Int. J. Nonlinear Anal. Appl. 14 (2023) 1, 2399–2407
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.7294

Zero watermarking technique using LWT

Saja Abdulameer Kahdim, Areej M. Abduldaim*

Mathematics and Computer Applications, Applied Sciences Department, University of Technology, Baghdad 10001, Iraq

(Communicated by Javad Vahidi)

Abstract

It is no secret to anyone the essential steps of mathematics in image processing and especially in image watermarking techniques. Transformations are one of the most important mathematical tools used in image processing. It is possible to reduce the size of the image very efficiently and extract important information from it. On the other hand, transformations enable us to move smoothly from the world of image processing (spacial domain) to the world of mathematics and matrices (frequency domain). In this paper, to build a zero-watermarking algorithm, the integer wavelet transform (IWT), is used alone to show the mathematical effect of the results obtained from the proposed zero-watermarking algorithms. One level of IWT is applied to the concealment image and the watermark is XORed with the features chosen from the crucial information obtained from the LL channel to generate the secret share. The results were very satisfactory and the proposed algorithm proved its resistance to different attacks through the robustness metric NC.

Keywords: image processing, robustness metric NC, watermarking, wavelet transform
2020 MSC: 68U10

1 Introduction

Mathematical transformations have drawn the attention of many researchers and appeared in many of their works in computer science. This is due to the characteristics of these transformations in the ability to extract the important locations within the data to be processed. In particular, signal processing took the largest share using these methods, and more accurately, image processing benefited from the advantages of these transformations in different topics, including watermark techniques. Depending on the procedure used to embed the watermark into the concealment image, these techniques are divided into two. The watermarking technique means that the watermark image will be embedded into the image pixels, changing the original image quality (spatial domain algorithms). While in the zero-watermarking technique, the crucial information is extracted to be used in the embedding steps keeping the original quality of the image (transform domain algorithms). currently, the research on robust watermarking mainly focuses on the transform domain. In general, the main aim of improving watermarking techniques is to improve the robustness of the watermarking algorithm by selecting the appropriate embedding positions. The famous transformations frequently used are the DCT (discrete cosine transform) [19], DFT (discrete Fourier transform) [7], and DWT (discrete wavelet transform) [3, 16].

Of course, there are endless possibilities to use various transformations with many mathematical tools such as algebraic transformations (algebraic decomposition methods), optimization algorithms, and others [4, 9]. The Discrete

*Corresponding author
Email addresses: as.20.26@grad.uotechnology.edu.iq (Saja Abdulameer Kahdim), areej.m.abduldaim@uotechnology.edu.iq (Areej M. Abduldaim)

Received: September 2022 *Accepted:* January 2023

Wavelet Transforms (DWT) and the Lift Wavelet Transforms (LWT) have been widely used in both watermarking and zero watermarking techniques, in addition to the Discrete Cosine Transform (DCT), to improve the quality of the results regarding the security and the invisibility of the hidden watermark. Alzahrani in [5] enhanced the invisibility and the robustness of digital image watermarking based on DWT-SVD while in [6] improved upon the SVD-based color image watermarking by incorporating integer wavelet transform (IWT) and chaotic maps. In [11, 2], the authors used first the SVD with a genetic algorithm (GA) without using any other popular transform and later designed an optimized image watermarking technique depending on the Generalized Singular Value Decomposition (GSVD) method and Binary Gravitational Search Algorithm (BGSA). In addition, the Heisenberg Decomposition (Hess) started being used recently as an algebraic transform. For watermarking technique, Pan et al.in [14] used both previous algebraic methods to propose a double-matrix decomposition image steganography scheme with multi-region coverage, to solve the problem of poor extraction ability of steganographic images under attack or interference. Or, with optimization algorithms like Nazir et al.in [13]. Zero watermarking techniques are also effective for medical images using double-tree complex wavelet transformed multi-level discrete cosine transform (MDCT) [8]. The Hess decomposition method is often optimized without any transformation in the YCbCr space for more robustness and security as in [12]. Or, without optimization in the same space [4].

