



A Novel Watermarking Method using Hadamard Matrix Quantization

Prajanto Wahyu Adi^{1,*} & Pramudi Arsiwi²

¹Department of Informatics Engineering, Universitas Dian Nuswantoro Semarang,
Jalan Imam Bonjol 207, 50131 Semarang, Indonesia

²Department of Industrial Engineering, Universitas Dian Nuswantoro Semarang,
Jalan Imam Bonjol 207, 50131 Semarang, Indonesia

*E-mail: prajanto@dsn.dinus.ac.id

Abstract. One of the most used watermarking algorithms is Singular Value Decomposition (SVD), which has a balanced level of imperceptibility and robustness. However, SVD uses a singular matrix for embedding and two orthogonal matrices for reconstruction, which is inefficient. In this paper, a Hadamard matrix is used to get a singular matrix for the reconstruction process. Moreover, SVD works with a floating-point value, which takes long processing time, while the Hadamard matrix works with an integer range, which is more efficient. Visual measurement showed that SVD and the new method had average NC values of 0.8321 and 0.8293, whereas the average SSIM values resulted in the same value (0.9925). In terms of processing time, the proposed method ran faster than SVD with an embedding and extraction time of 0.6308 and 0.2163 seconds against 0.8419 and 0.2935 seconds. The proposed method successfully reduced the running time while maintaining imperceptibility and robustness.

Keywords: *Hadamard matrix; image processing; quantization; SVD; watermarking.*

1 Introduction

The revolution of the internet has brought a new way of distributing media, where anyone can share anything at any time. This has led to convenience as well as a threat to the owners of digital media. In digital images, the ownership information is usually embedded in the form of a watermark. Image watermarking is a popular way to protect images from various illegal activities [1,2]. In line with the increasing use of watermarking, challenges in developing an improved watermarking algorithm arise. The algorithm should have good imperceptibility, great robustness against different types of attacks, and be able to reduce complexity in achieving a reliable watermarking system that can work in real time according to current demand. Most of the current research in watermarking is aimed at developing a robust or imperceptible watermarking model by combining several algorithms in the spatial or transform domain, which leads to

Received March 13th, 2019, 1st Revision December 12th, 2019, 2nd Revision February 28th, 2020, Accepted for publication April 3rd, 2020.

Copyright © 2020 Published by IRCS-ITB, ISSN: 2337-5787, DOI: 10.5614/itbj.ict.res.appl.2020.14.1.1

increased computational time. Several transformation algorithms are used, such as cosine transform [3], wavelet transform [4,5] and contourlet transform [6,7]. Transform domain methods are used to improve either the robustness or the imperceptibility by transmuting the raw pixel value into a certain coefficient, inserting the watermark, and then performing inverse transformation to get the embedded pixel value. They are combined with several spatial methods, such as the Chinese remainder theorem [8,9], histogram [10,11], and Singular Value Decomposition [12,13] to get good robustness or imperceptibility at the expense of computational time. Among them, Singular Value Decomposition (SVD) is one of the most popular methods due to its robustness against different types of attacks. SVD's decomposition process divides the image into three components, called U , S , and V , where only S is used in embedding and extraction. This causes inefficiency in the embedding and extraction processes.

This paper proposes a novel watermarking method that has a good level of robustness and imperceptibility, and runs in a shorter time, using quantization of the Hadamard matrix on the non-overlapping blocks of the host image. The orthogonality of the Hadamard matrix can be used to replace the decomposition and reconstruction processes of SVD in [14,15] to reduce the computational time. The watermark is embedded in the decomposed image by quantizing the highest value and reconstructs it using the inverse operation of the Hadamard matrix to get the watermarked image. A single Hadamard matrix, which has similar properties as a singular SVD matrix, can be used to simplify the process while maintaining the imperceptibility and robustness of the method.

