Iraqi Journal for Computer Science and Mathematics

Volume 5 | Issue 4 Article 5

2024

Robust Image Watermarking Based on Schur Decomposition

Ahmad Toha
Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia

Ferda Ernawan
Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia AND Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah Pekan Pahang, 26600, Malaysia, ferda1902@gmail.com

Agit Amrullah
Faculty of Computer Science, Universitas AMIKOM, Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, Indonesia

Recommended Citation

Toha, Ahmad; Ernawan, Ferda; and Amrullah, Agit (2024) "Robust Image Watermarking Based on Schur Decomposition," *Iraqi Journal for Computer Science and Mathematics*: Vol. 5: Iss. 4, Article 5.
DOI: https://doi.org/10.52866/2788-7421.1203
Available at: https://ijcsm.researchcommons.org/ijcsm/vol5/iss4/5

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2024;5:47–57

RESEARCH ARTICLE

Robust Image Watermarking Based on Schur Decomposition

Ahmad Toha [a], **Ferda Ernawan** [a,b,*], **Agit Amrullah** [c]

[a] Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia
[b] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah Pekan Pahang, 26600, Malaysia
[c] Faculty of Computer Science, Universitas AMIKOM, Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, Indonesia

ABSTRACT

The advanced of internet technology allows unauthorized people to distribute multimedia data. Copyright protection for digital images is needed to protect the intellectual properties of the digital image. This study presents a colour image watermarking using schur decomposition for protecting the digital copyright. This study investigates the significant contribution of the orthogonal U of schur decomposition with the size of 8×8 pixels. The proposed scheme embeds a watermark on the (U_2, U_6) of the U matrix to achieve high invisibly and robustness of the embedded watermark. The relationship of each coefficient on the U matrix of Schur decomposition is also investigated. The experimental results demonstrate that the proposed scheme achieved high invisibility with the SSIM value of about 0.9951. The proposed scheme was also evaluated by several image processing attacks such as added noise, resized image, filtered image, and compressed image. The proposed scheme obtained a high level of resilience with the NC value of 0.996.

Keywords: Watermark, Copyright protection, Image watermarking, Schur decomposition, Robust watermarking

1. Introduction

With the advanced internet technology, the ability to retrieve and distribute multimedia data, including images, videos, audio, and text, has become very accessible. However, multimedia data can be replicated, traded, or acquired without the owner's consent, posing challenges in safeguarding ownership rights [1]. Digital watermarking is an alternative solution and an effective approach to address this issue [2]. Watermarking is a method by embedding a watermark into digital data, such as images, video, or music, to label or safeguard the original content against unauthorized utilization. Digital watermarking can offer protection, verification of an image's validity and legally establish ownership of the image [3].

Image watermarking methods can be categorized into two distinct groups: spatial domain and transformation domain approaches. In the spatial domain [4], the technique involves embedding a watermark into an image pixels by directly changing the pixel values. This approach may embed the watermark into the least significant bit shifting (LSB) or pixel intensity modulation to conceal the watermark. The benefits of spatial domain approach that it can achieve high invisibility of the watermarked image. However, this approach is not resistance against attacks such as compression, filtered image and added noise to the watermarked image.

The transform domain method involves embedding the watermark into the transform coefficients of the host image. The transformation method such as DWT [5, 6], DCT [7], and IWT [8] have been widely implemented in image watermarking. In these methods, the watermark is inserted into the transform coefficients of the host image, which may subsequently be transformed back to the spatial domain using the same inverse transform. The approach has

Received 17 December 2023; accepted 25 August 2024.
Available online 25 November 2024

* Corresponding author.
E-mail address: ferda@umpsa.edu.my, ferda1902@gmail.com (F. Ernawan).

https://doi.org/10.52866/2788-7421.1203

some advantages, including the robustness against compression and image processing attacks [9–11]. However, this approach can be more complex to be implemented and it required more computational compared to spatial domain approach.