In the same mathematical framework, the Principal Component Analysis (PCA) is a statistical transform for analyzing large datasets containing a high number of features and is not commonly used in the watermarking technique, especially in zero watermarking. Video and image watermarking techniques have been studied by several authors such as Anjaneyulu in [13] that used hybrid DWT-PCA to protect the copyright of images with the Ant Colony Optimization Technique. Also, PCA is used to identify the appropriate bands that can be used for embedding the watermark to design a blind and reversible watermarking technique [8]. While in 2022 for COVID-19, PCA is computed between cover and mark image to develop SecDH as a medical data hiding scheme, which can guarantee the security and copyright protection of the COVID-19 images [12]. The only zero watermarking technique is found in [10] that utilized PCA with DWT to build a robust image zero-watermarking algorithm.

On the other hand, there are many ideas were put forward and various other algebraic transformations were used. In [1] authors developed a watermarking technique combining the QR algebraic decomposition method and new discrete wavelets derived from Hermite polynomials for obtained Discrete Hermite Wavelet Transformation (DHWT). The algebraic matrix decomposition method LU in [15] is employed successfully with Mamdani fuzzy inference system (FIS) on the original image to take out a controller factor for a trade-off between imperceptibility and robustness. In 2021 based on the bidimensional empirical mode decomposition (BEMD)- Schur decomposition and color visual cryptography Wu et al. [17] proposed a color zero-watermarking algorithm for medical images to effectively solve the poor robustness problem of traditional zero-watermarking under large-scale attacks.

In this work, the IWT is adopted without any other mathematical tool for the first time in the zero-watermarking scheme. This is to accentuate the mathematical power in image processing, particularly in zero watermarking schemes.

The organization of this paper is the following. In section 2 the background about the Integer wavelet transform (IWT) is recalled. The suggested zero watermarking techniques as embedding and restoring steps are given in section 3. The results of the experiments and the measurement values of the robustness and imperceptibility are calculated to judge the proposed technique and are illustrated in section 4. Section 5 gives a comparison between the proposed technique and another used IWT. Finally, the conclusion is given in section 6.

2 Integer wavelet transform (IWT)

IWT (integer wavelet transform) can be attributed to a special implementation of DWT (discrete wavelet transform). It is generally believed that the digital signal with integer amplitude can also get integer transform result after wavelet transform. At present, most of the watermarking algorithms are based on the traditional wavelet transform, which has the disadvantages of high complexity and error caused by foating-point rounding. Because the image watermark contains a lot of information, and its pixel values are integers, integer wavelet transform can directly transform the pixel values into integers, so there is no rounding error and can complete many watermarking algorithms. Integer wavelet transform consists of the following three steps [18].

1. Split step: The split step is also called the lazy wavelet transform. The operation just splits the input signal z(η) into odd and even samples: $Z_e(\eta)$ and $Z(\eta)$.

$$Z_e\left(\eta\right) = z\left(2\eta\right), \quad Z_\circ\left(\eta\right) = \ z\left(2\eta+1\right) \tag{2.1}$$

2. Prediction step: Keep even samples changeless, and use $Z_e(\eta)$ predicts $Z(\eta)$. The difference between the prediction value of $P[Z_e(\eta)]$ and the real value of $Z_\circ(\eta)$is defined as detail signal $d(\eta)$.

$$d(\eta) = Z_\circ(\eta) - P[Z_e(\eta)] \tag{2.2}$$

where P [•] is the predict operator. The detail signal $d(\eta)$ denotes the high-frequency component of the original signal $z(\eta)$.

