Fragile watermarking for image authentication using dyadic walsh ordering

Prajanto Wahyu Adi [a,1,*], Adi Wibowo [a,2], Guruh Aryotejo [a,3], Ferda Ernawan [b,4]

[a] Department of Informatics, Universitas Diponegoro, Semarang, Indonesia
[b] Faculty of Computing, Universiti Malaysia Pahang, Pekan, Malaysia
[1] prajanto@live.undip.ac.id ; [2] guruh2000@gmail.com; [3] bowo.adi@live.undip.ac.id; [4] ferda@ump.edu.my
* corresponding author

ARTICLE INFO

Article history
Received August 12, 2022
Revised June 26, 2023
Accepted October 15, 2023
Available online October 16, 2023

Selected paper from The 2022 5th International Symposium on Advanced Intelligent Informatics (SAIN'22), Yogyakarta (Virtually), September 14, 2022, http://sain.ijain.org/2022/. Peer-reviewed by SAIN'22 Scientific Committee and Editorial Team of IJAIN journal.

Keywords
Watermarking
Dyadic Walsh matrix
Active tampering detection
Image authentication

ABSTRACT

A digital image is subjected to the most manipulation. This is driven by the easy manipulating process through image editing software which is growing rapidly. These problems can be solved through the watermarking model as an active authentication system for the image. One of the most popular methods is Singular Value Decomposition (SVD) which has good imperceptibility and detection capabilities. Nevertheless, SVD has high complexity and can only utilize one singular matrix S, and ignore two orthogonal matrices. This paper proposes the use of the Walsh matrix with dyadic ordering to generate a new S matrix without the orthogonal matrices. The experimental results showed that the proposed method was able to reduce computational time by 22% and 13% compared to the SVD-based method and similar methods based on the Hadamard matrix respectively. This research can be used as a reference to speed up the computing time of the watermarking methods without compromising the level of imperceptibility and authentication.

1. Introduction

Manipulation of digital images is becoming more prevalent where such actions can be done quickly and easily through image processing software [1], [2]. The image manipulation technology that is currently developing has a good purpose, which is to improve the quality of an image, but on the other hand, it can also be used for bad purposes such as forgery or image plagiarism [3]. The process of forensic analysis of approximately a hundred thousand images by an expert takes about six to eighteen months and from the process, only less than one percent of the images contain violations [4]. Therefore, there is a need for a method that can help the initial verification process of the allegedly manipulated image quickly and accurately.

The most feasible solution to overcome this problem is through watermarking techniques [5]. There are two types of watermarking, namely robust watermarking which is used for copyright protection, and semi-fragile or fragile watermarking which is used for authentication [6]. In general, authentication methods can be classified into two types, namely passive and active tampering detection [7], [8]. The passive type carries out a detection process without prior information through three schemes, namely: region tampering, multiple compression, and inter-frame forgery [9]. This method is usually used to detect changes in the entire image region through several techniques such as sharpening [10], contrast

enhancement [11], and, JPEG compression [12]. Meanwhile, the active detection process is carried out more simply through embedding using a watermarking method and perceptual image hash [13]. It is generally used to detect the local tampered region of the image [14]. Active detection is capable of detecting multiple tampering points on an image [15] and has a high level of tampering tolerance [16], thus making it suitable for use in most cases of image manipulation.

Research on active tampering detection that is developing today focuses on the accuracy of location detection, preservation of image quality, and time efficiency [17]. The research conducted by [18] performed an analysis of artifacts on image datasets to improve detection results. A new embedding method was developed by [19] through Gauss-Jordan elimination to improve image quality and recovery results hence it can achieve an average value of PSNR above 44dB. Similar research was also conducted by [20] by combining the Remainder Value Differencing (RVD) and Merkle Tree methods. The focus of the study is an improvement through a correction logic to obtain the true value of pixels with an embedding and extraction time of 4.7 seconds. It can produce high imperceptibility and recovery ability with PSNR and SSIM values above 41dB and 0.96 respectively.

In the last decade, the Singular Value Decomposition (SVD) method has become very popularly used for image authentication. In the study [17] the feature of SVD was calculated with Euclidean distances to detect duplication forgery on sequential frames with a precision of 0.98. The combination of SVD and Polar Complex Exponential Transform (PCET) in the study [21] results in a feature extraction time of 4.15 seconds and a precision of higher than 0.93. SVD is also widely used in tampering and recovery detection such as research conducted by [22] utilizing Permutation Ordered of Binary (POB) before watermark detection via SVD. The experiment on an image shows that the quality of the recovered image has a PSNR value of 42.74dB at a tampering rate of 10%. Other research that focuses more on tampering detection carried out by [23] using SVD singular values from random blocks can detect tampering locations and keep imperceptibility values above 51dB.

The SVD-based active detection method does produce good image quality, but this method has a high level of complexity so it requires a long computational time [24]. This is due to the SVD decomposition process which results in one singular matrix S and two orthogonal matrices U and V on each block, where only the S is used and ignores the other two variables [25]. The main problem of implementing an image authentication system through watermarking is the high level of complexity of popular algorithms such as SVD. This is the motivation of this study to reduce the level of complexity without reducing the level of reliability. This study proposes the use of a single matrix operation that is close to S so that it can overcome redundant variables in the SVD method. The matrix was formed from a Hadamard and then ordered dyadically to produce a Walsh matrix that had a small degree of sign changes. The use of Walsh-based transformations also has fast computing time [26], requires little space, and can be applied to cryptographic-based security models [27] such as combined with message digest algorithm [28] so that it can replace image scrambling algorithm. The matrix generation process will also be carried out once at the beginning of the process to reduce computational time. This research proposes a model that can be used as a reference to reduce the complexity of popular SVD-based algorithms through the generation of signed integers matrices such as the Hadamard and Walsh matrix which have similar properties to SVD. The use of these matrices has proven to be able to speed up the computational process without reducing imperceptibility and authentication capabilities.