Furthermore, the existing approaches used BCH error correcting coding to achieve high resilient watermarked image [12]. The scheme aims to increase the security and resilience of image watermarking by utilizing the spread spectrum algorithm and BCH error correcting coding. In addition, a robust blind watermarking approach based on difference coefficients is also presented in [13], where the difference between two DCT coefficients of the block is utilized to insert the watermark. A unique DCT-based watermarking approach is employed in [14] to conceal binary bits within grayscale images. This approach has the capability to seamlessly integrate robust watermarking based on DCT coefficients, and the simplicity of incorporating human visual attributes. Su et al.'s [15] presented a watermarking scheme based on schur decomposition. The embedding and extracting watermark are performed by examining the correlation between the first column of 4×4 pixels. The scheme produced high a PSNR value, and it showed a high robustness under various attacks. While the imperceptibility and robustness performances still can be further improved.

In frequency domain, the existing transform methods consumed high computational complexity especially the used wavelet transform for transforming spatial domain. Image watermarking based on wavelet domain required high computational complexity during embedding and extracting watermark. The Schur decomposition is one of matrix decomposition techniques that can reduce the computational time for embedding process [10]. In linear algebra, the schur decomposition consists of square matrix with orthogonal matrix (U) and upper triangulate matrix (S) [11]. The embedding watermark by examining schur decomposition needs to be further investigated to achieve a high quality of the watermarked image and high robustness under various attacks.

This research proposed a new embedding watermark based on schur decomposition by examining the orthogonal U with the matrix size of 8×8 coefficients. This research investigates the best location of 8×8 in U matrix in schur decomposition for embedding the watermark. The matrix size of 8×8 and 4×4 of orthogonal U in schur decomposition is chosen to be investigated to achieve high balancing performance between the imperceptibility and robustness. The embedding watermark based on the relationship of each coefficient on the U matrix of schur decomposition is investigated. The proposed scheme will be evaluated under various attacks to measure robustness performance. The various attacks included blurred image, gaussian noise, median filter, salt & pepper noise, sharpening, JPEG compression, JPEG 2000, and resized image. The contributions of this study are summarized as follows:

(1) The proposed embedding watermark on the orthogonal U_2, U_6 matrix with the size of 8×8 schur decomposition can achieve high invisibility with the SSIM value of 0.9951.
(2) The proposed scheme also provides a high robustness performance with NC value of 0.9982 under JPEG 2000.
(3) The proposed scheme requires minimum computational time which is 0.3 second for embedding watermark and 0.2 second for extracting watermark image.

2. The existing watermarking schemes

The study conducted by Su and Chen [15] presented a colour image watermarking method that relies on Schur decomposition. The scheme aims to investigate certain columns of the schur decomposition-based watermarking approach for embedding watermarks. The scheme analyzed correlation of matrix U and matrix D of schur decomposition to get the maximum robustness performance. The scheme utilized orthogonal U_2 and U_4 for embedding the watermark. The results showed the embedding watermark by modifying orthogonal U_2 and U_4 achieved high imperceptibility. The embedded watermark is also resistant against several attacks. The imperceptibility and robustness performance still can be improved to achieve a high balance between imperceptibility and robustness.

Karajeh et al. [7] presented digital audio watermarking based on DWT and Schur decomposition. This research utilized DWT to transform the original audio. The DWT is employed to depict the audio signal in both the frequency, whereas the schur decomposition is utilized to incorporate and extract the watermark inside the audio signal. The wavelet coefficients are computed by using schur decomposition to embed the watermark. This scheme produced a good resilient to a wide range of attacks, including compression, and other forms of audio processing. The watermark is inserted in the frequency representation of the audio signal by the utilizations of DWT. Subsequently, the robustness of the watermark has improved by using the schur decomposition.

Hsu et al. [16] presented an enhanced colour image watermarking system that utilizes schur

