International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 333–343
DOI: https://doi.org/10.69793/ijmcs/01.2025/mutlk

Employing Algebraic Eigenvalue Decomposition in Zero Watermarking Technology

Ahmed Fadil Mutlk[1], **Areej M. Abdmldaim**[1], **Matheel E. Abdulmunim**[2]

[1]Mathematics and Computer Applications
Applied Science Department
University of Technology
Baghdad, Iraq

[2]Department of Computer Sciences
University of Technology
Baghdad, Iraq

email: as.22.20@grad.uotechnology.edu.iq

(Received October 1, 2024, Accepted November 6, 2024,
Published November 13, 2024)

Abstract

The new watermarking technology is highly sophisticated, utilizing advanced algorithms to ensure robust protection and seamless integration with digital content while maintaining the highest levels of security against potential attacks. The primary goal of this paper is to enhance the zero watermarking technology by leveraging the eigenvalue decomposition (EVD) method as an algebraic transformation, without relying on other common transforms. The image matrix is divided into 4×4 blocks, and EVD is applied to each block to extract feature matrix bits, forming the final zero-secret. The robustness of the proposed algorithm is evaluated, showing robust resilience to conventional attacks like noise, filtering, JPEG compression, and cropping, as indicated by the normalized correlation (NC) values.

Key words and phrases: Eigenvalue Decomposition, Watermarking Mechanism, Matrix Decomposition, Embedding Phase, Extraction Phase.
AMS (MOS) Subject Classifications: 15A18, 05C50, 65F50.
ISSN 1814-0432, 2025, https://future-in-tech.net

1 Introduction

In our new world, the need for technology in all its forms, aspects and uses is rapidly increasing. Electronic devices have become indispensable in all areas of our lives. These devices generally work with multiple communication media like text, image, audio, video, and animation [1]. The development of computer technology is significantly linked to mathematics and, in particular, image processing and its direct connection to linear algebra are mentioned, as each image is represented by a matrix to which all the manipulations applied to the matrix apply [2]. This close relationship between the sciences has led to a large and rapid development in the field of security which has received the attention of a significant number of researchers in this field [3], [4],[5]. Recently, interest has grown in using watermarks to safeguard property rights against tampering. New mathematical approaches, particularly using linear algebra, have emerged that integrate the watermark image into matrix features extracted from the original image [6], [7]. The stability of the results from these methods is largely due to their reliance on the extraction of eigenvalues and eigenvectors which inherently enhances their robustness [8]. Depending on how the watermark is embedded into the image, these techniques are categorized into two types. In traditional watermarking, a watermark (such as a logo, text, or pattern) is directly embedded into the original digital content (image, video, etc.) [9]. This modifies the content slightly but the watermark can be detected or extracted later to verify authenticity. Zero watermarking, on the other hand, doesn't modify the original content. Instead, it extracts unique features from the content, combines them with a watermark, and registers this combination separately. The original content remains unaltered and the watermark is verified by comparing the registered information with the content's features during the authentication process [10].

In the literature, eigenvalue decomposition is extremely rare in watermarking, especially in zero watermarking, if not nearly nonexistent. Referring to traditional watermarking techniques, many employ algebraic decomposition methods, either with or without standard transformations [11], [12], [13]. Matrix decompositions play an important role in most of watermarking techniques. Especially Singular Value Decomposition (SVD) is one of the most preferred techniques [14], [15], [16]. In addition, matrix decompositions such as ULV, QR, LU are some of the methods used in previous studies [17], [18], [19]. The feature value of each sub-block are extracted by schur decomposition [20] to effectively solve the poor robustness problem of traditional

zero-watermarking under large-scale attacks based on bidimensional empirical mode decomposition (BEMD) and color visual cryptography [21], [22].
In this study, a novel watermarking mechanism is introduced using an alternative matrix decomposition method. The use of Eigenvalue Decomposition, proposed here as an alternative to the decomposition techniques employed in numerous studies [23], [24], represents the original contribution of this research.
In the rest of this paper, the proposed zero watermarking mechanism using the eigenvalue decomposition (EVD): the watermark embedding and the watermark extraction are described in Section 2. In Section 3, the experiments and performance analysis are explained. In Section 4, the three cases proposed in this study are compared with each other on the one hand and with some sources on the other hand. Finally, the conclusions are presented in Section 5.