The further sections are organized as follows: Chapter 2 will explain the process of generating the Walsh matrix with Dyadic ordering, prove the orthogonality of the matrix, and the explanation of the proposed model. Chapter 3 presents the dataset used as well as a discussion of the results of experiments and comparisons of SVD and Hadamard-based methods on two computing devices. The conclusions gleaned from this study are discussed in Chapter 4.

2. Method

2.1. Dyadic Ordered Walsh Matrix

Walsh matrix is a matrix generated from the Hadamard matrix through Paley construction [29] nor dyadic ordering with dimensions of 2 power of n which contains the values 1 and -1. It can also be orthogonal where the multiplication of its transposed matrix will result in an identity matrix if the diagonal element is divided by its dimensions as shown in (1). Where H is a Hadamard matrix of dimension n. In this study, dimension 4 was used which is the tensor product of the smallest Hadamard matrix with the dimension of two in (2).

$$\frac{H_n * H_n^T}{n} = I \tag{1}$$

$$H_4 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2}$$

The main problem in the Hadamard matrix is in the order of sign changes which have a large number of bit changes. The Hadamard matrix needs to be rearranged to reduce the number of signed changes on the successive row which is known as Reflected Binary Code or Gray Code [30], [31]. Table 1 shows that in sequence ordering there is a change in 2 binary values between decimal values of 1 and 2 where the binary value changes entirely from '01' to '10'. In the Hadamard matrix which has natural ordering, the change in entire binary values occurs twice, namely at the value of 0 to the value of 3 and the value of 1 to the value of 2. From these sequences, it can be seen that the value changes from a decimal value of 1 to 2, and the decimal value of 0 to 3 should be avoided. Therefore, this paper uses dyadic ordering which has binary changes of 1 bit in the successive rows. In addition, this rearrangement is also used to scramble the row sequence of the Hadamard [32] block so that the process of inserting bits can be carried out without a scrambling algorithm such as Arnold Transform [23].

Table 1. Comparison of Binary Changes of Matrices Ordering

Sequence Walsh			Natural Walsh (Hadamard)			Dyadic Walsh		
Decimal	*Binary*	*Changes*	*Decimal*	*Binary*	*Changes*	*Decimal*	*Binary*	*Changes*
0	00	-	0	00	-	0	00	-
1	01	1	3	11	2	1	01	1
2	10	2	1	01	1	3	11	1
3	11	1	2	10	2	2	10	1

The rows in Hadamard matrix in (2) are reordered to produce a Walsh matrix with a size of four W_4 which have successive rows of 0, 1, 3, and 2 sign changes as shown in (3):

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{3}$$

2.2. The Orthogonality of Walsh Matrix

The orthogonality properties of (1) can be used to generate an approaching value for the singular value generated by the SVD function as shown in (4) and (5):

$$SVD(B) = [U\ S\ V] \tag{4}$$

$$\frac{W * B * W}{n} \approx S \tag{5}$$

Where $SVD(B)$ is an SVD function that generates a singular matrix S and two orthogonal matrices U and V from the image block B. The value of the approach used can preserve the value of the bits embedded in an image because the image is not very sensitive to small changes in pixel values [32].

Fig. 1 shows that the maximum value of the Walsh matrix operation in (5) has the same pattern and values close to the S value generated through SVD in (4). The tightness of the S value obtained from (4) and (5) can also be done by performing SVD decomposition of the Walsh matrix as shown in (6) until (8).

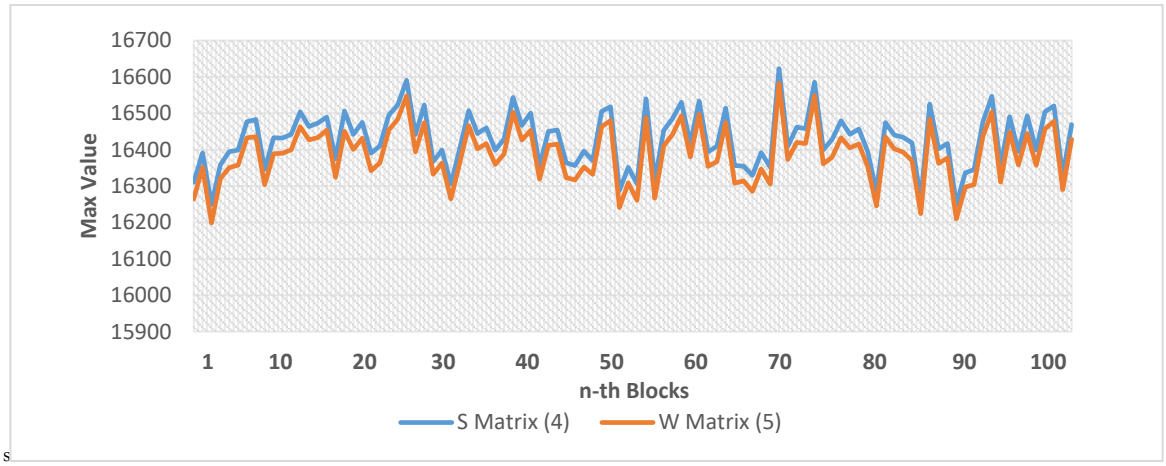

Fig. 1. Comparison of the max value of matrices of S in (4) and W in (5) from 100 random blocks

Fig. 2 shows that the dyadic Walsh matrix has the fastest computation time with 0.0154 seconds compared to sequence and natural ordering with running times of 0.0157 and 0.168 respectively.