2 Hadamard Matrix

A Hadamard matrix is an orthogonal matrix consisting of 1 and -1 within a size of 1, 2, or multiples of 4 [16]. In [17], the use of the H-matrix outperformed the cyclic S matrix in terms of reducing noise in the spectral image reconstruction process. The generation of a Hadamard matrix of size n follows this form:

$$\begin{bmatrix} h & h \\ h & -h \end{bmatrix}$$

where h is the value of 1 in the square matrix of 2, so enlargement of the matrix can be performed by duplicating the block according to the negative or the positive sign.

In watermarking, a Hadamard matrix can be used to embed a watermark bit by using the forward and inverse operation of the image block of n with the Hadamard matrix of n . The block size used is 8, which corresponds to the size of

the quantization matrix in image compression in order to retain the value under an attack. The Hadamard matrix of 8 is defined as follows:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \quad (1)$$

The orthogonality of H can be proved using the diagonal matrix S of SVD in Eqs. (2) and (3):

$$[U \ S \ V] = SVD(H) \quad (2)$$

$$H = U * S * V^T \quad (3)$$

where S is the diagonal matrix, and U and V are orthogonal matrices. The square of S will result in a diagonal matrix of 8, which is equal to the square of H , as defined in Eq. (4):

$$S * S = H * H = \begin{bmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix} \quad (4)$$

Hence, we can replace the use of a singular value in S with H and eliminate the use of matrices U and V to reduce the complexity. To get the identity matrix, we can divide the square of H with a block size of N , as described in Eq. (5).

It is guaranteed that the forward and inverse operation of the host image will have the same value. The use of the Hadamard matrix is able to generate singular values that are similar to those of SVD. A comparison of the singular values between SVD and Hadamard from 64 random blocks is presented in Figure 1.

$$\frac{H*H}{N} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (5)$$

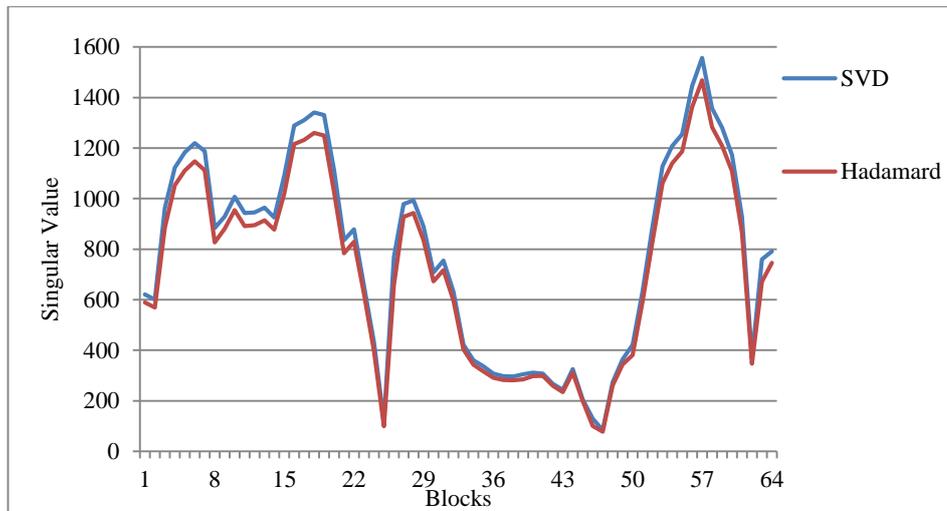


Figure 1 Comparison of singular value between SVD and Hadamard matrix operation from 64 random blocks.

3 Proposed Model

The main idea of this model is to use a single Hadamard matrix to develop a simple but powerful watermarking scheme. The Hadamard matrix is used to perform forward and inverse operations in both the embedding and the extraction process. The watermark is embedded using the generation of a quantization table, which is also used as the key. Compared with the SVD model used in [14] and [15], the proposed model is more straightforward, because it only needs a matrix and a quantization table as shown in Figure 1.