3. Update step: Introduce the update operator U [•], and use detail signal $d(\eta)$ to update even samples $Z_e(\eta)$. Then the approximate signal $c(\eta)$ denotes the low-frequency component of the original signal.

$$c(\eta) = zZ_e(\eta) + U[d(\eta)] \tag{2.3}$$

3 The Proposed Zero Watermarking Technique Based on IWT

In this section, all images used are of size 512 × 512. The concealment images and the watermark are converted from RGB space to grayscale space, applied IWT and choose LL to divided into 4 × 4 non-overlapping blocks to get the important information of the concealment images and then generate the features matrix bits.

3.1 Features Extraction and Embedding Process

The IWT is applied to host image and choose LL to divided in to 4 × 4 blocks to obtain the important information of the concealment images and then generate the features matrix bits and then the secret share. details are explained in Figure 1, the following are the steps of the embedding process:

Step 1: Input the concealment image of size $n \times n$ $\;(in\ our\ case\ 512 \times 512)$and switch to grayscale.

Step 2: Apply IWT on the original image to obtain the four bands {LL, LH, HL, HH}.

Step 3: Choose and split the LL band into 4 × 4 nonoverlapping k blocks F_k.

Step 4: Generate a binary matrix H according to the following:

$$\begin{aligned}
&\mathrm{avr}_k = \sum_{j=1}^{4} F_k(1,\ j)/k \qquad \text{where } k \text{ is the number of blocks}\\
&H(i,j) = 1 \quad if \ \ \mathrm{avr}_k \geq F_k(1,1)\\
&H(i,j) = 0 \qquad \text{otherwise}
\end{aligned}$$

where $1 \leq i \leq 64$ and $1 \leq j \leq 64$

Step 5: Insert and switch the watermark image W to binary to obtain the matrix BW.

Step 6: XORing H and BW matrices to generate the secret share K.

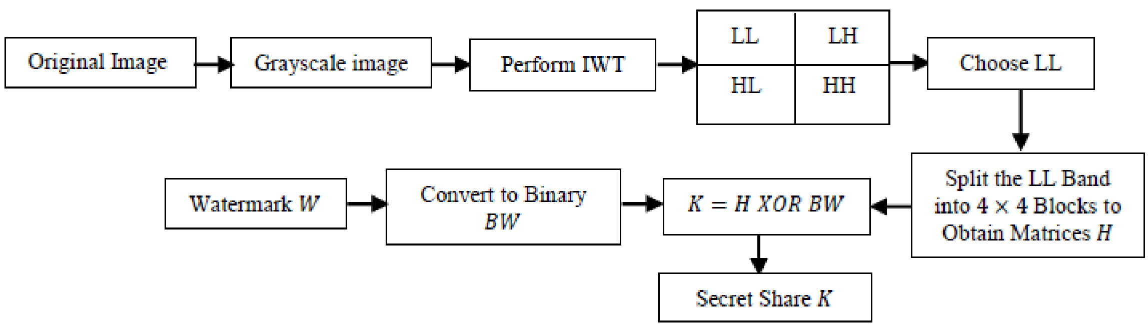


Figure 1: The diagram of the embedding procedure using IWT

3.2 Restoring Process

The restoration of the included watermark is illustrated in Figure 2. The exhaustive steps are given as follows:

Step 1: Input the concealment image of size $n \times n$ $(in\ our\ case\ 512 \times 512)$and switch to grayscale.

Step 2: Apply IWT on the original image to obtain the four bands {LL, LH, HL, HH}.

Step 3: Choose and split the LL band into 4×4 nonoverlapping k blocks F_k

Step 4: Generate a binary matrix H according to the following:

$$\begin{aligned}
&\text{avr}_k = \sum_{j=1}^{4} F_k(1,\ j)/k \qquad \text{where } k \text{ is the number of blocks}\\
&H\,(i,j) = 1 \quad if \ \ \text{avr}_k \geq F_k\,(1,1)\\
&H\,(i,j) = 0 \qquad\quad \text{otherwise}
\end{aligned}$$

where $1 \leq i \leq 64$ and $1 \leq j \leq 64$

Step 5: Input the secret share K and apply XOR logical operation between H and K to get the watermark.