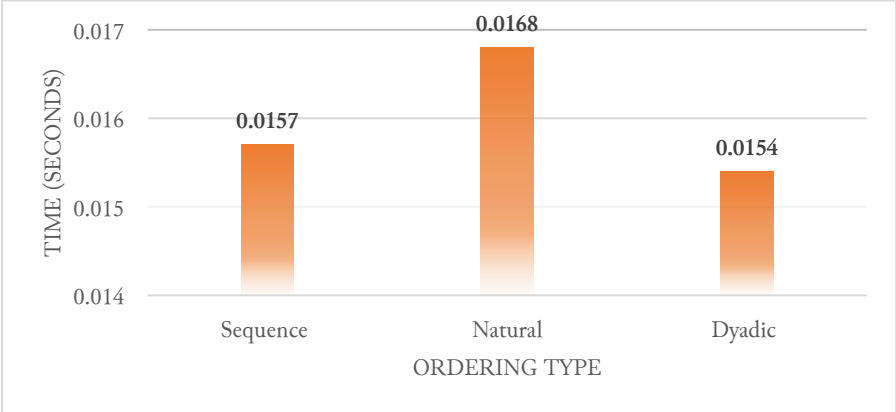

Fig. 2. Comparison of computation time of Walsh ordering

$$SVD(W_n) = [U\ S\ V] \tag{6}$$

$$S * S = W_n * W_n \tag{7}$$

$$\frac{S*S}{n} = I \tag{8}$$

The results of the substitutions and tests can be used to simplify the process of generating S values. Most uses of SVD in tampering and plagiarism detection only require an S value to insert an authentication bit in an image.

2.3. The Proposed Method

This research proposes improvements from the SVD block-based method proposed by Kang et. al [23] by developing the Walsh block from the Hadamard matrix in [32] to replace the U, S, V matrices,

and block scrambling as shown in Fig.3. The process of bits embedding is carried out on the first element of the Walsh block. It can then be used as a reference in the image authentication process with the same scheme as Kang's method to find the modified area. The blue channel was chosen as a place to embed the authentication bit because it has the lowest sensitivity level compared to red and blue [33], [34].

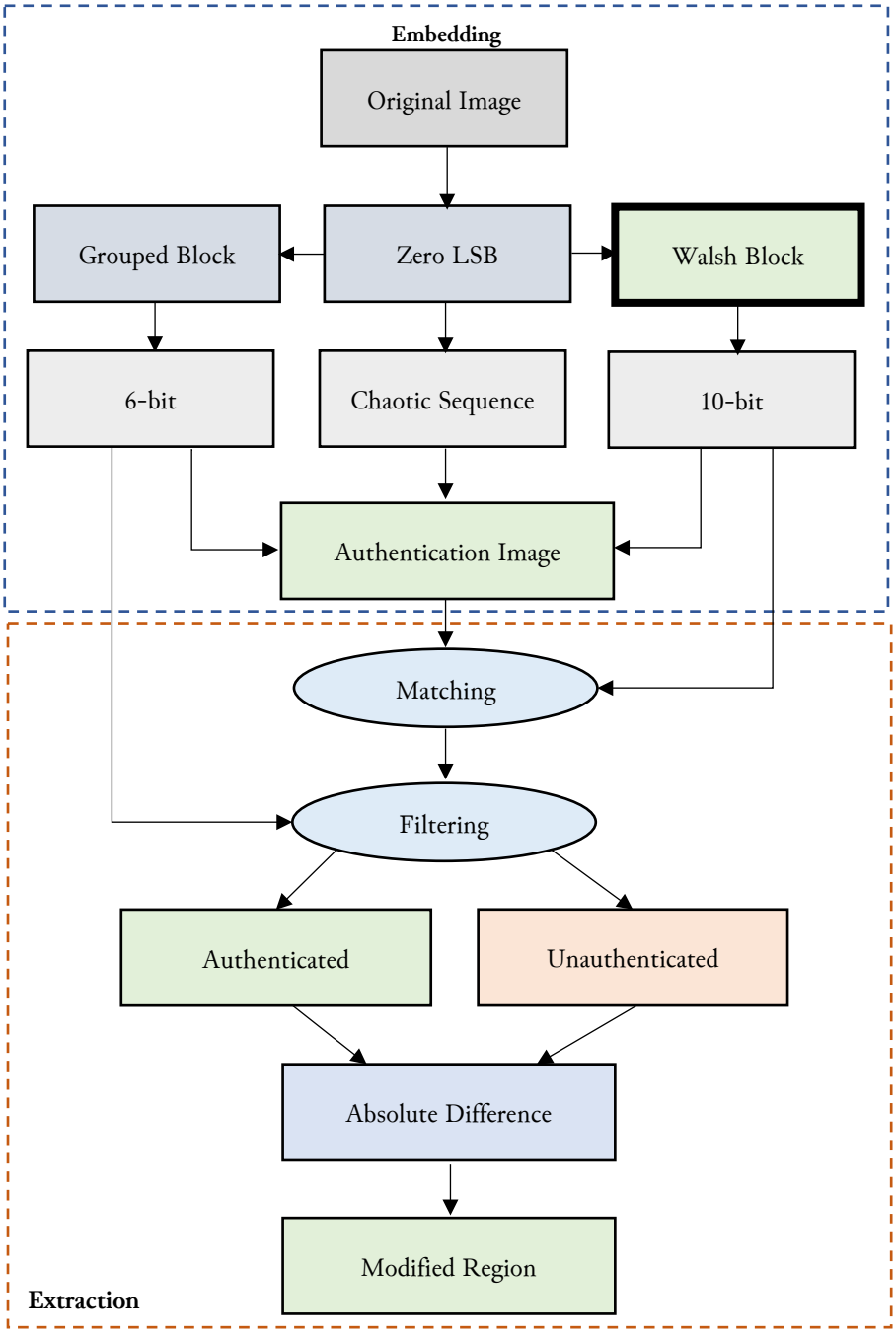

Fig. 3. Proposed scheme with Walsh block (bold outline)

