A Secure Blind Watermarking Scheme Using Wavelets, Arnold Transform and QR Decomposition

Ayesha Shaik

▶ **To cite this version:**

Ayesha Shaik. A Secure Blind Watermarking Scheme Using Wavelets, Arnold Transform and QR Decomposition. 3rd International Conference on Computational Intelligence in Data Science (ICCIDS), Feb 2020, Chennai, India. pp.143-156, 10.1007/978-3-030-63467-4_11 . hal-03434802

HAL Id: hal-03434802
https://inria.hal.science/hal-03434802

Submitted on 18 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Secure Blind Watermarking Scheme using Wavelets, Arnold Transform and QR decomposition

Ayesha Shaik

School of Computing Science and Engineering,
Vellore Institute of Technology
Chennai-600127, India
ayeshanoormd@gmail.com
orcid.org/0000-0002-9804-8031

Abstract. In recent years the amount of digitally stored content available as images, videos, documents, etc., has increased exponentially. With the invention of public storages like clouds etc., security and privacy of digital data are of extreme importance. With the availability of powerful editing tools, modification of digital data is no longer a challenging task. Content modification can be done either with positive intentions like image and video enhancement or with malicious intentions like image, video morphing, video piracy, etc. To detect malicious activities, ownership of digital content needs to be established. One possible solution is to embed owner information during the content generation process. So, a secure watermarking (WMG) scheme is proposed using Wavelet transform, Arnold transforms (AT) and QR factorization in this article. The novelty of this technique is the unique way of generating WM (watermark) which makes the WMG secure. The technique is analyzed using the images given in datasets, signal and image processing institute (SIPI), break our watermarking system (BOWS), and Copydays. The experimental results of the proposed scheme are promising.
Keywords: Watermarking, Robustness, Attacks, QR factorization, Arnold transform

1 Introduction

The very fast growth in multimedia communication over the interconnected networks has raised an important issue of security and privacy of the digital data. The data needs to be authenticated as there is a chance of getting attacked or modified by third parties. So, a technique known as digital WMG came into existence for data authentication (DA) and copyright protection (CP) where copyright is inserted into the digital content. The other applications of this scheme are automated control, broadcast monitoring, user identification/authentication and fingerprinting, etc. The digital WMG scheme is designed specifically to domain i.e., spatial and transform domain. Based on the perceptibility of the watermark (WM), the watermarking technique is classified as VISIBLE and INVISIBLE

schemes. Moreover, we can again classify them as blind (B) and non-blind (NB) WMG schemes depending on the requirement of the CI (cover image) during WM extraction. The basic requirements of the WMG scheme are the robustness (Ro) and imperceptibility (Im) of the scheme. Robustness is defined as the tolerance of the WMG scheme towards the attacks. The imperceptibility is defined as the invisibility of the WM i.e., the quality of the watermarked image (WMI). Based on the strength of the WM, the watermarking scheme is classified as robust (R), semi-fragile (SF) and fragile (F). A robust WMG scheme will tolerate a set of attacks, fragile WMG scheme can't tolerate any attack and the WMG scheme that is not R and F can be categorized as a semi-fragile WMG scheme.

In the existing works, the WM is embedded directly on the original data or in the frequency domain. A few works used a combination of discrete wavelet transform (DWT) and the singular value decomosition (SVD) decomposition, where the WM is embedded in the singular values (SVs) of the original values. The disadvantage of these schemes is they are susceptible to the false positive problem of ownership authentication. So, in the proposed work, a combination of DWT and QR decomposition is used followed by AT. Here, AT is used to disorder the pixel values using a secure key such that the third parties will not be able to find out the exact modification done to the data. The combination of these three algorithms and the way they have used in the proposed work both are novel. One more advantage of the proposed work is that a content dependent watermark is generated from the original watermark using QR decomposition which was detailed in detail in the later sections. On the whole, the proposed technique is secure and robust, and it helps to protect the copyrights of the owner.

