International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 09 – Issue 08 || August 2024 || PP. 70-75

Enhancing Image Steganography using Linear Algebra Approaches

Areej M. Abduldaim, Anwar Khaleel Faraj, Shatha A. Salman
Mathematics and Computer Applications, Applied Sciences Department,
University of Technology, Baghdad 10001, Iraq
Areej.M.Abduldaim@uotechnology.edu.iq, anwar.k.faraj@uotechnology.edu.iq,
Shatha.A.Salman@uotechnology.edu.iq

Abstract: Linear algebra is a core subject in computer science, influencing to development of every step of algorithm design, result analysis, and numerous other details. This paper highlights the significance and effectiveness of linear algebra by utilizing the QU decomposition to extract critical information from the concealment image to develop an image steganography mechanism. The proposed system applies the QU decomposition to all blocks obtained from dividing the LH1 and LH2 bands into 4*4 nonoverlapping blocks after implementing the DWT twice to the concealment image and once to the watermark and creating the watermarked image. The watermark image is restored successfully. The results show the success of the suggested technique via the measurements used NC and PSNR.

Keywords: Discrete Wavelet Transformations (DWT), Embedding and Extraction Algorithms, Image Steganography, Linear Algebra, QU Algebraic Decomposition.

1. INTRODUCTION

Linear algebra is the mainstay in image processing, this is due to the representation of the image as a matrix. In particular, factorization methods are used as algebraic transformations in image watermarking algorithms rather than traditional transformations. Moreover, these algebraic methods effectively determine the image's properties by analyzing the eigenvalues and eigenvectors of the image matrix. Watermarking techniques are divided into two types: image watermarking (the modifications on the original image will appear in the watermarked image) and zero watermarking (no changes appearing on the image). Many authors address image watermarking techniques in different ways. Algebraically, SVD is profusely used to improve the watermarking algorithm's robustness as in [1] the robustness is achieved via the SVD analysis-based watermarking scheme and the mathematical characteristics of SVD in addition to performing Arnold transform on the watermark image, good robustness against various attacks is kept. Zhu et al. in [2] improved the image watermarking algorithm with the Genetic Algorithm (GA) by using the integer wavelet transform (IWT) and the test outcomes explained the good imperceptibility and robustness obtained of the watermarking mechanism. Moreover, the authors in [3, 4] utilized the Gravitational Search Algorithm (GSA) and Shuffled Frog Leaping (SFL) Algorithm with GSVD and SVD. Furthermore, the computational complexity of SVD is high. Especially, when the matter is repeated, the SVD needs $O(n^3)$ flops for a matrix of order n.

As another algebraic transform namely Hessenberg algebraic factorization (Hess), a blind color image watermarking technique has been suggested in [5] by utilizing a two-level of the FWHT (fast Walsh Hadamard transform) and the DWT (discrete wavelet transform). In order to embed the watermark bits, the element in row number one, and column number one of the upper Hessenberg matrix is modified. The experiments have shown that the suggested watermarking mechanism is highly invisible with high resistance to geometrical and popular image processing attacks. Furthermore, authors in [6,7] used GA with Hess to design a zero-watermarking scheme. Due to the strength of Hess, Dhar et al. in [8] considered the parametric Slant-Hadamard transform (PSHT) as a basis of a blind symmetric audio watermarking algorithm. In addition to the RGB space, the Hess is effective in the YCbCr space as an algebraic transform to build a zero watermarking mechanism [9].

DWT plays an important role in image watermarking because it prefers dividing the image into two frequencies (high and low). As the simplest approach using wavelet transforms, the Haar wavelet is used in [10] with the Least Significant Bit (LSB) to improve the safety of the watermarking mechanism to hide a logo image in the original image. On the other hand, in quantum fields, an image logo can be included in a cover image by transforming wavelets like geometric transformation and Haar base transformation where the logo image is encoded by encapsulating a specific amount of texture [11]. Chebyshev Polynomial is utilized with the homogenous method of Diffie-Hellman to embed a watermark image (logo) in different samples from the transformed file (DCT) of the audio file [12]. According to [13] an efficient and fast technique has been designed to detect and identify the digital image copy-move forgery without any prior information concerning the image under analysis. In [14] the controller parameter is obtained by utilizing the LWT with LU algebraic factorization on the original image employing the Mamdani fuzzy inference system (FIS) which depends on getting a comparison between robustness and imperceptibility.