The detailed steps of the proposed scheme can be described as follows:

- Read the original image *A*.
- Divide *A* into *B* image blocks with a size of 4x4.
- Set the LSB value of the entire image block to zero.

$$C = B - (B \bmod 2) \tag{9}$$

where C is the new image block.

- Generate matrix S through the Dyadic Walsh matrix block.

$$S = \frac{W_4 * C * W_4}{4} \tag{10}$$

Then take the largest element $S(1)$ which is the first element of the matrix. The next process is the same as the steps in Kang's methods starting from the 6th until the 19th equations for the embedding process and the equations 20 and 21 for the authentication or extraction process.

3. Results and Discussion

This experiment is carried out using two devices to measure the delta of the increase in speed between low and high computing power. The first device has a dual-core Core i3-1005G1 @1.2 - 3.4 GHz processor with 4GB of RAM and the second device has a 12-core Core i7-1260P @2.1 - 4.7 GHz processor with 16GB of RAM. The devices run on Windows 10 and 11 operating systems respectively. The dataset used was taken from the standard repository from USC-SIPI and the natural image repository from True Color Kodak image datasets each of 3 images randomly with a color depth of 24-bit. The first testing process is to compare the image quality before and after the authentication bit insertion is performed. The next step is to carry out an irregular attack on all these images and then an authentication process is carried out to find the modified region. The entire test is also measured by time parameters to compare the SVD [23], Hadamard [32], and the proposed method.

3.1. Imperceptibility

This section discusses the testing of image quality by embedding authentication bits into the original image and then comparing them through measurements of Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM). The comparison of image quality can be seen in Table 2.

Table 2. Comparison of Imperceptibility

Images	PSNR			SSIM		
	SVD [23]	*Hadamard [32]*	*Proposed*	*SVD [23]*	*Hadamard [32]*	*Proposed*
Airplane	55.91	55.91	**55.91**	0.9986	0.9986	**0.9986**
House	55.90	55.91	**55.92**	0.9996	0.9996	**0.9996**
Kodim01	55.92	55.92	**55.91**	0.9998	0.9998	**0.9998**
Kodim20	55.73	55.83	**55.80**	0.9994	0.9994	**0.9991**
Kodim21	55.93	55.90	**55.91**	0.9991	0.9991	**0.9996**
Sailboat	55.89	55.92	**55.91**	0.9996	0.9996	**0.9997**

The test results showed that the image quality of all methods had the same level of imperceptibility with an average PSNR value of 55.9 dB and an average SSIM of 0.9994. This is because the generation of the new S value can produce a value that is almost equal to the S value of the SVD and Hadamard block. The results prove that the Walsh block scheme at (4) and (5) can replace the SVD block scheme.

3.2. Authentication

The next experiment begins with manipulating marked images irregularly. The types of modifications used are enhancement, transformation, duplication, deletion, and addition of objects. The modifications are then authenticated to find the tampered region as shown in Fig.4. The first modification process is an enhancement carried out on the 'Airplane' image by balancing the color of the aircraft object to be bluer and then adjusting the contrast and brightness. The color adjustment process was also carried out to the 'Kodim20' image by changing the color of the shaft and the reverse end of the aircraft to be redder. The results of watermark extraction showed that the two images changed the location corresponding to their treatment.