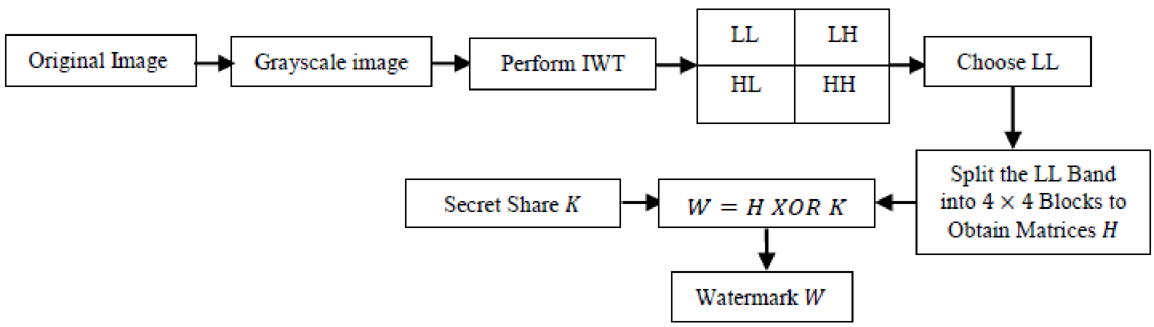


Figure 2: The diagram of the Extraction procedure using IWT

4 The Experiential Results of the Proposed Technique

In this section, the results before and after putting images under attacks are given and explained in three cases: the thoroughness of the suggested technique, the impact and the importance of IWT, and the results of performing the IWT after attacks.

4.1 The Thoroughness of the Suggested Technique

Some experiments are performed, before exposing the images to any attack, to measure the robustness and imperceptibility of the suggested technique.

Figure 3: The Concealment Images and the Watermark Used in this Work

The proposed zero watermarking scheme is examined on four grayscale images of size 512×512. A binary image of size 512×512 is used as the watermark image. Figure 3 shows the concealment images and the watermark used in this work. From a mathematical point of view, to check the proposed technique and to locate whether the final results are reasonable or not the NC measurement is used (the realistic value of NC=1). Before attacking the concealment images, the NC=1 after performing the proposed techniques. See Table 1.

Table 1: NC Values with No Attacks

Images	**Lena**	**Girl**	**Baboon**	**Peppers**
NC	1	1	1	1

4.2 The Impact and the Importance of IWT

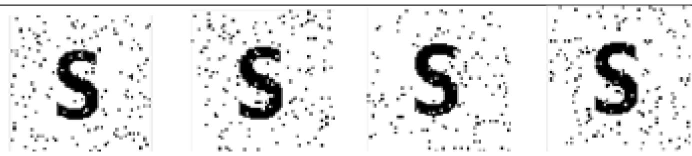
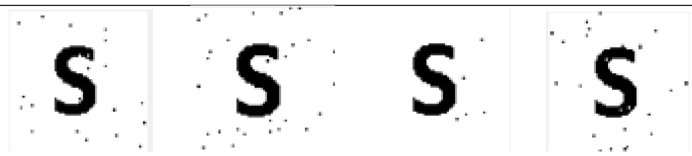
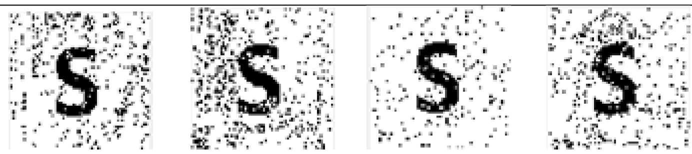
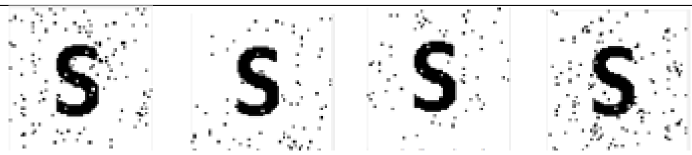
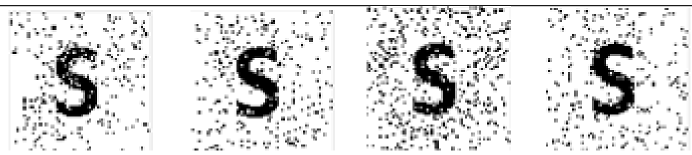
The main aim is to elicit the feature matrix using the IWT to hide the binary watermark such that the same included watermark is obtained exactly after the restoring process. The proposed embedding technique used the IWT only on the concealment image, choosing and dividing the LL channel into 4×4 nonoverlapping blocks. To generate a binary feature matrix from the important information obtained, the average of the first row of each block is evaluated to be the threshold. Consequently, it is virtual that the embedded watermark can be extracted exactly the same as the original watermark image depending on the strength and stability properties of the LL band. Furthermore, the process of restoring the watermark from the concealment images that were attacked gave good and passable results.