2 The Proposed Eigenvalue Zero Watermarking Mechanism

Eigenvalue decomposition is the factorization of a matrix into a canonical form, whereby the matrix is represented in terms of its eigenvalues and eigenvectors. The obtained eigenvalues are not unique where EDV is unique if all eigenvalues are unique. Eigenvalue decomposition of a matrix A is represented as:

$$A = VDV^{-1},$$

where A is the square matrix to be decomposed, V is the matrix of eigenvectors, D is the diagonal matrix of eigenvalues, V^{-1} is the inverse of eigenvectors [25].
Eigenvalue decomposition provides an effective method to embed and extract watermarks in host images through image analysis and extraction of pertinent details, followed by the addition of watermarks in a manner that preserves image quality and renders them resistant to tampering or watermark removal. The reason for relying on EVD is to explore the advantages and disadvantages of this decomposition method. This means that the EVD is used to extract the essential information of the image matrix depending on the eigenvalues obtained by this algebraic method.

2.1 The Process of Extracting Features and Watermark Embedding

The algorithm of embedding the watermark into the cover image based on eigenvalue decomposition is given as follows and illustrated in Figure 1.
Step 1: Input the original image of size 256×256 and the watermark of size 256×256,128×128,64×64 and convert all images into a grayscale case.
Step 2: Input the watermark and convert $W_{(i,j)}$ to the binary matrix.
Step 3: Divide the image into 64×64 blocks each block is of size 4×4.
Step 4: Apply the eigenvalue decomposition method on each block in Step 3 to get 3 matrices per block $(V_{(i,j)}, D_{(i,j)}, V^{-1}_{(i,j)})$, where $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
Step 5: Three cases are tested for all blocks to create a new matrix to be the matrix of features:
`Case 1`: Choose the matrix $D_{(i,j)}$ to form a new matrix (feature matrix) U of size 256×256.
`Case 2`: Choose the main diagonal of each $D_{(i,j)}$ to form a new matrix (feature matrix) U of size 128×128.
`Case 3`: Choose the maximum number of each $D_{(i,j)}$ to form a new matrix (feature matrix) U of size 64×64.
Step 6: Convert the U to binary matrix K where $1 \leq i \leq n$ and $1 \leq j \leq n$.
where: case1: $n = 256$ case1: $n = 128$ case1: $n = 64$.
step 7: Perform XOR operation between watermark W and K to obtain the three secret shares SS_1, SS_2, and SS_3.
end

2.2 The Process of Watermark Extracting

Step 1: Input the original image of size 256×256 and convert them into a grayscale case.
Step 2: Input the three secret shares SS_1, SS2, and SS3.
Step 3: Divide the image into 64×64 blocks each block is of size 4 ×4.
Step 4: Apply the eigenvalue decomposition method in Step 3, on each block to get 3 matrices $(V_{(i,j)}, D_{(i,j)}, V^{-1}_{(i,j)},)$ where $1 \leq i \leq 64$ and $1 \leq j \leq 64$.
Step 5 : Three cases are tested for all blocks to create a new matrix to be the matrix of features:
`Case 1`: Choose the matrix $D_{(i,j)}$ to form a new matrix (feature matrix) U of size 256×256.
`Case 2`: Choose the main diagonal of each $D_{(i,j)}$ to form a new matrix (fea-

ture matrix) U of size 128×128.
`Case 3`: Choose the maximum number of each $D_{(i,j)}$ to form a new matrix (feature matrix) U of size 64×64.
Step 6: Convert the U to binary matrix K, where $1 \leq i \leq n$ and $1 \leq j \leq n$.
where: case1: $n = 256$ case1: $n = 128$ case1: $n = 64$.
Step 7: Apply XOR operation between the binary features K and the secret shares SS_1, SS_2, and SS_3 to get the embedding Watermark.
end