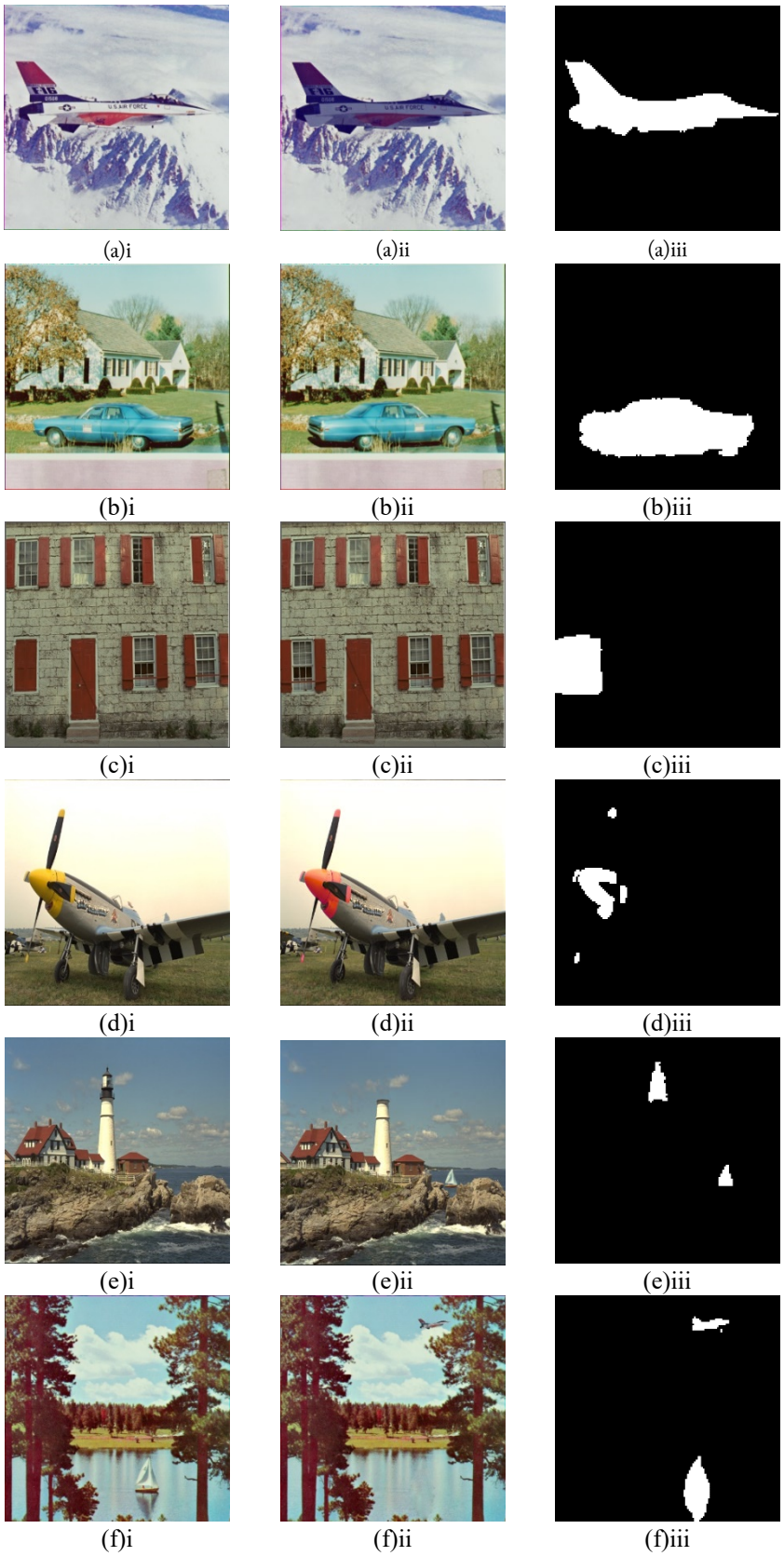

Fig. 4. Irregular modification on images: (a) airplane, (b) house, (c) kodim01, (d) kodim20, (e) kodim21, and (f) sailboat; i) Original image, ii) modified image, iii) tampered detection

The second modification process is a transformation carried out on the image of the 'House' by reflecting on the car object vertically so that the car faces to the right. The results of the watermark

extract show that two tampered regions intersect which are the loss of the original object and the emergence of a new object. The next process is duplication of the 'Kodim01' image by copying the window object on the right of the door and placing it on the left side of the door. The results of the authentication carried out show that there is a change in the window on the left side of the door while in the right window it does not change because it is only copied without changing the original object.

The last tampering process is carried out with two types of modifications, namely deletion and addition of objects. In the 'Sailboat' image by removing the sailboat object in the middle of the lake and adding the aircraft object from the 'Airplane' image on the upper right side of the image. Furthermore, in the image of 'Kodim21', a disappearance was carried out on the top of the lighthouse, and added the object of the sailing ship from the image of 'Sailboat'. The results of the extracts carried out on the two images can detect the loss of objects and the emergence of new objects in different regions that do not intersect with each other. The entire process of manipulation carried out on images can be found through the process of watermark extraction

3.3. Running Time

The last variable measured is the processing time which includes the bit embedding time and the image authentication process. Measurements are made on the process in the prior subsections. Preliminary experiments were conducted to compare the proposed method with the SVD and Hadamard methods which have the same scheme on the low computing device. The result of the embedding time comparison in Fig. 5 showed that Walsh's Dyadic-based methods can reduce average computational time by 10% and 6% against SVD and Hadamard methods respectively. Extraction testing also showed similar results where the proposed method can work faster up to 10% against the SVD method and 6% compared to the Walsh method as shown in Fig. 6.