In this article, a secure WMG scheme using wavelet, Arnold transform and QR factorization is proposed. Section 2 discusses the overview of the WMG schemes existing in the literature. Section 3 presents the preliminaries required to implement the proposed work. Section 4 presents the proposed method in detail. Section 5 gives the results and analysis of the proposed method. Section 6 gives a conclusion followed by the references.

2 Literature Survey

In transform domain, DWT [4], Discrete Cosine Transform (DCT) [9] , SVD [5] and Walsh-Hadamard transform (WHT) are existing. In [16] an adaptive WMG scheme is discussed, where the WM is inserted into the most significant part of the CI. A WMG scheme that uses Just-Noticeable Difference (JND) and Fuzzy Inference System (FIS) along with genetic algorithm (GA) is presented in [26]. An SVD WMG technique is discussed in [18] along with Tiny-GA. Fuzzy logic and Tabu search combined digital image WMG scheme is presented in [19]. A color image WMG using QR decomposition is discussed in [25].

A WMG technique using multi-resolution (MR) and complex Hadamard transform is proposed in [10], where the first multi-resolution transform is applied and then insert the WM using Hadamard transform. A watermarking technique

which utilizes an optimal transport to map a list of original signals to a list of watermarked signals is discussed in [21]. In [17], the author has proposed a digital image WMG technique using DWT and SVD with least significant bit (LSB)-based techniques to protect copyrights and robust to many atatcks.

In [12], the combined 3-level DWT and DCT coefficients are selected to embed a binary WM bit in the cover image (CI) and support vector machine (SVM) is used to retrieve the watermark. Here, the PSNR achieved for 300 images is around 42.45 dB. A review of optical image hiding (IH) and WMG techniques has been discussed in [14]. In this technique, a review of various optical systems and architectures for IH and the summary of processing algorithms related to optical IH are presented. A review of different digital image WMG algorithms in the frequency domain to prove the ownership of the data into the digital image without affecting its Visual Quality (VQ) has been proposed in [15]. Here, the author has found a wide variety of applications and classifications of the same for digital watermarking methods. The author used the Discrete Orthonormal Stockwell Transform (DOST) to achieve improved robustness and imperceptibility of the WMI.

A selected wavelet SVD-based WMG scheme has been presented in [23], in which the author mentioned that the embedding in the RGB and YCbCr color channels achieves high imperceptibility. Here, three different SVD-based image WMG schemes with different wavelet transforms are selected for color image testing and eavaluation. A digital image WMG technique based on DWT and encryption has been discussed in [4]. Here, the demonstration of WM inserting and retrieval algorithm using DWT coefficients, distance measures, and encryption has been discussed. Authors of [4] presented that the DWT through multi-resolution analysis provides the much-needed simplicity in WM inserting and retrieval through WM encryption. In [6], the authors discussed the standard WMG system frameworks and listed the needed requirements to design WMG techniques, and reviewed them to find the limitations of state-of-the-art methods.

3 Preliminaries

3.1 QR factorization

The QR factorization [25] of a matrix will be done using the following equation 1.

$$[E_A \ F_A \ G_A] = qr(A) \tag{1}$$

Where A is a d $\times$ d matrix that we need to decompose, E_A is an d $\times$ d unitary matrix, G_A is an d $\times$ d permutation matrix and F_A is an d $\times$ d upper triangular matrix. Using Gram-Scmidth orthogonalization technique the columns of E_A are generated from columns of A. If $A = [\ a_1, a_2, \ldots, a_k]$ and $E_A = [e_1, e_2, \ldots, e_k]$, where a_i and e_i are column vectors, then matrix F_A can be calculated as shown

below:

$$F_A = \begin{bmatrix} \langle a_1, e_1 \rangle & \langle e_2, q_1 \rangle & \langle e_3, q_1 \rangle & \dots & \langle e_k, q_1 \rangle \\ \langle a_1, e_2 \rangle & \langle e_2, q_2 \rangle & \langle e_3, q_2 \rangle & \dots & \langle e_k, q_2 \rangle \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle a_1, e_k \rangle & \langle e_2, q_k \rangle & \langle e_3, q_k \rangle & \dots & \langle e_k, q_k \rangle \end{bmatrix} \tag{2}$$

where $\langle \cdot, \cdot \rangle$ denotes an inner product.