3.1 Embedding

Embedding consists of processes such as host image partition, Hadamard operation, and quantization. The detailed process is as follows:

Input : Host image I and watermark image w with size of I / block size

Output : Watermarked Image I'

Step 1 : Read the host image I . If I is a color image, transform it into YCbCr, get the Y channel and divide it into non-overlapping blocks of 8×8

Step 2 : Build a Hadamard matrix H using Eq. (1)

Step 3 : Get the singular matrix from each block using:

$$S_n = \frac{H * I_n * H}{N} \quad (6)$$

where N is the block size, I_n and S_n is are the image and singular matrix of the n -th block.

Step 4 : Take the first element from singular matrix S_n (1) as the singular value S_n

Step 5 : Define the bin size q for quantization using:

$$q = (\max(s) - \min(s)) / k \quad (7)$$

where k is a bin number and s is the singular value of the entire block

Step 6 : Define the key using quantization as follows:

$$b_i = \min(s) + q(i - 2) \quad (8)$$

$$t_i = \min(s) + q(i - 1) \quad (9)$$

$$m_i = (b_i + t_i) / 2 \quad (10)$$

where m is the value for embedding the watermark, t and b are the top and bottom tolerance limits, which are used to preserve the watermark value at the i -th quantization bin. Thus, there will be no change in value or false positive in the watermark bit.

Step 7 : Change the value of s according to the watermark bit using the following rule:

$$s'_n = \begin{cases} (b_i + m_i) / 2 & , \text{if } w = 1 \\ (t_i + m_i) / 2 & , \text{if } w = 0 \end{cases} \quad (11)$$

where s'_n is the new singular value of n and w is the watermark bit

Step 8 : Apply the inverse operation to get the watermarked block:

$$I'_n = \frac{H * S'_n * H}{N} \quad (12)$$

where S' is the new singular matrix and I' is the watermarked image of block n

Step 9 : Repeat the process on the remaining blocks to build the watermarked image I'

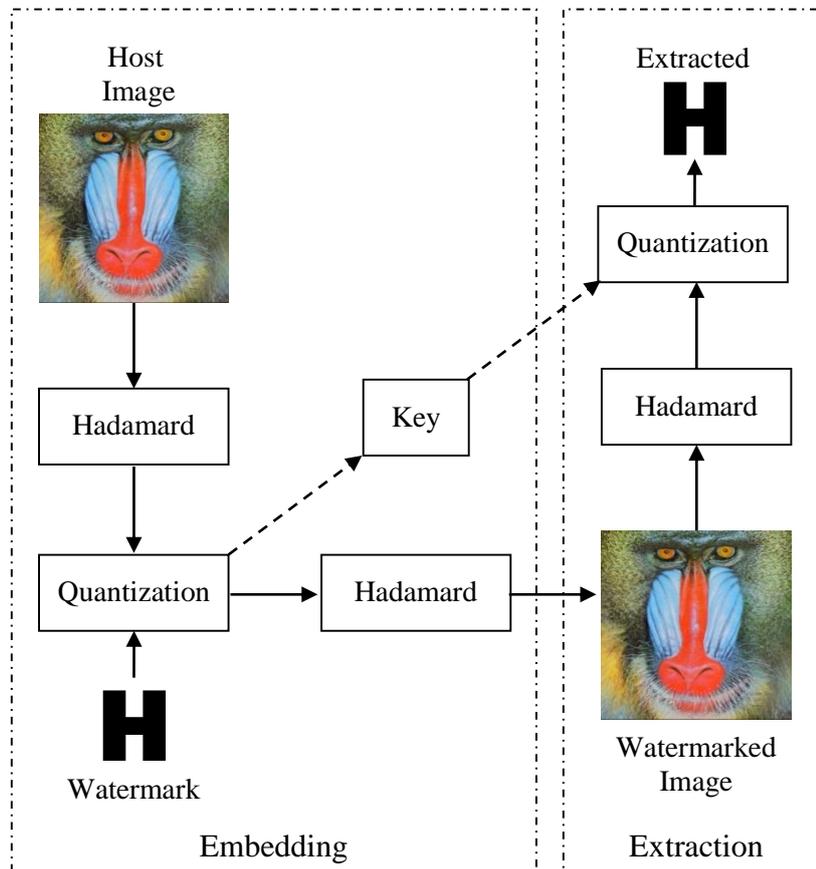


Figure 2 Proposed model.