As a major moderate stride in SVD, the QUalgebraic factorization has lower computational complexity than SVD since the former only needs $O(n^3)$ flops while the latter needs $O(n^2)$ [15,16]. For this advantage, authors in [17] used the shearlet transform as an upgraded version of the wavelet technique which fundamentally depends on multi-resolution and multidirectional to optimize the displaying of multidimensional information. The shearlet transform overcomes the obstacle on the main characteristic that the wavelet's edge offers the image, so the host image is modeled with another texture. Robustness and imperceptibility are well-known features of the watermark. By employing QU algebraic factorization, robustness, and security improvement can be done while imperceptibility can be achieved using the Shearlet transform [18].

It is worth noting that the subject of algebra in general and linear algebra in particular has many applications, especially in computer science, as in: [19], [20], [21].

This paper adopted the QU algebraic factorization method to design a watermarking technique utilizing two levels of DWT on the original image and one level on the watermark image.

The organization of the paper is as follows. Section 2 is devoted to restating background information on the QU algebraic factorization. The methodology and the proposed technique are given in section 3. While the experimental results are shown in section 4 and finally the conclusion is presented in section 5.

2. QUALGEBRAIC FACTORIZATION METHOD

In linear algebra, a QU decomposition, also known as a QU factorization, is a decomposition of a matrix A into a product $A = QU$ of an orthonormal matrix Q and an upper triangular matrix U. Any real square matrix A may be decomposed as

$$A = QU$$

where Q is an orthogonal matrix (its columns are orthogonal unit vectors meaning $Q^T = Q^{-1}$) and U is an upper triangular matrix (also called right triangular matrix). If A is invertible, then the factorization is unique if we require the diagonal elements of U to be positive.

3. METHODOLOGY: THE PROPOSED TECHNIQUE USING QU AND DWT

In this section, the original images and the watermark are converted to grayscale space. The QU is applied to each block of the LH1 resulting from the DWT as an algebraic transform to get the important information of the host. The technique includes two algorithms, embedding, and extraction.

3.1 Embedding Algorithm:

In the proposed algorithm the size of the original color image is 512×512 at the same time the size of the watermark image is 64×64, the algorithm steps and the diagram are given below.

Algorithm: The Watermarking Technique Using $\boldsymbol{QU}$ and DWT Embedding Algorithm
Input: Original Image I, Watermark Image W Output: Watermarked Image IW
Begin Step 1: Input the original image that has size $\boldsymbol{n} \times \boldsymbol{n}$ and watermarking that has size $\boldsymbol{m} \times \boldsymbol{m}$ and convert it to a grayscale image. Step 2:The original image is decomposed by two-level DWT to obtain the sub-bands LL, LH, HL, and HH, each band is of size $\frac{\boldsymbol{n}}{\boldsymbol{4}} \times \frac{\boldsymbol{n}}{\boldsymbol{4}}$. The watermark image is decomposed by One level of DWT to obtain the sub-bands LL, LH, HL, and HH, each band is of size $\frac{\boldsymbol{m}}{\boldsymbol{2}} \times \frac{\boldsymbol{m}}{\boldsymbol{2}}$. Step 3: Divide the bands LH1 and LH into $\boldsymbol{4} \times \boldsymbol{4}$ nonoverlapping blocks. Step 4: Implement the $\boldsymbol{QU}$ algebraic factorizationto each block of the original image and the watermark. Step 5: Embed the bits of the watermark according to the following: $\boldsymbol{UIW} = \boldsymbol{UI} + \boldsymbol{S} \times \boldsymbol{UW}$ (1) Step 6: Apply the reverse operations for $\boldsymbol{QU}$ and DWT to get the watermarked image. End.