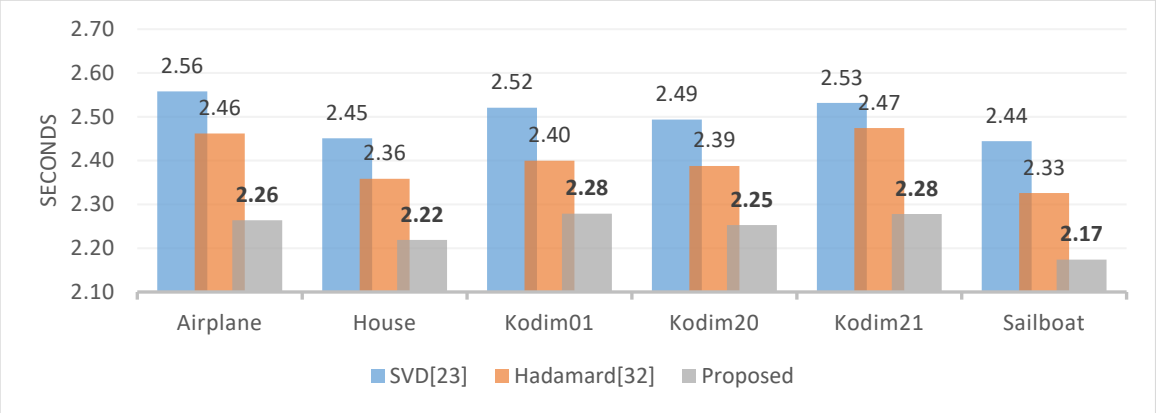

Fig. 5. Comparison of embedding time in a low computing device

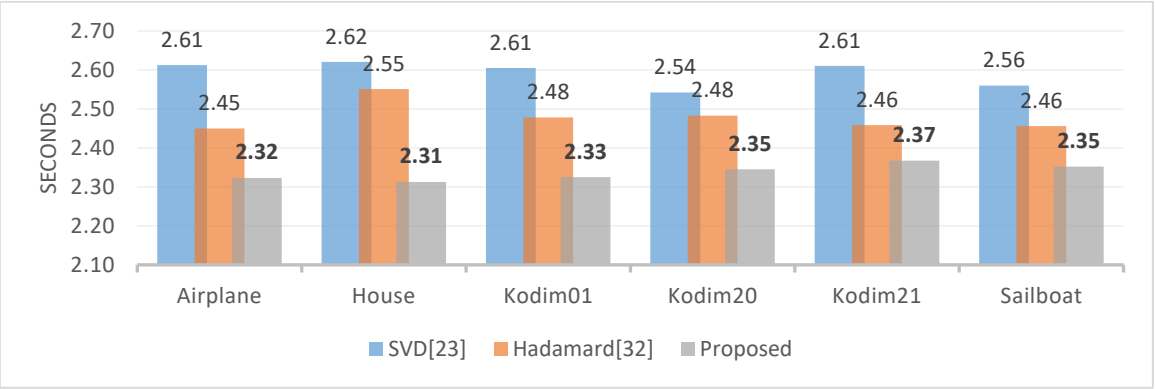

Fig. 6. Comparison of extraction time in a low computing device

The next testing process is carried out on high computing devices by comparing the proposed methods against SVD and Hadamard-based methods that have the same scheme. Test results in Fig. 7

show that the proposed method has the highest speed when compared to both SVD and Hadamard-based methods. Walsh's Dyadic-based method was able to reduce the average computational time reduction by 16% compared to the SVD-based method. The largest speed improvement that can be achieved is by 22% and 13% when compared to SVD and Hadamard-based methods respectively.

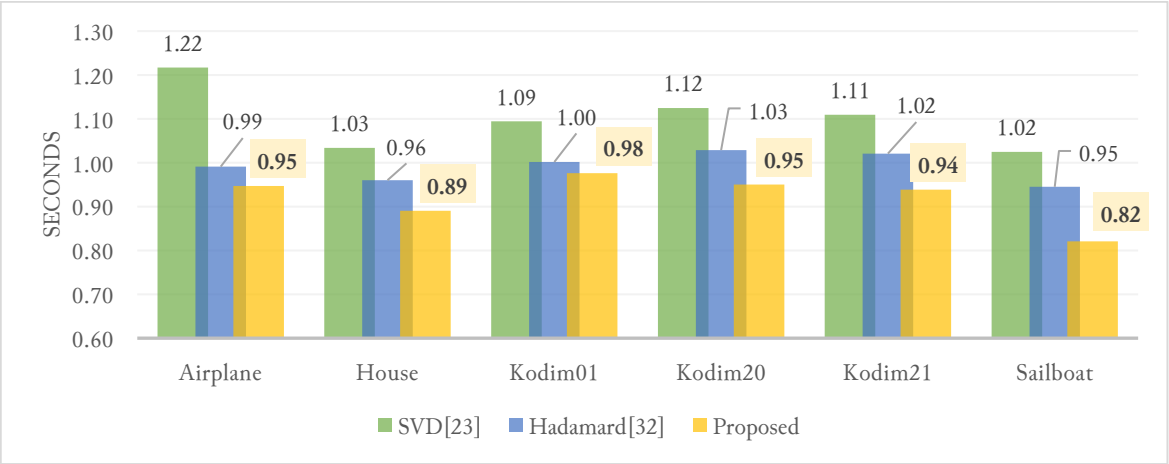

Fig. 7. Comparison of extraction time in a high computing device

Similar results are also seen in the extraction process in Fig. 8 which shows that the average speed improvement against the SVD method was 17% with the highest time reduction of 20% and 12% against the SVD and Hadamard methods respectively.