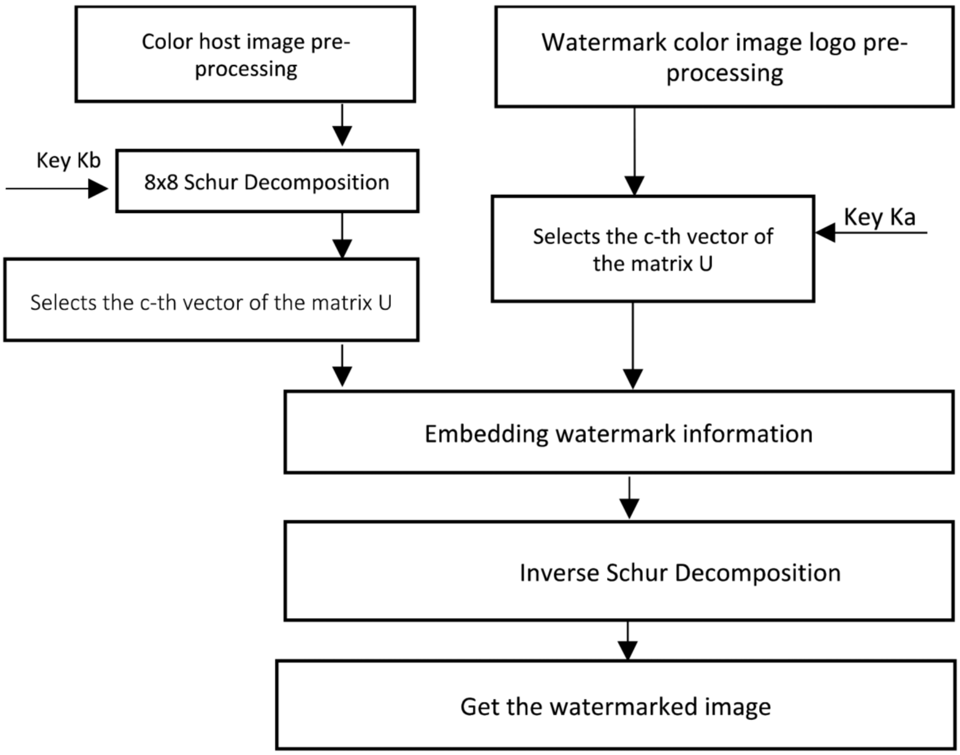


Fig. 1. Watermark embedding procedure.

decomposition. The watermark is inserted and extracted without the need for the original image. The schur decomposition method is employed to obtain matrix U and matrix D of schur decomposition. The scheme exhibits high resilience against a wide range of image attacks and image processing attacks, including compression, filtering, and other forms of manipulation. This approach utilizes a fusion of schur decomposition to achieve resilience of the watermark.

A scheme by Maqableh et al. [17] presented audio watermarking based on DCT and schur decomposition. The scheme provided high-payload-insertion-capacity audio watermarking, the watermarks in a manner that is undetectable to the human ear, hence preserving the audio quality without any compromise. Furthermore, the scheme produced a high level of resilience against a wide range of attacks, including compression, filtration, and other forms of audio processing.

Su et al. [18] presented an image watermarking scheme based on QR decomposition. A cover image is split into non-overlapping 4×4 pixel and each block is computed by using QR decomposition. The watermark is inserted based on the relation between the second row first column and the third row first column in the matrix Q. The scheme produced minimum false-positive problem for extracting watermark and it has minimum computational complexity. The results produced a good robustness performance and better invisibility.

3. Proposed watermarking method

3.1. Watermark embedding

The watermark embedding procedure is shown in Fig. 1. The host image is divided into three primary channels, specifically R (red), G (green), and B (blue). The Arnold transform is applied to permute each component watermark using the private key *Ka*. Furthermore, the pixel value of every individual watermark component is transformed into an 8-bit binary sequence to strengthen the security and resilience of the watermark. Each component of the cover image is subdivided into 8×8 pixels. In addition, to enhance security, the blocks for embedding watermark are randomly selected by using a pseudo-random sequence generated by the private key *Kb*.

The procedure of embedding watermarks is explained as follows:

Step 1: The watermark sequence is permuted using the Arnold transform with a private key.

Step 2: The selected block is performed with the following steps.

$$[R, C] = \text{randinterval}\,(HT, ST, Kb) \tag{1}$$

where R, C represents the selected rows and columns of blocks, HT denotes the total non-overlapping 8×8 blocks, *ST* denotes the selected block number, and *Kb* is the private key.