3.2 Extraction

The watermarked image is processed with a Hadamard matrix and then quantized to get the watermark image. The detailed process is as follows:

Input : Watermarked image I'

Output : Watermark image w

Step 1 : Read watermarked image I' . If I' is a color image, transform it into YCbCr, get the Y channel and then divide it into blocks of 8×8

Step 2 : Get the Hadamard matrix from Eq. (1)

Step 3 : Get the singular matrix from each block using:

$$S'_n = \frac{H * I'_n * H}{N} \quad (13)$$

Step 4 : Take the first element from the singular matrix as a singular value s'_n

Step 5 : Get the watermark bit from the singular value following this rule:

$$w_n = \begin{cases} 1 & ,if\ b_n \leq s'_n < m_n \\ 0 & ,if\ m_n \leq s'_n < t_n \end{cases} \quad (14)$$

Step 6 : Repeat the process for the entire block to extract the watermark

4 Experiment Results and Analysis

Three color images i.e. ‘Baboon’, ‘F16’, ‘Peppers’, and three greyscale images i.e. ‘Barbara’, ‘Goldhill’, ‘Pirate’ were used as host images with a size of 512 x 512. For the watermark, a binary image with a size of 64 x 64 was used.



(a) Baboon



(b) F16



(c) Peppers



(d) Barbara



(e) Goldhill



(f) Pirate



Watermark

Figure 3 Host images and watermark.

4.1 Imperceptibility

To measure the visual quality after the embedding process, the proposed model is compared with the existing SVD method. The structural similarity (SSIM) index [18] was chosen because of its ability to measure visual quality on par with the human visual system.

Table 1 Comparison of SSIM with existing method (SVD).

Images	SVD	Proposed
Baboon	0.9964	0.9964
F16	0.9873	0.9876
Peppers	0.9868	0.9868
Barbara	0.9946	0.9947
Goldhill	0.9942	0.9942
Pirate	0.9954	0.9955

The comparison was performed with a bin size of 40 according to the previous research on SVD. Table 1 shows that the proposed method and the SVD method had the same average SSIM value of 0.9925.

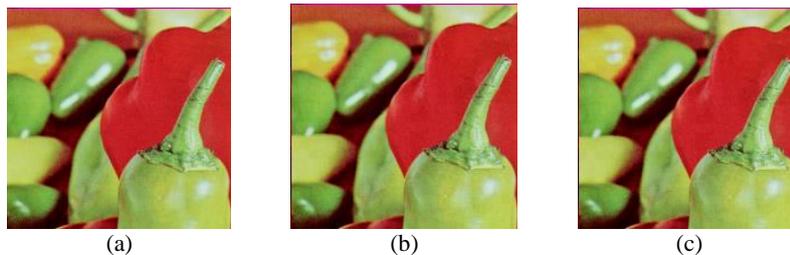


Figure 4 Visual comparison of (a) host image and the watermarked image from (b) proposed method and (c) SVD.

Figure 4 shows no visible difference between both methods compared with the host image. This is due to the capability of the Hadamard operation, which is able to produce singular values close to those of the S matrix of SVD, as shown in Figure 1. The singular value decomposition in Eqs. (2) and (3) can be replaced using Eqs. (6) and (12).

4.2 Robustness

The next test was performed on the watermarked image under five different attacks, namely: JPEG compression with quality at 50%; Gaussian filtering with a sigma of 0.5; contrast enhancement at 0.02; resizing [2 0.5]; center cropping at 100 x 100 pixels; gamma correction at 0.95; and rotation at 45°. The attacks on the watermarked image 'Peppers' are presented in Figure 5.