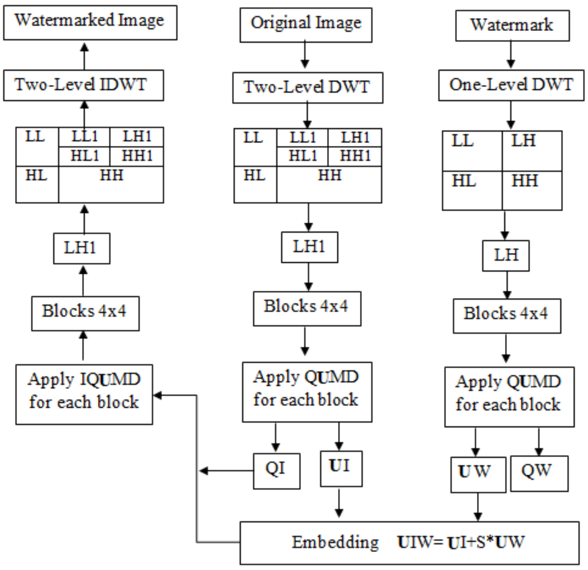


Figure 1: Steps of the Embedding Algorithm

3.2 Extraction Algorithm:

The details of the extraction are explained in the algorithm and the diagram below.

Algorithm: The Watermarking Technique Using QUMD and DWT Extraction Algorithm
Input: Watermarked Image IW Output: Watermark Image W
Begin Step 1: Input the watermarked image and the original image with size n× $\boldsymbol{n}$ and convert these images to a grayscale image. Step 2:The watermarked image is decomposed by two-level DWT to obtain the sub-bands LL, LH, HL, and HH, each band is of size $\frac{n}{4} \times \frac{n}{4}$. Step 3: Divide the band LH1 band into $\mathbf{4} \times \mathbf{4}$ nonoverlapping blocks, Step 4: Implement the $\boldsymbol{QU}$ algebraic factorization to each block in the watermarked image and original image. Step 5: Extract the bits of the watermark according to the following: $\boldsymbol{UW} = (\boldsymbol{UIW} - \boldsymbol{UI})/\boldsymbol{S}$ (2) Step 6: Apply reverse operations for $\boldsymbol{QU}$ and DWT to get the watermark. End.

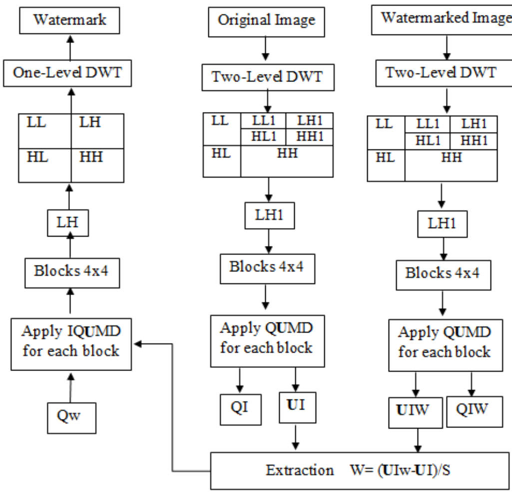


Figure 2: Steps of the Extraction Algorithm

4. EXPERIMENTAL RESULTS AND DISCUSSION

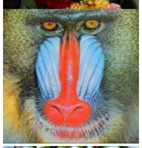
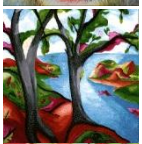
In this section, experiments will be presented to prove the efficiency and strength of the proposed algorithm in this work using color images, which are the cover image with a size of 512 x 512 with a watermark, which is a size of 64 x 64 as in table 1 that shows the images that are tested with the watermark

Table 1: The Original Images and Watermark used

W	Image_1	Image_2	Image_3	Image_4
				

The results that Table 2 displays are the ones that prove the efficiency and validity of the proposed algorithm in this work, table 3 shows the attacks that the image was exposed to with the watermark, the extracted watermark will be denoted by Ex.W.