Step 3: Perform schur decomposition on H_{ij} to get $U_{i,j}$ and $D_{i,j}$ matrix of each block.

$$[U_{i,j}, D_{i,j}] = \text{schur}\ (H_{i,j}) \tag{2}$$

Step 4: Using the following equation. (3), define the column *c* of the eigenvalue maximum in $D\ i,j$ matrix.

$$c = \text{find}\ (\max(D_{i,j})) \tag{3}$$

Step 5: Embed a watermark *w* by modifying orthogonal $U_{i,j}$ as defined in the following equations (4) and (5).

$$\text{if abs } (u_{2,c}) - \text{ abs } (u_{3,c}) <= T \text{ and } w = 1,$$
$$\begin{cases} u^*_{2,c} = \text{sign}\,(u_{2,c}) * (U_{\text{avg}} + \beta * T) \\ u_{3,c} = \text{sign}\,(u_{3,c}) * (U_{\text{avg}} - (1-\beta) * T) \end{cases} \tag{4}$$

$$\text{if abs } (u_{3,c}) - \text{abs}\,(u_{2,c}) <= \text{T and } w = 0,$$
$$\begin{cases} u^*_{2,c} = \text{sign}\,(u_{2,c}) * (U_{\text{avg}} - \beta^* T) \\ u^*_{3,c} = \text{sign}\,(u_{3,c}) * (U_{\text{avg}} + (1-\beta) * T) \end{cases} \tag{5}$$

The watermark information is denoted by w. The function sign(x) reflects the sign of x, while abs(x) calculates the absolute value of x. $u_{2,c}$ * and $u_{3,c}$ * are the result of modified value of $u_{2,c}$ and $u_{3,c}$ respectively. β represents the embedding coefficient, *T* is the threshold value, and *U* avg is an average value of $u_{2,c}$ and $u_{3,c}$.

Step 6: The inverse schur decomposition is obtained by following equation:

$$H^*_{i,j} = U^*_{i,j} D_{i,j} U^{*T}_{i,j} \tag{6}$$

Step 7: Repeat Step 3 to Step 6 until all the watermark information was embedded into the host image.

Step 8: Merge the watermarked component images R, G, and B to get the watermarked image.

3.2. Watermark extraction

The extraction process is used to retrieve the watermark in binary form from the watermarked image. Fig. 2 illustrates the extraction procedure.

Step 1: The watermarked image is divided into three components namely R (red), G (green), and B (blue). Each channel is partitioned into 8×8 pixels.

Step 2: Applying Schur decomposition to *watermarked* $H_{i,j}$ blocks and get matrix $U_{i,j}$, $D_{i,j}$. Subsequently, and a pseudo-random sequence specified by the private key *Kb*, certain watermark blocks $H_{i,j}$ are chosen from the previously created blocks.

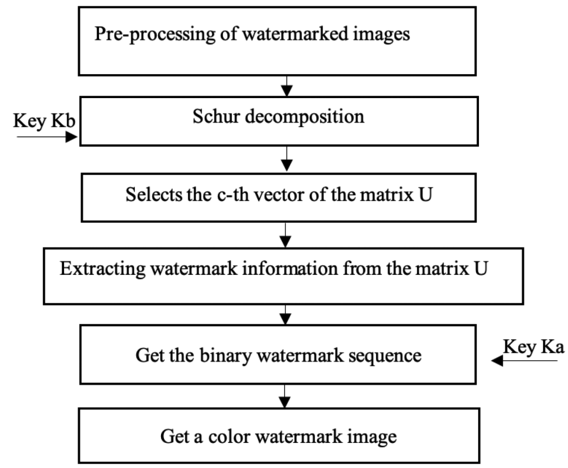


Fig. 2. Procedure watermark extraction.

Step 3: Determine the *c* column of the orthogonal matrix *U*.

Step 4: Extract the watermark by following rules:

$$w^* = \begin{cases} 0, & \text{if} \quad u^*_{2,c} > u^*_{3,c} \\ 1, & \text{if} \quad u^*_{2,c} \le u^*_{3,c} \end{cases} \tag{7}$$

Step 5: Repeat from Step 2 to Step 4 until all the watermark bits are extracted. All successfully extracted bit is computed by inverse-Arnold transform using a private key *Ka*.

Step 6: The extracted watermark is obtained and merged the extracted watermarks from the three components (R, G, and B).