3.2 Arnold Transform (AT)

This transform [27] is widely used because of its periodicity. It is usually used for digital encryption and it is the process of reallignment of the pixels in the digital data (image). A 2D AT is computed as shown:

$$\begin{pmatrix} k^{'} \\ l^{'} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} mod\ S \tag{3}$$

Where k and l are the coordinates of digital image, $k^{'}$ and $l^{'}$ are the coordinates of the scrambled image. S is the size (height or width) of the image (If the image size is $x \times x$ then height will be x). If this operation done repeatedly then the output will be an entirely disordered image compared to the original digital image for a few number of iterations.

3.3 Normalized cross correlation (NC)

$$NC(B, \hat{B}) = \frac{\sum_c \sum_d B(c,d)\hat{B}(c,d)}{\sqrt{\sum_c \sum_d B(c,d)^2}\sqrt{\sum_c \sum_d \hat{B}(c,d)^2}} \tag{4}$$

where B and $\hat{B}$ are original image and the image that is processed.

4 Proposed Watermarking Scheme

The proposed WMG scheme for embedding the WM is given in Fig. 1. The original image I is divided into 4 SBs by applying 2-level DWT. These subbands (SBs) are undergone QR decomposition and Arnold transform to obtain the upper triangular matrices (UTMs) of the original image. The watermark W is converted to hexadecimal form and a predictive watermark is generated as given in equation (5). On W, QR decomposition is applied to produce UTMs of the watermark. The UTMs of original data are modified with the UTMs of the WM using the embedding strengths $\alpha_{LL}, \alpha_{LH}, \alpha_{HL}, \alpha_{HH}$ and predicted watermark to obtain the WMI I_W. The WMG procedure and extraction is provided in detail in the algorithms.

The proposed WM embedding scheme is detailed in Algorithm 1. The WM is generated in a unique way in this article. It has all the information related to the

Algorithm 1 Watermark embedding

Input: Original Image I, Watermark W and embedding strengths $\alpha_{LL}, \alpha_{LH}, \alpha_{HL}, \alpha_{HH}$

Output: WMI I_W

1: Apply 2-level DWT on I and W to decompose into sub bands (SBs),

$$(LL_I,\ LH_I,\ HL_I,\ HH_I) = DWT(I)$$
$$(LL_W,\ LH_W,\ HL_W,\ HH_W) = DWT(W)$$

2: Perform QR decomposition on $(LL_I,\ LH_I,\ HL_I,\ HH_I)$

$$QR(LL_I) = Q_{LL_I}\ R_{LL_I}\ P_{LL_I}$$
$$QR(LH_I) = Q_{LH_I}\ R_{LH_I}\ P_{LH_I}$$
$$QR(HL_I) = Q_{HL_I}\ R_{HL_I}\ P_{HL_I}$$
$$QR(HH_I) = Q_{HH_I}\ R_{HH_I}\ P_{HH_I}$$

3: Apply QR on W

$$QR(LL_W) = Q_W\ R_W\ P_W$$

4: Convert W to hexadecimal i.e., W_H

5: Calculate predictive watermark W_B from W as shown.

$$\text{if}(W_i = W_{i+1}) \text{ then } W_{B_i} = 0;\ \text{else } W_{B_i} = 1 \tag{5}$$

6: Apply Arnold transform on $R_{LL_I}, R_{LH_I}, R_{HL_I}$ and R_{HH_I}

$$\begin{aligned} R^a_{LL_I} &= Arnold(R_{LL_I}) \\ R^a_{LH_I} &= Arnold(R_{LH_I}) \\ R^a_{HL_I} &= ArnoldR_{HL_I}) \\ R^a_{HH_I} &= Arnold(R_{HH_I}) \end{aligned} \tag{6}$$