Table 2: The Watermarked Images and the Extracted Watermark

	Original image	W	Watermarked Image	Ex. W
1				
2				
3				
4				

After the immersion and extraction process, the quality and efficiency of the watermark must be evaluated. The PSNR measurement has been relied upon. Good values have been reached. The following equation is relied upon.

$$PSNR = 10\log 10\,(\frac{MAX^2}{MSE}) \quad (3)$$
$$MSE = \frac{1}{rs}\sum_{i=0}^{r-1}\sum_{j=0}^{s-1}[I(i,j) - J(i,j)]^2 \quad (4)$$

The max value of the gray border is equal to 256.

As for the value calculated to measure the value of congruence and creative correlation (CC) between the old watermark image denoted by W and the extracted watermark image denoted by W' the following formula is used:

$$CC = \frac{W(i,j)W'(i,j)}{\sqrt{W(i,j)}\sqrt{W'(i,j)}} \quad (5)$$

In Table 3 the results obtained by applying the proposed algorithms are presented to show the PSNR values and the CC values.

Table 3: The Results Obtained Before the Attacks

Image	Image_1	Image_2	Image_3	Image_4
PSNR	57.87	57.6648	57.7806	57.7708
CC	0. 9997	0. 9997	0.99984	0.999751

The PSNR and CC are given in Table 4 below:

Table 4: The Results Obtained after the Attacks

The_Attacks	Image_1		Image_2		Image_3		Image_4	
	PSNR.	CC.	PSNR.	CC.	PSNR.	CC.	PSNR.	CC.
Salt_and_Pepper %1	26.0764	0.7134	27.3943	0.75964	26.1951	0.71705	26.7634	0.73171
Adjust_image	18.736	0.9815	19.3872	0.75964	32.5663	0.99833	21.3969	0.99283
Average_filter	37.9176	0.9708	30.9957	0.85018	30.645	0.90331	34.05	0.90331
Gaussian_Noise	37.6847	0.9662	37.6553	0.95225	37.7363	0.95373	37.6801	0.96348
Histogram_equalization	10.1288	0.8789	16.4761	0.74546	19.7047	0.93628	20.5139	0.96348
Speckle_noise	41.0426	0.9827	35.5005	0.93455	36.3188	0.94857	35.7229	0.94677

5. CONCLUSION

In this work, the QU algebraic factorization and the Discrete Wavelet Transformations (DWT) are considered to build a new technique. The DWT is applied twice to the original image and once to the watermark image. The modification is done on the selected information of the LH1 and LH channels respectively to obtain the watermarked image. The watermark was extracted successfully and good results were reached before and after the attacks.

REFERENCES

[1] Heng Zhang, Chengyou Wang, and Xiao Zhou, A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain, *Future Internet* 2017, *9, 45*; doi:10.3390/fi9030045.

[2] Ting Zhu, Wen Qu, Wenliang Cao, An optimized image watermarking algorithm based on SVD and IWT. J Supercomput **78**, 222–237 (2022). https://doi.org/10.1007/s11227-021-03886-2.

[3] A. M . Abduldaim, A. K. Faraj, Combining Algebraic GSVD and Gravitational Search Algorithm for Optimizing Secret Image Watermark Sharing Technique, *International Journal of Mathematics and Computer Science,17*,(2022),*2*,753-774.

[4] Waleed, J., Abduldaim, A.M., Alyas, H.H., Mohammed, A.Q., An Optimized Zero-Watermarking Technique Based on SFL Algorithm *2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering, ICECCPCE 2019,* 2019*, pp. 171–175, 9072723*.

[5] Omar Abodena and Mary Agoyi, Colour Image Blind Watermarking Scheme Based on Fast Walsh Hadamard Transform and Hessenberg Decomposition, *Studies in Informatics and Control, 27(3)* 339-348, September 2018.

[6] N. S. Mohammed, A.M. Abduldaim, Algebraic Hessenberg Decomposition Method Optimized by Genetic Algorithm for Zero Watermarking Technique, *International Journal of Mathematics and Computer Science, 16, no.4,* (2021), 1497-1514.