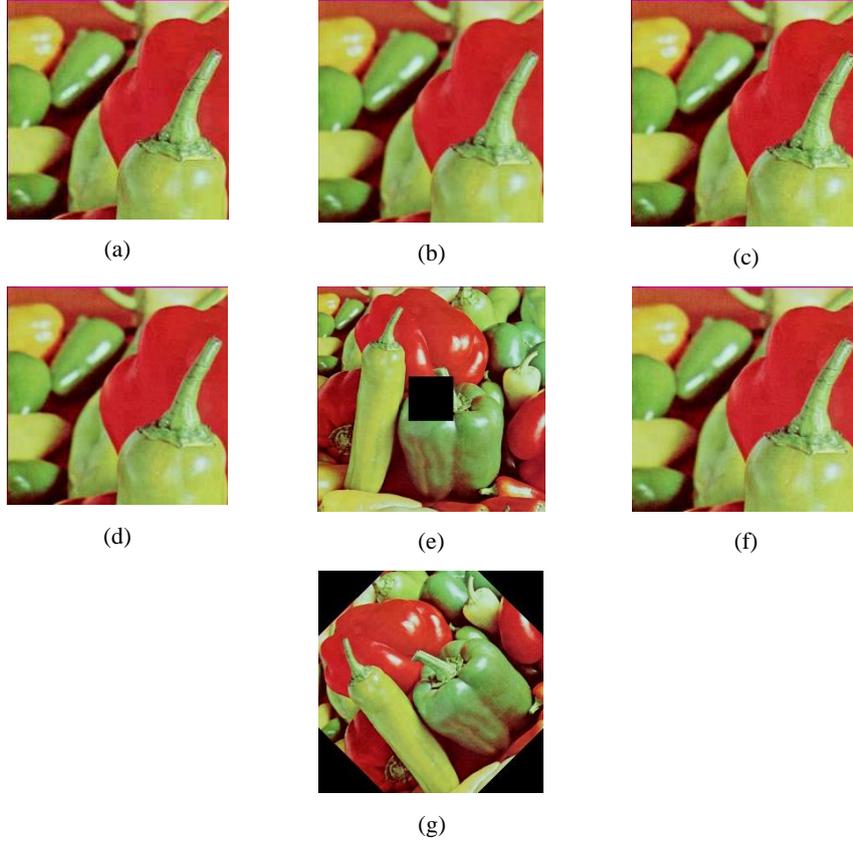


Figure 5 Attacks on watermarked image 'Peppers': (a) JPEG compression; (b) Gaussian filtering; (c) contrast enhancement; (d) resizing; (e) cropping; (f) gamma correction; (g) rotation.

The attacked watermarked image was extracted to get the watermark. The extracted watermark is shown in Figure 6. They were then compared with the original watermark to measure the robustness using normalized correlation (NC), defined as follows:

$$NC = \frac{\sum_{p=1}^P w_p w'_p}{\sqrt{\sum_{p=1}^P w_p^2} \sqrt{\sum_{p=1}^P w'_p{}^2}} \quad (15)$$

where w_p and w'_p are the original and extracted watermark respectively in pixel p out of P pixels. A comparison of the NC value between SVD and the proposed method is presented in Table 2.

Method	Attacks	Baboon	F16	Peppers	Barbara	Goldhill	Pirate
SVD	JPEG (50%)						
	Gaussian (0.5)						
	Contrast (0.02)						
	Resize (2 0.5)						
	Crop (100)						
	Gamma (0.95)						
	Rotation (45°)						
Proposed	JPEG (50%)						
	Gaussian (0.5)						
	Contrast (0.02)						
	Resize (2 0.5)						
	Crop (100)						
	Gamma (0.95)						
	Rotation (45°)						

Figure 6 Extracted watermarks.

Table 2 Comparison of NC with existing method (SVD).

