850	41.857
Peppers	43.954	43.955	43.952
Baboon	37.483	37.481	37.485
Airplane	46.375	46.371	46.371

Table 2: The NC values with no attacks

Cover image	Watermark1	Watermark2	Watermark3
Lena	1.000	1.000	1.000
Sailboat	1.000	1.000	1.000
Peppers	1.000	1.000	1.000
Baboon	1.000	1.000	1.000
Airplane	1.000	1.000	1.000

Fig. 5: The watermarked images and extracted watermark 1 with no attack

Fig. 6: The watermarked images and extracted watermark 2 with no attack

Fig. 7: The watermarked images and extracted watermark 3 with no attack

For more explanations, figures 5 and 7 show the watermarked grayscale images with different watermark images under no attacks in visual observations. As can be observed from Tables 1 to 2 and figures 5 to 7, the watermarked grayscale images and the original grayscale images are more similar which means the proposed method is more imperceptible. Furthermore, as can be seen from Table 2 and figures 5 to 7, the watermark images can be extracted fully and are more similar to the original watermark images which means the proposed method is more robust.

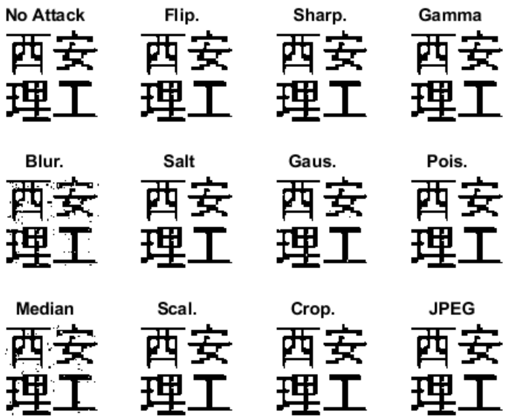

Fig. 8: The extracted watermark 1 from Lena image under different attack

Tables 3 to 5 show the NC values with watermark images from original images under different attacks while figures 8 to 10 show the extracted watermark images from Lena image under various attacks in visual observations. As can be observed from these figures, the extracted watermark images are very similar to the original watermark images and are extracted fully except that extracted under blurring and median filter attacks which have a little distortion.

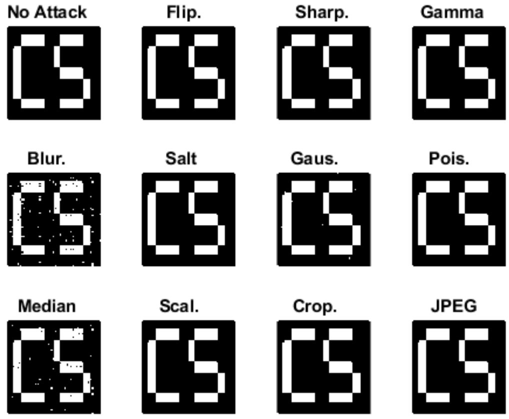

Fig. 9: The extracted watermark 2 from Lena image under different attack

Fig. 10: The extracted watermark 3 from Lena image under different attack

It can be concluded from these Tables and figures that the proposed grayscale image watermarking scheme is a superior performance in terms of both imperceptibility and robustness against common attacks. For more investigation, the proposed grayscale image watermarking scheme is compared with the existing scheme [19] that utilized the same original grayscale images and the same watermark image (watermark 2). Table 6 demonstrates the comparison of the proposed grayscale image watermarking scheme with this existing scheme. As can be determined from this Table, the proposed grayscale scheme watermarking has a superior performance in terms of robustness against some attacks than this existing scheme.

Table 3: The NC values of extracted watermark with watermark1 under different Attacks

Attack	Lena	Sailboat	Peppers	Baboon	Airplane
Flipping up to down	1.000	1.000	1.000	1.000	1.000
Sharpening (1)	1.000	1.000	1.000	1.000	1.000
Gamma correction (1.0)	1.000	1.000	1.000	1.000	1.000
Blurring (1)	0.946	0.954	0.965	0.907	0.943
Salt & Pepper noise (0.001)	1.000	1.000	1.000	1.000	1.000
Gaussian noise [0,0.001]	0.996	1.000	0.999	1.000	0.983
Poisson noise	1.000	1.000	1.000	1.000	1.000
Median filter (3×3)	0.972	0.963	0.935	0.941	0.986
Scaling (7)	1.000	1.000	1.000	1.000	1.000
Cropping (75%)	1.000	1.000	1.000	1.000	1.000
JPEG2000 (Comp. Ratio=5)	1.000	1.000	1.000	1.000	1.000

Table 4: The NC values of extracted watermark with watermark2 under different Attacks