4.3 The Results of Performing IWT after Attacks

Testing the imperceptibility and robustness of the proposed scheme shows that the results of the values of NC and PSNR after restoring the watermark from the attacked images are acceptable and reasonable, Table 2. While Figure 4 gives the restored watermark image after the concealment images are attacked.

Table 2: PSNR and NC values after Attacks

Attacks	**Lena Image**		**Girl Image**		**Mandrill Image**		**Peppers Image**	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Salt pepper noise	26.949	0.976	25.938	0.976	27.087	0.980	26.918	0.977
JPEG Compression	61.305	0.997	61.287	0.996	60.684	0.999	60.933	0.996
Gaussian noise	37.658	0.942	37.689	0.926	37.668	0.973	37.670	0.945
Histequalization	18.985	0.980	10.096	0.989	16.369	0.990	20.56	0.979
Gaussianlowpassfilter	34.068	0.959	38.137	0.960	31.327	0.932	34.277	0.962
Poisson noise	27.199	0.874	30.476	0.876	26.982	0.921	27.336	0.874
Speckle noise	35.651	0.932	41.070	0.958	35.515	0.967	35.728	0.940
Motion filter	26.036	0.874	28.352	0.861	23.921	0.817	25.502	0.878
Average filter	34.068	0.959	38.137	0.960	31.327	0.932	34.277	0.962
Med filter	31.721	0.956	35.401	0.955	30.439	0.929	31.512	0.960

W	Lenna	Girl	Mandrill	Peppers
				
Salt Pepper				
EW				
JPEG Compression				
EW				
Gaussian Noise				
EW				
Histogram equalization				
EW				
Gaussianlowpassfilter				
EW				