7: Find

$$\begin{aligned} R^{ma}_{LL_I} &= {R_{LL_I}}^a + \frac{\alpha_{LL} \times R_W \times W_B}{W_H} \\ R^{ma}_{LH_I} &= {R_{LH_I}}^a + \frac{\alpha_{LH} \times R_W \times W_B}{W_H} \\ R^{ma}_{HL_I} &= {R_{HL_I}}^a + \frac{\alpha_{HL} \times R_W \times W_B}{W_H} \\ R^{ma}_{HH_I} &= {R_{HH_I}}^a + \frac{\alpha_{HH} \times R_W \times W_B}{W_H} \end{aligned} \tag{7}$$

8: Multiply the matrices as given below

$$\begin{aligned} R^{QR}_{LL_I} &= Q_{LL_I} \times R^{ma}_{LL_I} \times P_{LL_I} \\ R^{QR}_{LH_I} &= Q_{LH_I} \times R^{ma}_{LH_I} \times P_{LH_I} \\ R^{QR}_{HL_I} &= Q_{HL_I} \times R^{ma}_{HL_I} \times P_{HL_I} \\ R^{QR}_{HH_I} &= Q_{HH_I} \times R^{ma}_{HH_I} \times P_{HH_I} \end{aligned} \tag{8}$$

9: Perform inverse DWT to obtain WMI, I_W

$$I_W = Inverse\ DWT(R^{QR}_{LL_I},\ R^{QR}_{LH_I},\ R^{QR}_{HL_I},\ R^{QR}_{HH_I}) \tag{9}$$

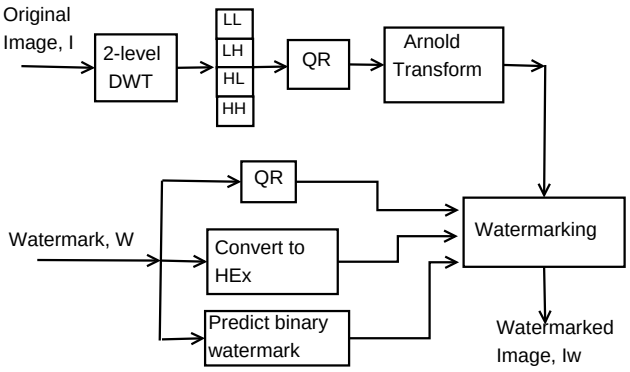

Fig. 1: Block diagram proposed WMG scheme for WM embedding

WM and it is encrypted using the predicted WM and binary WM. According to Algorithm 1, the OI and WM is gone through 2-level DWT to obtain the SBs. The 2-level SBs (LL_I, LH_I, HL_I, HH_I) of the OI will be decomposed into their corresponding unitary matrices and UTMs using QR decomposition. The 2-level sub-band of WM, LL_W will be decomposed into unitary matrix Q_W and UTM R_W. The WM is converted into hexadecimal form W_H, and the WM is predicted to get a binary WM W_B as shown in equation (5). The upper triangular matrices (UTMs) $R_{LL_I}, R_{LH_I}, R_{HL_I}, R_{HH_I}$ of the original image SBs will be transformed using AT to obtain $R^a_{LL_I}, R^a_{LH_I}, R^a_{HL_I}, R^a_{HH_I}$. In the transformed UTMs $R^a_{LL_I}, R^a_{LH_I}, R^a_{HL_I}, R^a_{HH_I}$, the unique generated watermark (GW) G_W will be embedded as given in equation (6) to obtain $R^{ma}_{LL_I}, R^{ma}_{LH_I}, R^{ma}_{HL_I}, R^{ma}_{HH_I}$. The GW is holding properties of W_H, W_B and the UTM of the WM, $G_W = \frac{\alpha_{SB} \times R_W \times W_B}{W_H}$, where α_{SB} is α_{LL} for LL sub-band, α_{SB} is α_{LH} for LH sub-band, α_{SB} is α_{HL} for HL sub-band and α_{SB} is α_{HH} for HH sub-band respectively. The unitary matrices and permutation matrices are multiplied with the WM embedded UTMs to obtain the product matrices $R^{QR}_{LL_I}, R^{QR}_{LH_I}, R^{QR}_{HL_I}, R^{QR}_{HH_I}$ as given in equation (8), and the inverse 2-level DWT is performed on them to obtain WMI I_W.