Attack	Lena	Sailboat	Peppers	Baboon	Airplane
Flipping up to down	1.000	1.000	1.000	1.000	1.000
Sharpening (1)	1.000	1.000	1.000	1.000	1.000
Gamma correction (1.0)	1.000	1.000	1.000	1.000	1.000
Blurring (1)	0.941	0.942	0.956	0.882	0.933
Salt & Pepper noise (0.001)	1.000	1.000	1.000	1.000	1.000
Gaussian noise [0,0.001]	0.995	1.000	0.998	1.000	0.981
Poisson noise	1.000	1.000	1.000	1.000	1.000
Median filter (3×3)	0.971	0.954	0.942	0.924	0.986
Scaling (7)	1.000	1.000	1.000	1.000	1.000
Cropping (75%)	1.000	1.000	1.000	1.000	1.000
JPEG2000 (Comp. Ratio=5)	1.000	0.999	0.999	0.995	0.998

Table 5: The NC values of extracted watermark with watermark3 under different Attacks

Attack	Lena	Sailboat	Peppers	Baboon	Airplane
Flipping up to down	1.000	1.000	1.000	1.000	1.000
Sharpening (1)	1.000	1.000	1.000	1.000	1.000
Gamma correction (1.0)	1.000	1.000	1.000	1.000	1.000
Blurring (1)	0.958	0.960	0.971	0.917	0.947
Salt & Pepper noise (0.001)	1.000	1.000	1.000	1.000	1.000
Gaussian noise [0,0.001]	0.994	1.000	0.999	1.000	0.983
Poisson noise	1.000	1.000	1.000	1.000	1.000
Median filter (3×3)	0.970	0.974	0.954	0.949	0.970
Scaling (7)	1.000	1.000	1.000	1.000	1.000
Cropping (75%)	1.000	1.000	1.000	1.000	1.000
JPEG2000 (Comp. Ratio=5)	1.000	0.999	0.999	0.998	1.000

Table 6: The comparison of the proposed scheme of watermark 2 with the existing scheme

Image	Scheme	PSNR	NC			
			Gaussian noise 0.001	Median filter 3×3	Scaling ×2	Poisson noise
Lena	[19]	37.369	1.000	0.875	1.000	1.000
	Proposed	44.882	0.995	0.971	1.000	1.000
Baboon	[19]	33.143	1.000	0.896	1.000	1.000
	Proposed	37.481	1.000	0.924	1.000	1.000
Airplane	[19]	36.939	1.000	0.820	1.000	1.000
	Proposed	46.371	0.981	0.986	1.000	1.000

Conclusion

A novel robust blind grayscale image digital watermarking scheme is introduced in this paper based on lifting wavelet transform in combination with discrete cosine transform, Hessenberg decomposition, and entropy analysis for copyright protection of multimedia information. In this scheme, different standard grayscale images are utilized to hide different watermarks to analyze the effect of different watermarks on different original grayscale images. Various digital watermarking attacks are applied including adding noise, filtering, Gamma correction, scaling, cropping, sharpening, blurring, and JPEG 2000 compression attacks. Two main properties imperceptibility and robustness in digital watermarking technology are obtained in this scheme with a peak signal to noise ratio (PSNR) value with no attack > 37 dB and normalize cross-correlation (NC) value with no attack = 1.000. The proposed grayscale image digital watermarking scheme is invariant against common attacks with different grayscale images and different watermarks. The proposed grayscale image digital watermarking scheme has a superior performance in terms of imperceptibility and robustness.

References

[1]- Patra J. C., Phua J. E., Bornand C., (2010), A Novel DCT Domain CRT-Based Watermarking Scheme for Image Authentication Surviving JPEG Compression., Digital Signal Processing, **20**, 1597-1611.

[2]- Byun S.-W., Son H.-S., Lee S.-P., (2019), Fast and Robust Watermarking Method Based on DCT Specific Location., IEEE

Access, **7**, 100706-100718.

[3]- VERMA V. S., JHA R. K.,OJHA A., (2015), Significant Region Based Robust Watermarking Scheme in Lifting Wavelet Transform Domain., Expert Systems with Applications, **42**, 8184-8197.

[4]- LEI B., SOON Y., ZHOU F., LI Z.,LEI H., (2012), A Robust Audio Watermarking Scheme Based on Lifting Wavelet Transform and Singular Value Decomposition., Signal processing, **92**, 1985-2001.

[5]- ERNAWAN F., KABIR M. N., (2020), A Block-Based RDWT-SVD Image Watermarking Method using Human Visual System Characteristics., The Visual Computer, **36**, 19-37.

[6]- JAMAL S. S., SHAH T., FARWA S.,KHAN M. U., (2019), A New Technique of Frequency Domain Watermarking Based on a Local Ring., Wireless Networks, **25**, 1491-1503.

[7]- MAKBOL N. M., KHOO B. E.,RASSEM T. H., (2016), Block-Based Discrete Wavelet Transform-Singular Value Decomposition Image Watermarking Scheme using Human Visual System Characteristics., IET Image processing, **10**, 34-52.