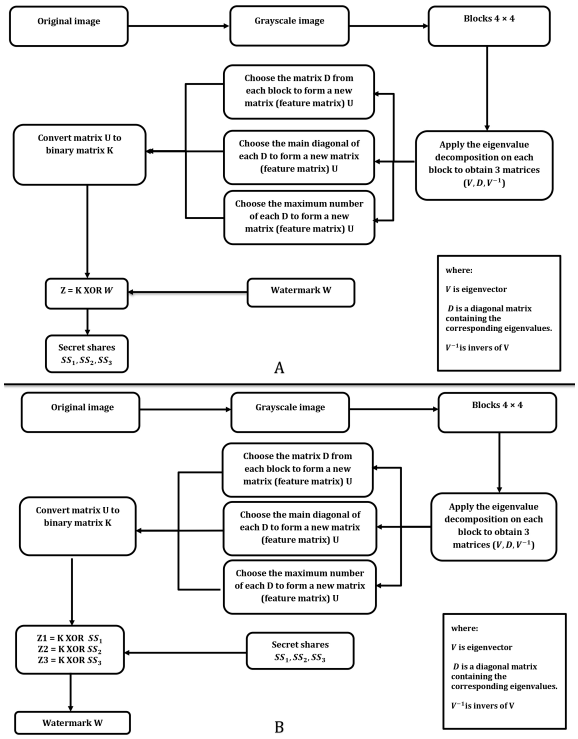


Figure 1: (A) The diagram of the Embedding procedure using EVD,(B) The diagram of the Extraction procedure using EVD

3 Results and Analysis of the Proposed Scheme

In this section, we analyze the results of the proposed scheme to assess its robustness. Four standard test images are adopted to evaluate the approach's effectiveness as one can see in Figure 2.

Figure 2: The Images Used in the Work.

The primary objective is to extract the feature matrix through the algebraic method of EVD to embed the binary watermark so that the watermark can be recovered exactly during the restoration process. The proposed embedding technique applies EVD exclusively, without any public transformation, to each block after dividing the concealment image into 4x4 non-overlapping blocks. Each block is decomposed into high-frequency components (the significant information of the image), represented by the diagonal matrices $D_{(i,j)}$, which contain the eigenvalues, while the low-frequency components (the less critical information) are captured by the matrices V and V^{-1}. This algebraic decomposition method functions similarly to a transformation, as both separate the image into high- and low-frequency components. As a result, before any attacks, the embedded watermark can be precisely recovered as the original due to the robustness of the eigenvalues. Furthermore, the watermark extraction from the concealment images subjected to attacks yielded satisfactory results.

To check the proposed technique and to locate whether the final results are reasonable or not, the NC measurement is used before attacking the concealment images and after performing the proposed techniques.

Table 1: The NC Values without Attacks

images	Lenna	Girl	Mandrill	Peppers
NC	1	1	1	1

In this section, the results of the proposed scheme based on eigenvalue decomposition are obtained under large-scale attacks: Geometric attacks, Noise attacks, Filter attacks, and Image enhancement and explained in details to show and test the robustness and imperceptibility of the zero watermarking technique without using any transform, Figure 3.

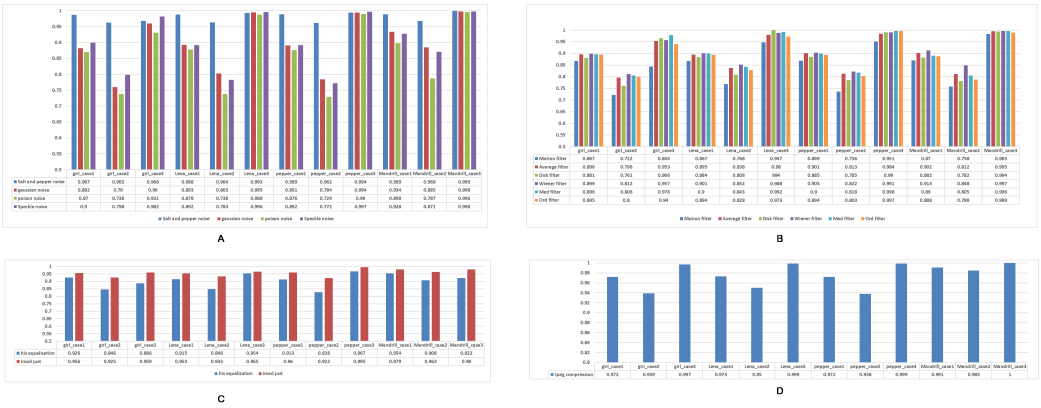
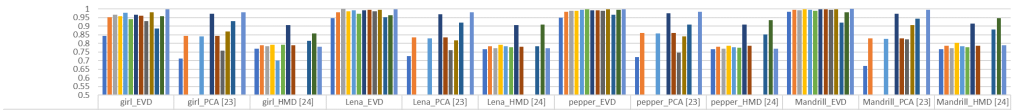