For retrieval of the watermark, WM extracting algorithm is detailed in Algorithm 2. In this algorithm, the possibly modifed WMI, $I^{'}_W$ is undergone 2-level DWT to decompose into sub-bands $(LL^{'}_I, LH^{'}_I, HL^{'}_I, HH^{'}_I)$ and perform QR decomposition QR decomposition to obtain the UTMs of all SBs. Inverse AT is applied on those UTMs to produce the $R^{inv}_{LL_I}, R^{inv}_{LH_I}, R^{inv}_{HL_I}, R^{inv}_{HH_I}$ matrices as given in Algorithm 2. Now, extract the WM $W_{ex_{LL}}$ as given in equation (11) and calculate W^*_{LL} as given in equation (12). The steps are repeated for the other SBs to extract $W^*_{LH}, W^*_{HL}, W^*_{HH}$. After extraction of the WM, the inserted WM is correlated with the extracted WM as given in equation (4). If the correlation is high then the ownership identification can be done else it can't be done.

Algorithm 2 Watermark extraction

Input: Possibly modified WMI, $I_W^{'}$,$(\alpha_{LL}, \alpha_{LH}, \alpha_{HL}, \alpha_{HH})$,$W_B$, W_H,$(R_{LL_I}, R_{LH_I}, R_{HL_I}, R_{HH_I})$

Output: Extracted encrypted watermark,W^*

1: Apply DWT on $I_W^{'}$ and decompose into sub bands,$(LL_I^{'},\ LH_I^{'},\ HL_I^{'},\ HH_I^{'})$

2: Perform QR on all the subbands $(LL_I^{'},\ LH_I^{'},\ HL_I^{'},\ HH_I^{'})$

$$QR(LL_I^{'}) = Q_{LL_I}^{'}\ R_{LL_I}^{'}\ P_{LL_I}^{'}$$

3: Calculate

$$R_{LL_I}^{inv} = invArnold(R_{LL_I}^{'}) \tag{10}$$

4: Calculate

$$W_{ex_{LL}} = \frac{(R_{LL_I}^{inv} - R_{LL_I}) \times W_H}{W_B \times \alpha_{LL}} \tag{11}$$

5: Calculate W_{LL}^*

$$W_{LL}^* = Q_W \times\ W_{ex_{LL}} \times\ P_W \tag{12}$$

6: Similarly repeat the steps for all the SBs and extract WMs $W_{LH}^*, W_{HL}^*, W_{HH}^*$

7: Find NC between inserted encrypted and extracted encrypted WM by using equation (4).

8: If the NC is greater than the predefined threshold then the ownership is authenticated. Otherwise it is not authenticated.

5 Results and analysis

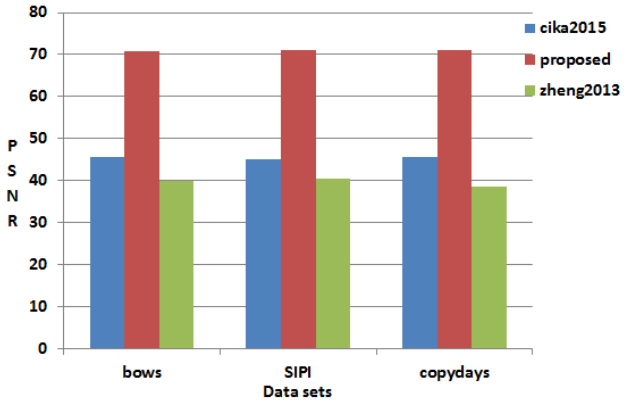

Fig. 2: PSNR values for the images in standard data sets

The proposed WMG method is analyzed using the images dataset [1], [2] and [3]. The original and WMIs is shown in Fig. 3, where Fig. 3(a) and Fig. 3(b)

are the original flower image and watermarked flower images, Fig. 3(c) and Fig. 3(d) are the original boat image and watermarked boat images, Fig. 3(e) and Fig. 3(f) are the original scenary image and watermarked scenary images, and Fig. 3(g) and Fig. 3(h) are the original mountain image and watermarked mountain images respectively. The average PSNR values for the images in three datasets BOWS, SIPI, and Copydays for the methods presented in [8], [28] and for the proposed method are shown in Fig. 2. From this figure 2, it is clear that the average PSNR value obtained for the proposed method is higher than the other two listed methods.