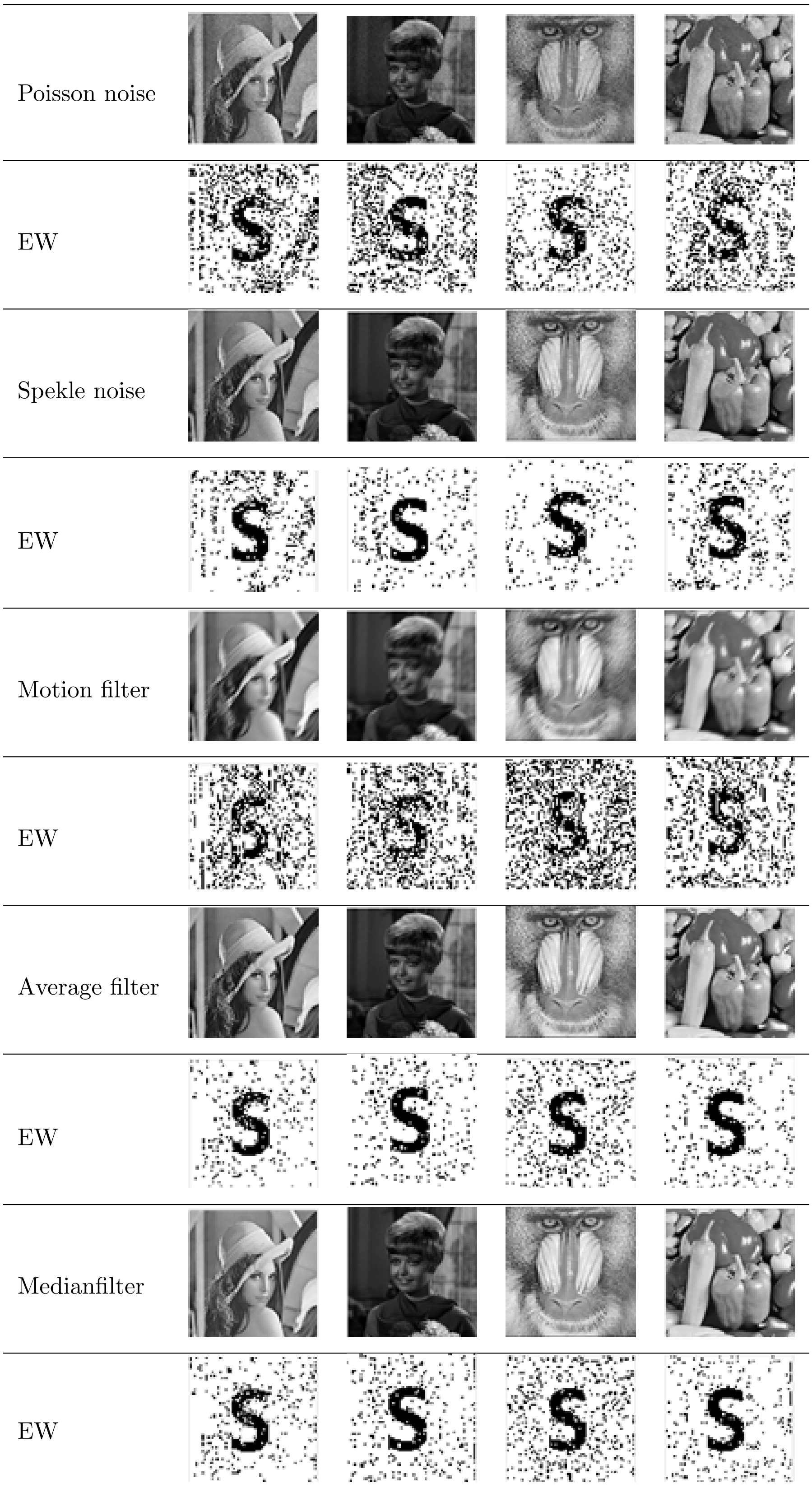


Figure 4: The Extraction of the Zero Watermarking Algorithmwith Using IWT after Attacks

5 Comparison

In this work, the IWT has been applied to transform the concealment images into a frequency domain to create the master secret. The results are more than acceptable depending on the values obtained. The algorithm given in [18] used the SVD and genetic algorithm in addition to IWT. Table 3 explained the differences:

Table 3: Comparison Between the Proposed Technique and [18] Technique under NC Metric

Attacks	**Lena Image**	
	The proposed Technique Based on IWT Only	[18] Technique IWT+SVD+Genetic Algorithm
Gaussian low pass filter	0.959	0.987
JPEG compression	0.997	0.998
Gaussian noise	0.942	0.999

6 Conclusion

An effective technique of zero watermarking is proposed in this paper. The integer wavelet transform (IWT) is adopted that has not been used in zero watermarking techniques before without auxiliary tools. The proposed technique relied on IWT to extract the features matrix from the original color images (with size 512×512) for creating the master secret, which is being kept by the third party, in order to protect the rights of property from tampering. The IWT utilization was effective and the significance and strength of the results were so close (if not better) to the optimal results achieved from using several tools in addition to IWT that extract the image features optimally. The proposed technique gave good flexibility against different types of common attacks.