[8]- ZEAR A., SINGH A. K.,KUMAR P., (2018), A Proposed Secure Multiple Watermarking Technique Based on DWT, DCT and SVD for Application in Medicine., Multimedia Tools and Applications, **77**, 4863-4882.

[9]- CEDILLO-HERNÁNDEZ M., GARCÍA-UGALDE F., NAKANO-MIYATAKE M.,PÉREZ-MEANA H. M., (2014), Robust Hybrid Color Image Watermarking Method Based on DFT Domain and 2D Histogram Modification., Signal, Image and Video Processing, **8**, 49-63.

[10]- ABODENA O., AGOYI M.,CELEBI E., Hybrid Technique for Robust Image Watermarking using Discrete Time Fourier Transform, in 2017 25th Signal Processing and Communications Applications Conference (SIU), 2017, 1-4.

[11]- GUO Y., LI B.-Z., (2016), Blind Image Watermarking Method Based on Linear Canonical Wavelet Transform and QR Decomposition., IET image processing, **10**, 773-786.

[12]- VALI M. H., AGHAGOLZADEH A.,BALEGHI Y., (2018), Optimized Watermarking Technique using Self-Adaptive Differential Evolution Based on Redundant Discrete Wavelet Transform and Singular Value Decomposition., Expert Systems with Applications, **114**, 296-312.

[13]- ABODENA O., AGOYI M., (2018), Colour Image Blind Watermarking Scheme Based on Fast Walsh Hadamard Transform and Hessenberg Decomposition., Studies in Informatics and Control, **27**, 339-348.

[14]- THANKI R., KOTHARI A.,TRIVEDI D., (2019), Hybrid and Blind Watermarking Scheme in Dcut–RDWT Domain., Journal of Information Security and Applications, **46**, 231-249.

[15]- HU H.-T., CHANG J.-R.,LIN S.-J., (2018), Synchronous Blind Audio Watermarking via Shape Configuration of Sorted LWT Coefficient Magnitudes., Signal Processing, **147**, 190-202.

[16]- BRAHIMI N., BOUDEN T., BRAHIMI T.,BOUBCHIR L., (2020), A Novel and Efficient 8-Point DCT Approximation for Image Compression., Multimedia Tools and Applications, 1-17.

[17]- SU Q., CHEN B., (2017), A Novel Blind Color Image Watermarking using Upper Hessenberg Matrix., AEU-International Journal of Electronics and Communications, **78**, 64-71.

[18]- SWELDENS W., (1998), The lifting scheme: A Construction of Second Generation Wavelets., SIAM journal on mathematical analysis, **29**, 511-546.

[19]- KAZEMIVASH B., MOGHADDAM M. E., (2017), A Robust Digital Image Watermarking Technique using Lifting Wavelet Transform and Firefly Algorithm., Multimedia Tools and Applications, **76**, 20499-20524.

[20]- BHARDWAJ A., VERMA V. S.,JHA R. K., (2018), Robust Video Watermarking using Significant Frame Selection Based on Coefficient Difference of Lifting Wavelet Transform., Multimedia Tools and Applications, **77**, 19659-19678.

[21]- SUN L., LIANG S., CHEN P.,CHEN Y., (2021), Encrypted Digital Watermarking Algorithm for Quick Response Code using Discrete Cosine Transform and Singular Value Decomposition., Multimedia Tools and Applications, **80**, 10285-10300.

[22]- ABODENA O., ALASHTIR A., (2021), High Hiding Capacity Audio Watermarking Method Based on Discrete Cosine Transform., International Journal Of Advance Research And Innovative Ideas In Education, **7**, 677-684.

[23]- SU Q., (2016), Novel Blind Colour Image Watermarking Technique using Hessenberg Decomposition., IET image processing, **10**, 817-829.

[24]- KUMAR S., SINGH B. K., (2021), Entropy based Spatial Domain Image Watermarking and its Performance Analysis., Multimedia Tools and Applications, **80**, 9315-9331.

[25]- KUMAR S., SINGH B. K., (2021), DWT Based Color Image Watermarking using Maximum Entropy., Multimedia Tools and Applications, **80**, 15487-15510.

[26]- WEBER A. G., (2006), The USC-SIPI Image Database: Version 5. http://sipi. usc. edu/database/,

[27]- YADAV A. K., MEHTA R., KUMAR R.,VISHWAKARMA V. P., (2016), Lagrangian Twin Support Vector Regression and Genetic Algorithm Based Robust Grayscale Image Watermarking., Multimedia Tools and Applications, **75**, 9371-9394.

[28]- KESHAVARZIAN R., AGHAGOLZADEH A., (2016), ROI Based Robust and Secure Image Watermarking using DWT and Arnold Map., AEU-International Journal of Electronics and Communications, **70**, 278-288.