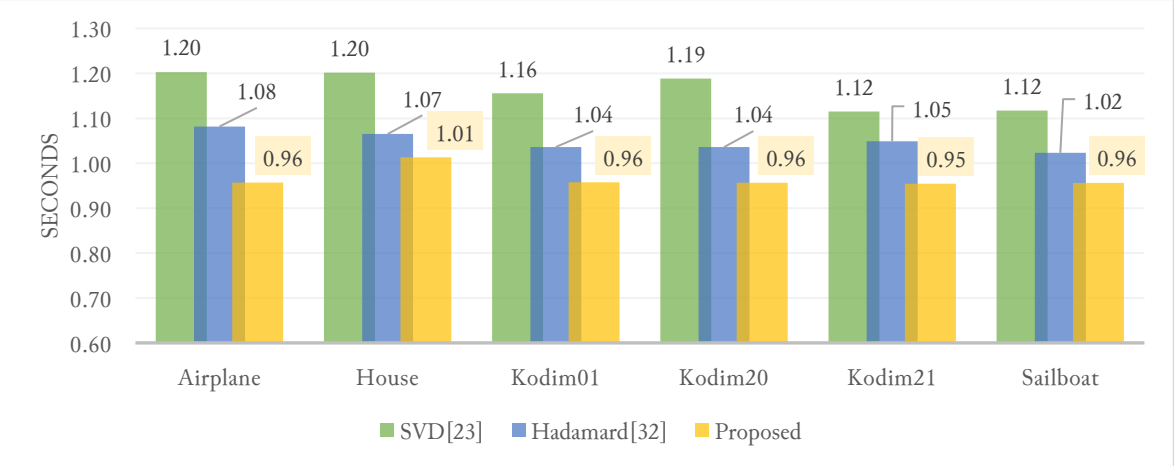

Fig. 8. Comparison of extraction time in a high computing device

The experiment results on two different computing devices showed that the increase in speed is directly proportional to the capabilities of the devices used. In low computing devices, the average improvement of the Dyadic Walsh method compared to the SVD method is only 10% in both embedding and extraction time while the results on high-end devices showed a maximum improvement is 22% in the embedding process and 20% in the extraction process. The comparisons to the Hadamard-based method also result in progressive improvements. The experiment in low-end devices showed that the proposed method is only able to reduce the computational time of the Hadamard method by an average of 6% on both the embedding and extraction process. While in high-performance devices the best time efficiency achieved is 13% in the embedding process and 12% in the extraction process.

This time reduction can be achieved by removing the useless matrices U and V on (4) and replacing them with a new generation method with (10). Moreover, in the SVD-based method, the decomposition process is carried out on each block to obtain an S value while in the Hadamard and the proposed method the generation of the matrices is only done once and can be used to obtain the S value of the

entire block. However, the Hadamard matrix has a high rate of binary changes, causing a slower generation process compared to the proposed method.

4. Conclusion

This paper proposes the use of dyadic Walsh blocks that have a lower level of complexity compared to SVD and Hadamard blocks in the image authentication process. The process of embedding bits is done by tracing the largest element of the Walsh block while the authentication bit is done through a grouped group. The results of the experiment showed that the proposed method has the same capabilities as the previous methods in terms of imperceptibility and authentication abilities. Meanwhile, in terms of computational time, the proposed method can work faster than SVD and Hadamard methods. For future work, the research will focus on optimizing the tracing process with a smaller bit range. In addition, it is necessary to develop a self-recovery system from an image that has been modified. The tracing results of the Walsh block can also be used as a feature in the development of an image plagiarism detection system in the case of copy-move forgery.

Acknowledgment

The author would like to thank the Institute for Research and Community Service (LPPM) of Universitas Diponegoro which has provided full support for this research.

Declarations

Author contribution. All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.
Funding statement. This research is funded by LPPM of Universitas Diponegoro through research grants No. 569-131/UN7.D2/PP/VII/2022.
Conflict of interest. The authors declare no conflict of interest.
Additional information. No additional information is available for this paper.

References

[1] M. Rezaei and H. Taheri, "Digital image self-recovery using CNN networks," *Optik (Stuttg).*, vol. 264, no. 1, pp. 1–12, 2022, doi: 10.1016/j.ijleo.2022.169345.

[2] J. Chen, X. Liao, and Z. Qin, "Identifying tampering operations in image operator chains based on decision fusion," *Signal Process. Image Commun.*, vol. 95, no. April, p. 116287, 2021, doi: 10.1016/j.image.2021.116287.

[3] J. V. C. I. R, L. Zheng, Y. Zhang, and V. L. L. Thing, "A survey on image tampering and its detection in real-world photos q," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 380–399, 2019, doi: 10.1016/j.jvcir.2018.12.022.

[4] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," *Comput. Electr. Eng.*, vol. 85, pp. 1–9, 2020, doi: 10.1016/j.compeleceng.2020.106685.

[5] H. M. Al-Otum and A. A. A. Ellubani, "Secure and effective color image tampering detection and self restoration using a dual watermarking approach," *Optik (Stuttg).*, vol. 262, pp. 1–22, 2022, doi: 10.1016/j.ijleo.2022.169280.

[6] A. Aminuddin and F. Ernawan, "AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no.8, pp. 5822-5840, 2022, doi: 10.1016/j.jksuci.2022.02.009.

[7] P. Johnston and E. Elyan, "A review of digital video tampering : From simple editing to full synthesis," *Digit. Investig.*, vol. 29, pp. 67–81, 2019, doi: 10.1016/j.diin.2019.03.006.

[8] M. Raveendra and K. Nagireddy, "Tamper video detection and localization using an adaptive segmentation and deep network technique," *J. Vis. Commun. Image Represent.*, vol. 82, pp. 1–13, 2022, doi: 10.1016/j.jvcir.2021.103401.

[9] K. Sitara and B. M. Mehtre, "Digital video tampering detection : An overview of passive techniques," *Digit. Investig.*, vol. 18, pp. 8–22, 2016, doi: 10.1016/j.diin.2016.06.003.

[10] F. Ding, G. Zhu, W. Dong, and Y. Shi, "An efficient weak sharpening detection method for image forensics," *J. Vis. Commun. Image Represent.*, vol. 50, pp. 93–99, 2018, doi: 10.1016/j.jvcir.2017.11.009.

[11] J. Sun, S. Kim, S. Lee, and S. Ko, "A novel contrast enhancement forensics based on convolutional neural networks," *Signal Process. Image Commun.*, vol. 63, pp. 149–160, 2018, doi: 10.1016/j.image.2018.02.001.

[12] D. Bhardwaj and V. Pankajakshan, "A JPEG blocking artifact detector for image forensics," *Signal Process. Image Commun.*, vol. 68, pp. 155–161, 2018, doi: 10.1016/j.image.2018.07.011.

[13] X. Wang, Q. Zhang, C. Jiang, and J. Xue, "Perceptual hash-based coarse-to-fine grained image tampering forensics method," *J. Vis. Commun. Image Represent.*, vol. 78, pp. 1–15, 2021, doi: 10.1016/j.jvcir.2021.103124.