References

[1] A.M. Abduldaim, A.A. Abdulrahman and F.S. Tahir, *The effectiveness of discrete Hermite wavelet filters technique in digital image watermarking*, Indones. J. Electric. Engin. Comput. Sci. **25** (2022), no. 3, 1392–1399.

[2] A.M. Abduldaim and A.K. Faraj, *Combining algebraic GSVD and gravitational search algorithm for optimizing secret image watermark sharing technique*, Int. J. Math. Comput. Sci. **17** (2022), no. 2, 753–774.

[3] A.K. Abdulrahman and S. Ozturk, *A novel hybrid DCT and DWT based robust watermarking algorithm for color images*, Multimed. Tools Appl. **78** (2018), 17027–17049.

[4] H.B. Abdul Wahab, A.J. Abdul-Hossen and S.A. Kadhom, *Encrypted image watermark in audio files using homogenous Deffie-Hellman with Chebyshev polynomial*, Eng. Tech. J. **34** (2016).

[5] W. H. Alshoura, Z. Zainol and J. M.Alawida, *An FPP-resistant SVD based image watermarking scheme based on chaotic control*, Alexandria Engin. J. **61** (2022).

[6] A. Alzahrani, *Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD*, Appl. Bionics Biomech. **2022** (2022).

[7] M. Hamidi, M. El Haziti, H. Cherifi and M. El Hassouni, *Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimed*, Tools Appl. **77** (2018), 27181–27241.

[8] T. Huang, Jia Xu, Y.Yang and B.Han, *Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and Hessenberg decomposition*, Math. **10** (2022), 1154.

[9] L.F. Jalil and M.M. Laftah, *Text Hiding in 3D Object*, Eng. Tech. J. **34** (2016).

[10] X. Leng, J.Xiao and Y. Wang, *A robust image zero-watermarking algorithm based on DWT and PCA*, Commun. Comput. Inf. Sci., 2012, pp. 484–492.

[11] N.S. Mohammed and A.M. Abduldaim, *Algebraic decomposition method utilized in optimized zero watermarking technique*, 1st Babylon Int. Conf. Inf. Technol. Sci., 2021.

[12] N.S. Mohammed and A.M. Abduldaim, *Algebraic Hessenberg decomposition method optimized by genetic algorithm for zero watermarking technique*, Int. J. Math. Comput. Sci. **16** (2021), no. 4, 1497–1514.

[13] H. Nazir, I.S. Bajwa, M. Samiullah, W. Anwar and M.Moosa, *Robust secure color image watermarking using 4D hyperchaotic system, DWT, HbD, and SVD based on improved FOA algorithm*, Secur. Commun. Networks **2021** (2021),

[14] P. Pan, Z. Wu, C. Yang and B.Zhao, *Double-matrix decomposition image steganography scheme based on wavelet transform with multiregion coverage*, Entropy **24** (2022), no. 246, 1–21.

[15] R.I. Sabri, A.M. Abduldaim and J. Waleed, *Mamdani FIS combined with LU decomposition method and two-level LWT for image watermarking technique*, 3rd Int. Conf. Engin. Technol. Appl., IICETA-IEEE, 2020, pp. 1217.

[16] B.W. Wang and P. Zhao, *An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain*, Math. **8** (2020), no. 8, 691.

[17] D Wu, M Wang, J Zhao, J Wang, M Zhong, H. Zheng, S. Hu, Y. Tang and C. Qu, *Color zero-watermarking algorithm for medical imagesBased on BEMD-Schur decomposition and color visual cryptography*, Secur. Commun. Networks **2021** (2021).

[18] T. Zhu, W. Qu and W. Cao, *An optimized image watermarking algorithm based on SVD and IWT*, J. Supercomput. **78** (2022), 222–237 .

[19] Q. Zhang, Y. Li and X. Wei, *An improved robust and adaptive watermarking algorithm based on DC*T. J. Appl. Res. Technol. **10** (2012), 405–415.