Figure 3: (A) NC values after using noise Attacks,(B) NC values after using filter Attacks,(C) NC values after using enhancement Attacks,(D) NC values after using Geometric Attacks

4 Comparison

Until now, no existing zero watermarking technologies have used the algebraic eigenvalue decomposition method. For this reason, the comparison was made between the three proposed cases between themselves on the one hand and between the results of the proposed scheme and other existing works on the other hand [23] and [24].



	girl_EVD	girl_PCA [23]	girl_HMD [24]	Lena_EVD	Lena_PCA [23]	Lena_HMD [24]	pepper_EVD	pepper_PCA [23]	pepper_HMD [24]	Mandrill_EVD	Mandrill_PCA [23]	Mandrill_HMD [24]
Motion filter	0.844	0.713	0.77	0.947	0.726	0.767	0.951	0.722	0.767	0.983	0.669	0.766
Average filter	0.953	0.845	0.789	0.98	0.834	0.784	0.984	0.862	0.78	0.995	0.829	0.786
Disk filter	0.966	_	0.785	984	–	0.773	0.99	–	0.769	0.994	_	0.773
Wiener filter	0.957	_	0.791	0.988	–	0.792	0.991	_	0.786	0.997	–	0.804
Med filter	0.978	0.842	0.7	0.992	0.829	0.783	0.996	0.857	0.779	0.996	0.828	0.784
Ord filter	0.94	–	0.791	0.973	–	0.778	0.997	–	0.776	0.989	–	0.777
Salt and pepper noise	0.968	0.972	0.907	0.993	0.97	0.908	0.994	0.976	0.909	0.999	0.972	0.914
Gaussian noise	0.96	0.845	0.789	0.995	0.834	0.782	0.994	0.862	0.786	0.998	0.829	0.786
Poisson noise	0.931	0.758	–	0.988	0.762	–	0.99	0.746	–	0.996	0.824	–
Speckle noise	0.982	0.87	–	0.996	0.819	–	0.997	0.842	_	0.998	0.907	–
His equalization	0.886	0.93	0.816	0.954	0.92	0.784	0.967	0.911	0.853	0.922	0.945	0.881
Imad just	0.959	–	0.857	0.965	–	0.91	0.995	–	0.936	0.98	_	0.946
JPEG compression	0.997	0.981	0.781	0.999	0.981	0.773	0.999	0.984	0.769	1	0.995	0.789

Figure 4: The Comparison NC Between the Proposed Technique Zero watermarking with [23], [24]

5 Conclusions

In this paper, we presented an effective zero-watermarking technique using eigenvalue decomposition (EVD), a method not previously applied to image zero-watermarking technologies, even with popular transforms. The proposed approach directly utilizes EVD without any additional transformation to extract the feature matrix from the original images. Three cases were adopted depending on the way of choosing elements of the feature matrix, yielding satisfactory results based on NC values. After various attacks, NC values in case 3 were superior to those in cases 1 and 2. This improvement was attributed to selecting the highest diagonal value from each block after applying EVD. The best NC value was 1 in case 3 achieved with the Jpeg compression attack on the Mandrill image, while the lowest NC value was 0.722 in case 2 occurred with Motion filter attack on the girl image. The use of EVD not only enabled us to design an algebraically robust algorithm but also produced results that are as strong and significant as those achieved in the algorithms that use common transforms for image feature extraction.

References

[1] Economic Commission for Latin America and the Caribbean, Digital technologies for a new future (LC/TS.2021/43), Santiago, 2021

[2] Suresh Rasappan, Pugalarasu Rajan, An Overview of Linear Algebra in Image Processing, Southeast Europe Journal of Soft Computing, **12,** no. 2, (2023), 72–77.