[7] N. S. Mohammed, A. M. Abduldaim, Algebraic Decomposition Method Utilized in Optimized Zero Watermarking Technique, *1st. Babylon International Conference on Information Technology and Science*(2021).

[8] Pranab Kumar Dhar, Azizul Hakim Chowdhury, and Takeshi Koshiba, Blind Audio Watermarking Based on Parametric Slant-Hadamard Transform and Hessenberg Decomposition, *Symmetry* 2020*, 12, 333*; doi:10.3390/sym12030333.

[9] N. S. Mohammed, A. M. Abduldaim, Algebraic Decomposition Method for Zero Watermarking Technique in YCbCr Space, *Engineering and Technology Journal,04*,(2022),605-616.

[10] Hussain, R.A., Abdulmunem, M.E., Abdul-Hossen, A.M.J., Propose Image Encryption Watermarking Algorithm Based on Frequency and Geometric Transform, SCCS 2019 - 2019 *2nd Scientific Conference of Computer Sciences,* 2019, pp. 143–147, 8852591.

[11] Abdulrida, R., A-Monem, M.E., Jaber, A.M., Quantum image watermarking based on wavelet and geometric transformation, *Iraqi Journal of Sciencethis link is disabled*, 2020*, 61(1)*, pp. 153–163.

[12] H . B. Abdul Wahab, A. J. Abdul-Hossen, S. A. Kadhom, Encrypted Image Watermark in Audio Files Using Homogenous Deffie-Hellman with Chebyshev Polynomial, *Eng.&Tech. Journal,34*,(2016).

[13] Khudhur, Mokhles Hussein, Waleed, Jumana, Hatem, Hivam, Abduldaim, Areej M., Abdullah, Dhahir Abdulhade, An efficient and fast digital image copy-move forensic technique, *2nd International Conference for Engineering, Technology and Sciences of Al-Kitab, ICETS 2018Pages 78 – 82*, December 2018 Article number 8724611.

[14] R. I. Sabri, A. M. Abduldaim, J. Waleed, Mamdani FIS Combined with LU Decomposition Method and Two-Level LWT for Image Watermarking Technique, *3rd International Conference on Engineering Technology and its Applications*, IICETA-IEEE, (2020), 1217.

[15] Li, X. H. and Fan, H., QR Factorization Based Blind Channel Identification and Equalization with Secondorder Statistics,*IEEE Transaction on Signal Processing, Vol. 48, No. 1, pp. 60-69* .(2000)

[16] Moor, B. D. and Dooren, P. V., Generalizations of the Singular Value and QR Decompositions, *SIAM Journal on Matrix Analysis and Applications, Vol. 13, No. 4,* pp. 993-1014 (1992).

[17] Sivakannan Subramani, L. Omprakash Narayanan, C. Kamalanathan, Sunitha Panda and Bhaskara Sreenivas, Design of robust image watermarking technique based on shearlet transform and QR matrix decomposition, *Journal of Interdisciplinary Mathematics, 23:1*, 163-174,(2020).

[18] Pranab Kumar Dhar, Pulak Hazra, and Tetsuya Shimamura, Blind Color Image Watermarking Using Fan Beam Transform and QR Decomposition, *Symmetry* 2020*, 12, 486*; pp: 1-14.

[19] Abduldaim, A.M., Waleed, J., Abdul-Kareem, A.S., Mohmmedali, M.N., Algebraic Authentication Scheme, (2017) 2017 *2nd Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications,* AIC-MITCSA 2017, art. no. 8722971, pp. 319-324. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8718247

[20] Faraj, A.K., Abduldaim, A.M., Salman, S.A., Al-Saidi, N.M.G., An interactive proof via some generalized reduced rings, (2017) *International Conference on Current Research in Computer Science and Information Technology*, ICCIT 2017, art. no. 7965560, pp. 42-47.

[21] Abduldaim, A.M., α-Skew π-Armendariz ring for improving secure algebraic zero knowledge cryptosystem, *Journal of Theoretical and Applied Information TechnologyVolume 97, Issue 24*, Pages 3682 - 3691December 2019.