Attacks	Method	Baboon	F16	Peppers	Barbara	Goldhill	Pirate
JPEG	SVD	0.9641	0.9594	0.9675	0.9834	0.9994	0.9790
	Proposed	0.9360	0.9492	0.9485	0.9637	0.9951	0.9517
Gaussian	SVD	0.9131	0.9529	0.9646	0.9471	0.9691	0.9496
	Proposed	0.9487	0.9585	0.9697	0.9642	0.9726	0.9581
Contrast	SVD	0.8945	0.8505	0.8500	0.8622	0.8859	0.8757
	Proposed	0.8718	0.8326	0.8379	0.8373	0.8697	0.8487
Resize	SVD	0.9807	0.9998	0.9938	0.9837	0.9986	0.9982
	Proposed	0.9889	0.9982	0.9860	0.9973	0.9998	1.0000
Crop	SVD	0.8628	0.8636	0.8578	0.8625	0.8624	0.8619
	Proposed	0.8600	0.8632	0.8578	0.8632	0.8643	0.8523
Gamma	SVD	0.8054	0.1404	0.1602	0.8369	0.7495	0.8944
	Proposed	0.7954	0.1659	0.1938	0.8443	0.7553	0.8956
Rotation	SVD	0.5997	0.4859	0.4841	0.6352	0.6253	0.6378
	Proposed	0.5932	0.4648	0.4954	0.6285	0.6233	0.6310

The robustness test also gave similar average NC values for the proposed method and SVD, i.e. 0.8293 and 0.8321 respectively. Most of the extracted watermarks can still be seen quite clearly, especially after JPEG compression, Gaussian filtering and resizing. The proposed method had a lower NC value in JPEG compression and contrast enhancement, while it got a better result in Gaussian and gamma correction. This is due to the characteristic of the attack: JPEG and contrast enhancement work in homogeneous areas with small differences in pixel values. This produces a sufficient number of differences compared to SVD. But overall, the two methods only showed a very small difference.

The proposed method uses Hadamard quantization as defined in Eqs. (7) to (11). It is able to assign the watermark in the middle value of the Hadamard coefficient, which has a large error tolerance. Hence, the robustness can be maintained by keeping the singular values as close as possible to the singular values of SVD.

4.3 Running Time

The last assessment was to compare the running time of the watermark embedding and extraction processes from all attacks on watermarked images. The experiments were performed on a laptop with a 2nd-generation Core i3 2310M 2.1Ghz, 6GB of RAM and MATLAB 2015a. The measurements are expressed in seconds.

Figure 7 shows that the embedding process of the proposed method was about 25% faster than that of SVD. The average embedding time of the proposed method was 0.6308 seconds, compared to SVD with 0.8419 seconds. The extraction processes of the proposed method took 0.2163 seconds of running time compared to 0.2935 seconds with the SVD method, as shown in Figure 8.

Extraction time measurement was performed on all images that were attacked, as shown in Figure 8.

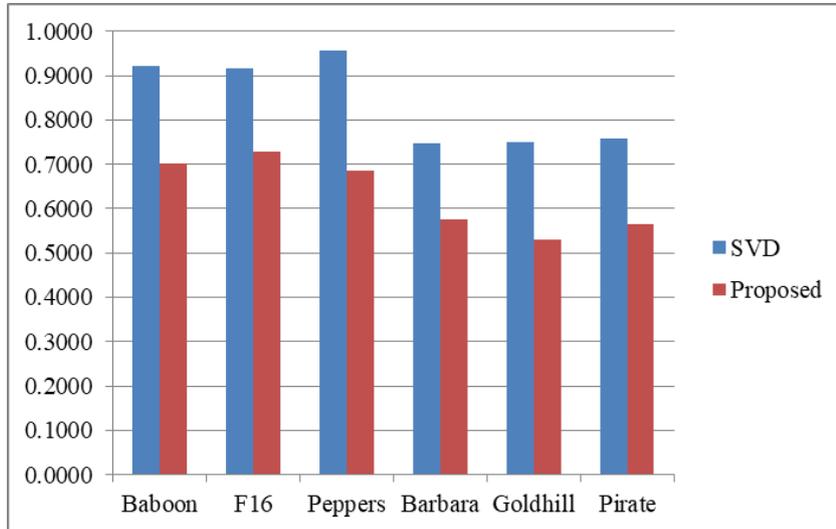


Figure 7 Embedding time in seconds.