The correlation betwen the inserted and extracted WMs is listed in Table 1 for the proposed method and the method presented in [21]. From this table 1, one can clearly notice that the correlation values for the proposed scheme is better than the listed existing scheme. One should understand that if the correlation value is closer to zero, the ownership authentication can't be done and if the correlation value is close to 1, then ownership authentication can be done. So, from the table, it is clear that the proposed method shows better performance than the listed scheme. The PSNR values obtained by the proposed technique and the method given in [20] are listed in Table 2. From this table 2, one can clearly notice that the PSNR values for the proposed scheme is better than the listed existing scheme.

The execution time for the existing techniques and the proposed method is listed in 3. The first five rows presents the execution time taken by the existing techniques and the last three rows shows the execution time taken by the proposed method for the three datasets (SIPI, Copydays, and BOWS) respectively. From the table, one can notice that the proposed method consumes lesser time compared to the existing methods. Hence, one can say that the proposed method exhibits better performance compared to the listed existing techniques. The average PSNR values for the images in three datasets BOWS, SIPI, and Copydays for the methods presented in [8], [28] and for the proposed method are shown in Fig. 4. From this figure 4, it is clear that the average BER value obtained for the proposed method is lower than the other two listed methods, which means that the proposed method exhibits better performance compared to the other two listed techniques. The PSNR values obtained by the proposed technique and the method given in [12] are listed in Table 4. From this table 4, one can clearly notice that the PSNR values for the proposed scheme is better than the listed existing scheme. One should understand that if the PSNR value is higher (infinite in ideal case), then the VQ of WMI is better else it will be of less VQ. So, from the table, it is clear that the proposed method shows better performance than the listed scheme.

(a) Original flower

(b) Watermarked flower

(c) Original boat

(d) Watermarked boat

(e) Original scenary

(f) Watermarked scenary

(g) Original mountain

(h) Watermarked Mountain

Fig. 3: Original and WMIs for proposed method

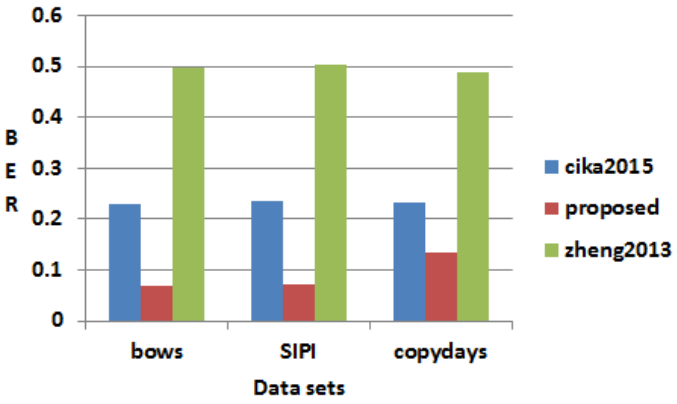

Fig. 4: bit error rate (BER) values for the images in standard data sets

Table 1: NC correlation values between extracted and original watermarks

Sl. No	Attack	Proposed	TNW [21]
1	Crop	0.896	0.682
2	Gaussian Noise	0.9395	0.675
3	Salt And Pepper Noise	0.93	0.665
4	Histogram Equalization	0.9314	0.678
5	Xshear	0.75	0.607
6	Yshear	0.81	0.613

Table 2: PSNR values for the proposed and [20]

Sl. No	Image	Proposed	Majumder [20]
1.	Boat	47.77	45.9
2.	Monkey	51.4852	45.9
3.	Woman	53.9	45.12
4.	Peppers	47.6	44.87
5.	Nature	55.28	44.8
6.	Lena	49.9	44.37
7.	Aeroplane	53.4	45.36
8.	Correction	54.4	44.86

The comparison of execution time of different existing techniques are listed in Table 2 and compared with the proposed technique. In this experimental analysis, a laptop computer with a Intel(R) Core(TM) i7-5500U CPU at 2.40GHz, Win 10, MATLAB R 2015 a is used as computing platform.