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

[4] A.M. Abduldaim, A.M. Ajaj, A new paradigm of the zero-knowledge authentication protocol based-Armendariz rings, Annual Conference on New Trends in Information and Communications Technology Applications, (2017), Article number 7976143, 97–104.

[5] A.M. Abduldaim, α-Skew π-Armendariz ring for improving secure algebraic zero knowledge cryptosystem, Journal of Theoretical and Applied Information Technology, **97,** no. 24, (2019), 3682–3691.

[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] A.M. Abduldaim, J. Waleed, A.N. Mazher, An Efficient Scheme of Digital Image Watermarking Based on Hessenberg Factorization and DWT, Proceedings of the International Conference on Computer Science and Software Engineering, (2020), Article number 9142096, 180–185.

[8] S. Eisenträger et al., An eigenvalue stabilization technique for immersed boundary finite element methods in explicit dynamics, Computers and Mathematics with Applications, **166,** (2024), 129–168.

[9] M. Begum et al., Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness, Algorithms, **17,** (2024), 32.

[10] Quan Wen, Tan-feng Sun, Shu-xun Wang, Concept and Application of Zero-Watermark[J], Acta Electronica Sinica, **31,** no. 2, (2003), 214–216.

[11] Jumana Waleed, Ihab Mahdi Almaameri, A.M. Abduldaim, Waleed Al-Azzawi, Two Stages of Algebraic Matrix Decomposition in Optimal Image Steganographic Approach, 5th International Conference on Engineering Technology and its Applications, (2022), Code 183264, 294–299.

[12] R. Nasser, Y. Abouelseoud, M. Mikhail, Robust watermark based on Schur decomposition and dynamic weighting factors, Vis. Comput., **40,** (2024), 3249–3269.

[13] 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), Code 176707, 52–57.

[14] Ran Chu, Shufang Zhang, Jun Mou, Xinyu Gao, A zero-watermarking for color image based on LWT-SVD and chaotic system, Multimedia Tools and Applications, **82,** (2023), 34565–34588.

[15] A.M. Abduldaim, A.K. Faraj, Combining Algebraic GSVD and Gravitational Search Algorithm for Optimizing Secret Image Watermark Sharing Technique, (2022) International Journal of Mathematics and Computer Science, **17,** no. 2, 753–774.

[16] J. Waleed, A.M. Abduldaim, H.H. Alyas, A.Q. Mohammed, An Optimized Zero-Watermarking Technique Based on SFL Algorithm, 2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering, (2019), Article number 9072723, 171-175.

[17] Fahrettin Horasan, A novel image watermarking scheme using ULV decomposition, Optik, **259,** (2022), 168958.

[18] P.T. Nha, T.M. Thanh, N.T. Phong, Consideration of arobust watermarking algorithm for color image usingimproved QR decomposition, Soft Comput., **26,** (2022), 5069–5093.

[19] 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, (2020), Article number 9318829, 12–17.

[20] Deyang Wu et al., Color Zero-Watermarking Algorithm for Medical Images Basedon BEMD-Schur Decomposition and Color Visual Cryptography, Security and Communication Networks, (2021), Article ID 7081194, 12 pages.

[21] A.M. Abduldaim, J. Waleed, A.S. Abdul-Kareem, M.N. Mohmmedali, Algebraic Authentication Scheme, 2nd Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications,(2017), Article number 8722971, 319–324.

[22] A.K. Faraj, A.M. Abduldaim, S.A. Salman, N.M.G. Al-Saidi, An interactive proof via some generalized reduced rings, International Conference on Current Research in Computer Science and Information Technology, (2017),Article number 7965560, 42–47.

[23] Saja Abdulameer Kahdim, A.M. Abduldaim, Principal Component Analysis for Zero Watermarking Technique, International Journal of Mathematics and Computer Science, **18,** no. 1,(2023), 85–97.

[24] Nada Sabeeh Mohammed, A.M. Abduldaim, Upper Hessenberg Decomposition Matrix Utilized to Build Zero Watermarking Technique in YCbCr Space, AIP Conference Proceedings, 23948, (2022), Article number 070034, 1st Samarra International Conference for Pure and Applied Sciences, Code 184125.

[25] Gene H. Golub,Charles F. Van Loan, Matrix Computations, 3rd ed., Johns Hopkins University Press, Baltimore, 1996, 310.