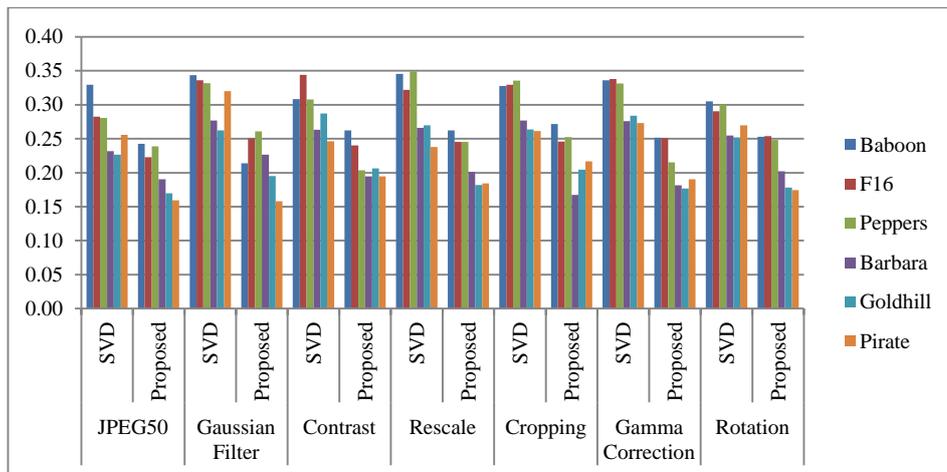


Figure 8 Extraction time in seconds.

The test results prove that the proposed method uses less processing time and is able to maintain the imperceptibility and robustness under different types of attacks. The SVD model requires complex mathematical equations, such as inverse transformation, eigenvalue, and eigenvector. In this paper, this was

simplified by using Eqs. (6) and (12), which use simple multiplication and division of the matrix.

5 Conclusion

This paper proposed a novel watermarking method using the Hadamard matrix to reduce the computational complexity in finding a singular value compared to SVD. SVD uses two orthogonal matrices in the reconstruction process and a singular matrix in watermark embedding. The new method uses only a single Hadamard matrix for the whole process. The Hadamard matrix can be used to find the singular matrix and reconstruct the watermarked image. Moreover, most of the processes in the proposed model are done using an integer range so that less computational resources are required compared with SVD, which works with a floating-point value.

The experimental results show that SVD and the proposed method had the same average SSIM value of 0.9925, while the average NC value was 0.8321 and 0.8293 respectively. In terms of processing time, the proposed method needed less time for embedding and extraction, i.e. 0.6308 and 0.2163 seconds, compared with SVD, i.e. 0.8419 and 0.2935 seconds. The proposed method was able to maintain the same level of imperceptibility and robustness with less processing time.

In a future work, this method can be tested with a false-positive scenario to ensure that the method cannot be authenticated with a wrong watermark. The embedding scheme can be improved using watermark weighting to balance imperceptibility and robustness.

Acknowledgement

This study was supported by the Institute of Research and Community Service of Universitas Dian Nuswantoro through research grant 241/A.38/UDN-09/XI/2018.

References

- [1] Adi, P.W., Ramhanti, F.Z. & Winarno, E., *Robust Watermarking through Dual Band IWT and Chinese Remainder Theorem*, Bulletin Electr. Eng. Informatics, **7**(4), pp. 561-569, 2018.
- [2] Singh, S.P. & Bhatnagar, G., *A New Robust Watermarking System in Integer DCT Domain*, J. Vis. Commun. Image Represent, **53**, pp. 86-101, 2018.