Table 3: Execution time for the listed techniques

Sl. No	Method	Execution time(in seconds)
1.	Chou [7]	2.5122319
2.	Golea [11]	2.815017
3.	Yashar [22]	1.368692
4.	Su [24]	1.855
5.	Qingtang [25]	1.11399
6.	Proposed (SIPI [3])	0.8525148
7.	Proposed (Copydays [1])	0.85324
8.	Proposed (BOWS [2])	0.852338

The execution time of the proposed method is very less compared to the listed techniques in the Table 2. In [7] the CI has to be changed to color space for the color quantization and its inverse-transformation is also involved, [22] involves wavelet and QR decomposition but it requires block decomposition which is time consuming and [24] uses schur decomposition which requires about $8N^3/3$ flops, SVD decomposition requires about $11N^3/3$ flops, and the QR decomposition in between [7] which makes it time consuming. The presented method uses 2 level DWT and QR only to a significant SBs which makes it fast compared to the listed tecniques.

Evaluation of the digital watermarking techniques is done based on the following categories:

- Theoritical computational complexity: Upper bound of the methodologies used for watermarking
- Practical computational time: System time consumed for watermarking
- Watermarked image quality: peak signal-to-noise ratio, structural similarity index
- Tolerance of the watermarking method against the atatcks such as Gaussian noise, Salt & pepper noise, Median filtering, Average filtering, and so on: bit error rate, normalized correlation.

In the table 3, different watermarking techniques have been compared for the time required for watermarking. This can be done as it is one of the factor to compare these techiques. If we see in detail, the method in [7] have the complexity of $O(n^2)$ and this method is presented in spatial domain, and as the spatial

domain techniques are considered to be fragile in nature (not tolerant), this method is not suggested for robust applications. Similarly, the computational complexities of the method given in [11] is $O(n^3)$ as it is using SVD transform, the method in [22] is $O(n^2)$ as it is using DWT transform, the method given in [24] is $O(n^3)$ as it is using Schur decomposition and Schur decomposition uses QR decomposition, and the method given in [25] is $O(n^3)$ as it is using QR decomposition. The proposed method has the computational complexity of $\max(O(n^3),O(n^3))$ which is $O(n^3)$, as it uses DWT and QR decomposition.

Table 4: PSNR values for the proposed and [12]

Sl. No	Image	Proposed	WT-DCT [12]
1.	Lena	47.77	42.98
2.	Peppers	47.6	43.24
3.	Mandril	53.9	41.79
4.	Jetplane	48.6	42.92
5.	Barbara	55.28	41.49
6.	Lake	50.9	42.88
7.	X-ray	52.4	43.01
8.	Galaxy	51.4	42.45
9.	Living room	47.4	42.18
10.	Elaine	45.4	41.96

The use of AT encrypts the WM that will make sure that the ordering of the original pixel are not proper and the GW embedded is also a mixture of different variations of the WM which makes the scheme secure. More over the degradation done to the CI is only to the UTM of the SBs which is not significantly perceptual which in turn produces a high quality WMI. The QR decomposition is used to prevent the degradation to the sub-bands, instead the the WM is embedded in UTMs of SBs which ensures the less quality degradation to get high quality visual image.

6 Conclusion

A digital image watermarking scheme using 2-level DWT, Arnold transform and QR decomposition is proposed in this article. The cover image is decomposed into the sub-bands and QR is applied on all the subbands, which gives

an unitary matrix and an upper triangular matrix. The watermark is undergone discrete wavelet transform and then QR decomposition. The watermark is then tranformed to hexadcimal form andtransformed to binary based on predictive process. Now the upper triangular matrix of the cover image sub-bands are modified with the upper triangular matrix of the watermark, binary predictive watermark and hex-watermark with the embedding strength. The experimental results of the proposed method are promising. It gives better PSNR and good robustness towards a list of geometric attacks making the scheme robust.