[14] M. Jana, B. Jana, and S. Joardar, "Local feature based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing AMBTC with fuzzy logic," *J. King Saud Univ. - Comput. Inf. Sci.*, pp. 1–14, 2022, doi: 10.1016/j.jksuci.2021.12.011.

[15] B. Bolourian Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, "TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA," *Inf. Sci. (Ny).*, vol. 486, pp. 204–230, 2019, doi: 10.1016/j.ins.2019.02.055.

[16] A. Aminuddin and F. Ernawan, "AuSR2: Image watermarking technique for authentication and self-recovery with image texture preservation," *Comput. Electr. Eng.*, vol. 102, pp. 1–17, 2022, doi: 10.1016/J.COMPELECENG.2022.108207.

[17] J. Yang, T. Huang, and L. Su, "Using similarity analysis to detect frame duplication forgery in videos," *Multimed. Tools Appl.*, vol. 75, no. 4, pp. 1793–1811, 2016, doi: 10.1007/s11042-014-2374-7.

[18] G. Cattaneo, G. Roscigno, and U. Ferraro Petrillo, "Improving the experimental analysis of tampered image detection algorithms for biometric systems," *Pattern Recognit. Lett.*, vol. 113, pp. 93–101, 2018, doi: 10.1016/j.patrec.2017.01.006.

[19] X. Yuan, X. Li, and T. Liu, "Gauss–Jordan elimination-based image tampering detection and self-recovery," *Signal Process. Image Commun.*, vol. 90, no. April 2020, p. 116038, 2021, doi: 10.1016/j.image.2020.116038.

[20] S. N. V. J. Devi Kosuru, G. Swain, N. Kumar, and A. Pradhan, "Image tamper detection and correction using Merkle tree and remainder value differencing," *Optik (Stuttg).*, vol. 261, no. January, p. 169212, 2022, doi: 10.1016/j.ijleo.2022.169212.

[21] Y. Wang, X. Kang, and Y. Chen, "Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures," *J. Inf. Secur. Appl.*, vol. 54, pp. 1–11, 2020, doi: 10.1016/j.jisa.2020.102536.

[22] Y. Xiang, D. Xiao, H. Wang, and X. Li, "A secure image tampering detection and self-recovery scheme using POB number system over cloud," *Signal Processing*, vol. 162, pp. 282–295, 2019, doi: 10.1016/j.sigpro.2019.04.022.

[23] Q. Kang, K. Li, and H. Chen, "An SVD-based Fragile Watermarking Scheme With Grouped Blocks," in *International Conference on Information Technology and Electronic Commerce*, 2014, pp. 172–179, 2015, doi: 10.1109/ICITEC.2014.7105595.

[24] P. W. Adi and P. Arsiwi, "Fast and Robust Watermarking Method using Walsh Matrix Partition," *2019 2nd Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2019*, pp. 468–472, 2019, doi: 10.1109/ISRITI48646.2019.9034627.

[25] F. Ernawan, P. W. Adi, S. C. Liew, E. A. Sarwoko, and E. Winarno, "Fast image watermarking based on signum of cosine matrix," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 25, no. 3, pp. 1383–1391, 2022, doi: 10.11591/ijeecs.v25.i3.pp1383-1391.

[26] K. Prabha and I. Shatheesh Sam, "An effective robust and imperceptible blind color image watermarking using WHT," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2982–2992, 2022, doi: 10.1016/j.jksuci.2020.04.003.

[27] J. Du, Z. Chen, S. Fu, L. Qu, and C. Li, "Constructions of 2-resilient rotation symmetric Boolean functions through symbol transformations of cyclic Hadamard matrix," *Theor. Comput. Sci.*, vol. 919, pp. 80–91, 2022, doi: 10.1016/j.tcs.2022.03.033.

[28] N. Budda, K. Meenakshi, P. Kora, G. V. Subba Reddy, and K. Swaraja, "Image Digest using Color Vector Angle and Dominant Walsh-Hadamard Transform Coefficients," *Mater. Today Proc.*, no. xxxx, 2021, doi: 10.1016/j.matpr.2020.11.488.

[29] A. Sergeev and A. Vostrikov, "Calculating symmetrical Hadamard matrices of Balonin-Seberry construction for coding and masking," *Procedia Comput. Sci.*, vol. 176, pp. 1722–1728, 2020, doi: 10.1016/j.procs.2020.09.197.

[30] J.-L. Baril, S. Kirgizov, and V. Vajnovszki, "Gray codes for Fibonacci q-decreasing words," *Theor. Comput. Sci.*, vol. 927, pp. 120–132, 2022, doi: 10.1016/j.tcs.2022.06.003.

[31] J. PejaS and L. Cierocki, "Reversible data hiding scheme for images using gray code pixel value optimization," *Procedia Comput. Sci.*, vol. 192, pp. 328–337, 2021, doi: 10.1016/j.procs.2021.08.034.

[32] P. W. Adi and P. Arsiwi, "A novel watermarking method using hadamard matrix quantization," *J. ICT Res. Appl.*, vol. 14, no. 1, pp. 1–15, 2020, doi: 10.5614/itbj.ict.res.appl.2020.14.1.1.

[33] R. Y. Abadi and P. Moallem, "Robust and optimum color image watermarking method based on a combination of DWT and DCT," *Optik (Stuttg).*, vol. 261, pp. 1–17, 2022, doi: 10.1016/j.ijleo.2022.169146.

[34] W. Wan, J. Wang, Y. Zhang, J. Li, H. Yu, and J. Sun, "A comprehensive survey on robust image watermarking," *Neurocomputing*, vol. 488, pp. 226–247, 2022, doi: 10.1016/j.neucom.2022.02.083.