- [3] Roy, S. & Pal, A.K., *A Blind DCT Based Color Watermarking Algorithm for Embedding Multiple Watermarks*, AEU - Int. J. Electron. Commun., **72**, pp. 149-161, 2017.
- [4] Sangeetha, N. & Anita, X., *Entropy Based Texture Watermarking Using Discrete Wavelet Transform*, Optik (Stuttgart), **160**, pp. 380-388, 2018.
- [5] Gangadhar, Y., Giridhar Akula, V.S. & Reddy, P.C., *An Evolutionary Programming Approach for Securing Medical Images Using Watermarking Scheme in Invariant Discrete Wavelet Transformation*, Biomed. Signal Process. Control, **43**, pp. 31-40, 2018.
- [6] Najih, A., Al-Haddad, S.A.R., Ramli, A.R., Hashim, S.J. & Nematollahi, M.A., *Digital Image Watermarking Based on Angle Quantization in Discrete Contourlet Transform*, J. King Saud Univ. – Comput. Inf. Sci., **29**(3), pp. 288-294, 2017.
- [7] Etemad, S. & Amirmazlaghani, M., *A New Multiplicative Watermark Detector in the Contourlet Domain Using T Location-Scale Distribution*, Pattern Recognit., **77**, pp. 99-112, 2018.
- [8] Patra, J.C., Karthik, A. & Bornand, C., *A Novel CRT-Based Watermarking Technique for Authentication of Multimedia Contents*, Digit. Signal Process, **20**(2), pp. 442-453, 2010.
- [9] Adi, P.W., Astuti, Y.P. & Subhiyakto, E.R., *Imperceptible Image Watermarking based on Chinese Remainder Theorem over the Edges*, in 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), pp. 1-5, 2017.
- [10] Lin, P.Y., *Imperceptible Visible Watermarking Based on Postcamera Histogram Operation*, J. Syst. Softw., **95**, pp. 194-208, 2014.
- [11] Manikandan, V.M. & Masilamani, V., *Histogram Shifting-Based Blind Watermarking Scheme for Copyright Protection in 5G*, Comput. Electr. Eng., **72**, pp. 614-630, 2018.
- [12] Jia, S.L., *A Novel Blind Color Images Watermarking Based on SVD*, Optik (Stuttgart), **125**(12), pp. 2868-2874, 2014.
- [13] Araghi, T.K., Manaf, A.A. & Araghi, S.K., *A Secure Blind Discrete Wavelet Transform Based Watermarking Scheme Using Two-Level Singular Value Decomposition*, Expert Syst. Appl., **112**, pp. 208-228, 2018.
- [14] Mohan, B.C. & Kumar, S.S., *A Robust Image Watermarking Scheme using Singular Value Decomposition*, J. Multimed., **3**(1), pp. 7-15, 2008.
- [15] Adi, P.W. & Rahmanti, F. Z., *Robust Integer Haar Wavelet Based Watermarking using Singular Value Decomposition*, J. Ilmu Komput. dan Inf., **9**(1), pp. 26-34, 2016.
- [16] Álvarez, V., Armario, J.A., Falcón, R.M., Frau, M.D., Gudiel, F., Güemes, M.B. & Osuna, A., *Generating Binary Partial Hadamard Matrices*, Discret. Appl. Math., **263**, pp. 2-7, 2019.

- [17] Yue, J., Han, J., Li, L. & fa Bai, L., *Denoising Analysis of Spatial Pixel Multiplex Coded Spectrometer with Hadamard H-Matrix*, *Opt. Commun.*, **407**, pp. 355-360, 2018.
- [18] Wang, Z., Bovik, A.C., Sheikh, H.R. & Simoncelli, E.P., *Image Image Quality Assessment: From Error Visibility to Structural Similarity*, *IEEE Trans. Image Process.*, **13**(4), pp. 600-612, 2004.