References

1. http://lear.inrialpes.fr/\~jegou/data.php\#copydays, accessed(May 2014)
2. http://bows2.ec-lille.fr, accessed(August 2015)
3. http://sipi.usc.edu/database/database.php\?volume=misc (July 2015), accessed
4. Ambadekar, S.P., Jain, J., Khanapuri, J.: Digital image watermarking through encryption and dwt for copyright protection. In: Recent Trends in Signal and Image Processing, pp. 187–195. Springer (2019)
5. Bao, P., Ma, X.: Image adaptive watermarking using wavelet domain singular value decomposition (2005)
6. Begum, M., Uddin, M.S.: Digital image watermarking techniques: A review. Information 11(2), 110 (2020)
7. Chou, C.H., Wu, T.L.: Embedding color watermarks in color images (2003)
8. CIKA, P., SKORPIL, V.: Robust image watermarking method based on 2d-wht and svd. Advances in Electrical and Computer Engineering pp. 134–137 (2015)
9. Cox, I.J., Miller, M.L.: Review of watermarking and the importance of perceptual modeling. Electronic Imaging'97 pp. 92–99 (1997)
10. Falkowski, B., Lim, L.S.: Image watermarking using hadamard transforms (2000)
11. Golea, N.E.H., Seghir, R., Benzid, R.: A bind rgb color image watermarking based on singular value decomposition. ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010 pp. 1–5 (2010)
12. Islam, M., Kumar, G.R., Shaik, A.S., Laskar, R.H.: Wt-dct domain based image watermarking technique using svm. TEST Engineering & Management 82, 3195–3200 (2020)
13. Jiansheng, M., Sukang, L., Xiaomei, T.: A digital watermarking algorithm based on dct and dwt. International Symposium on Web Information Systems and Applications (WISA09) pp. 104–107 (2009)
14. Jiao, S., Zhou, C., Shi, Y., Zou, W., Li, X.: Review on optical image hiding and watermarking techniques. Optics & Laser Technology 109, 370–380 (2019)
15. Jibrin, B., Tekanyi, A., Sani, S.: Image watermarking algorithm in frequency domain: A review of technical literature. ATBU Journal of Science, Technology and Education 7(1), 257–263 (2019)
16. Joshi, V., Rane, M.: Digital water marking using lsb replacement with secret key insertion technique (2014)
17. Kumar, A.: A review on implementation of digital image watermarking techniques using lsb and dwt. In: Information and Communication Technology for Sustainable Development, pp. 595–602. Springer (2020)
18. Lai, C.C.: A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm (2011)

19. Latif, A.: An adaptive digital image watermarking scheme using fuzzy logic and tabu search (2013)
20. Majumder, S., Das, T.S., Sarkar, S., Sarkar, S.K.: Svd and lifting wavelet based fragile image watermarking (2010)
21. Mathon, B., Cayre, F., Bas, P., Macq, B.: Optimal transport for secure spread-spectrum watermarking of still images (2014)
22. Naderahmadian, Y., Hosseini-Khayat, S.: Fast watermarking based on qr decomposition in wavelet domain. 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) pp. 127–130 (2010)
23. Rassem, T.H., Makbol, N.M., Khoo, B.E.: Performance evaluation of wavelet svd-based watermarking schemes for color images. In: International Conference on Advances in Cyber Security. pp. 89–103. Springer (2019)
24. Su, Q., Niu, Y., Liu, X., Zhu, Y.: Embedding color watermarks in color images based on schur decomposition (2012)
25. Su, Q., Niu, Y., Wang, G., Jia, S., Yue, J.: Color image blind watermarking scheme based on qr decomposition (2014)
26. Tsai, H.H., Lo, S.C.: Jnd-based watermark embedding and ga-based watermark extraction with fuzzy inference system for image verification (2014)
27. Wu, L., Zhang, J., Deng, W., He, D.: Arnold transformation algorithm and anti-arnold transformation algorithm. 2009 First International Conference on Information Science and Engineering pp. 1164–1167 (2009)
28. Zheng, P., Huang, J.: Walsh-hadamard transform in the homomorphic encrypted domain and its application in image watermarking. Information Hiding pp. 240–254 (2013)