Step 7: Receive the extracted watermark image

4. Evaluation

4.1. Structural Similarity Index (SSIM)

The perceptual structural similarity index (SSIM) is employed to quantify imperceptibility of the watermarked image. The SSIM can be computed by [19, 20]:

$$SSIM(o, w) = l(o, w)\ c(o, w)\ s(o, w) \tag{8}$$

$$l(o, w) = \frac{2\mu_o\mu_w + C_1}{\mu_o^2 + \mu_w^2 + C_1} \tag{9}$$

$$c(o, w) = \frac{2\sigma_o\sigma_w + C_2}{\sigma_o^2 + \sigma_w^2 + C_2} \tag{10}$$

$$s(o, w) = \frac{\sigma_{ow} + C_3}{\sigma_o\sigma_w + C_3} \tag{11}$$

Table 1. Attack types.

Attacks	Description
Blurring	Blurring is used to partially obscure the watermark image region by reducing the clarity and sharpness of the watermark in the image.
Gaussian Noise 0,1 dan 0,3	Gaussian Noise is used to disturb or obscure the watermark inserted in the image by adding noise components that have Gaussian characteristics.
Median 2×2 dan 3×3	Median filter is used to blur or distort image details by replacing the pixel value with the median value of its surroundings.
Salt & Pepper Noise (2%) dan (10%)	Salt & Pepper noise is used to disturb or damage the watermark that has been inserted in the image. This noise can cause image pixels to become distorted and disrupt the visual quality of the image.
Sharpening 0.2 dan 1.0	Sharpening is used to enhance its clarity or visual sharpness. The purpose of this attack is to increase the details visible in the image and make it appear sharper.
JPEG 30 dan 90	JPEG compression with quality factors can change the pixel intensity distribution and compromise the presence and integrity of the watermark.
JPEG 2000 (5:1) dan 10:1	JPEG 2000 can change the pixel intensity distribution.
Scaling (4) dan (1/4)	The scaling image changes the image size by enlarging or reducing its dimensions. This can be done using various interpolation techniques to increase the resolution or decrease the size of the image.

where *l(o,w)* is the structural component (luminance) that measures the similarity of intensity patterns (mean value), *c(o,w)* is the contrast component that measures the similarity of contrast between the two images and *s(o,w)* is the structural component that reflects the similarity in texture distribution between the two images.

4.2. Normalized Correlation (NC)

To measure the robustness of the proposed scheme, the experiments simulated different attacks, and the extracted watermark against the attack is measured by using NC and BER. NC and BER are defined by [21, 22]:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)\cdot W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}^{M}\sum_{j=1}^{N} W'(i,j)^2}} \quad (12)$$

$$\mathrm{BER} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)\oplus W'(i,j)}{\mathrm{M}\times\mathrm{N}} \quad (13)$$

where *W(i,j)* represents original watermark, *W'(i,j)* denotes the extracted watermark, *M* and *N* denote the row and column sizes of the watermark image. A perfect match between the two watermarks is represented by a value of 1, while no connection is shown by a value of 0. The range value of NC in between 0 and 1. The highest NC value means that the extracted watermark is closer to the original watermark.

4.3. Types of image attacks

An image that has been embedded with a watermark can be altered by some modification and diverse forms of attacks, such as added noise, filtered image and compressed image. Robustness performance is measured to assess the strength of the embedded watermark [16]. Therefore, it is crucial to expose the image to several attack scenarios. These types of attack are used to evaluate the durability of the watermark within the image when subjected to modifications. The various attacks are explained in Table 1. The sample images for evaluating the proposed scheme is shown in Fig. 3.

5. Experimental results and analysis

5.1. Perceptual quality

In the imperceptible test, the original image is embedded with the watermark to measure the similarity between the original image and watermarked image. The imperceptible known perceptual quality of watermarked images are evaluated for the schur decomposition with the size of 4×4 pixels and 8×8 pixels. The experiments computed the average SSIM values for all watermarked images. Based on the results, the proposed scheme successfully accomplishes embedding and extracting the watermark image. According to Table 2, the best location for embedding watermark by examining the relationship between orthogonal *U* on 4×4 blocks are located in CC(U_2,U_4). The SSIM value of the scheme by Su and Chen [15] is 0.989. The proposed scheme investigated the relationship between orthogonal *U* on 8×8 blocks, which are located in CC(U_2,U_6). The SSIM value of the proposed scheme achieved 0.9951, which indicates that C(U_2,U_6) is best location for embedding the watermark image for 8×8 schur decomposition. This indicates that the values in the second row and the sixth row of the U matrix in the c-th column achieved highest imperceptibility than the scheme by Su and

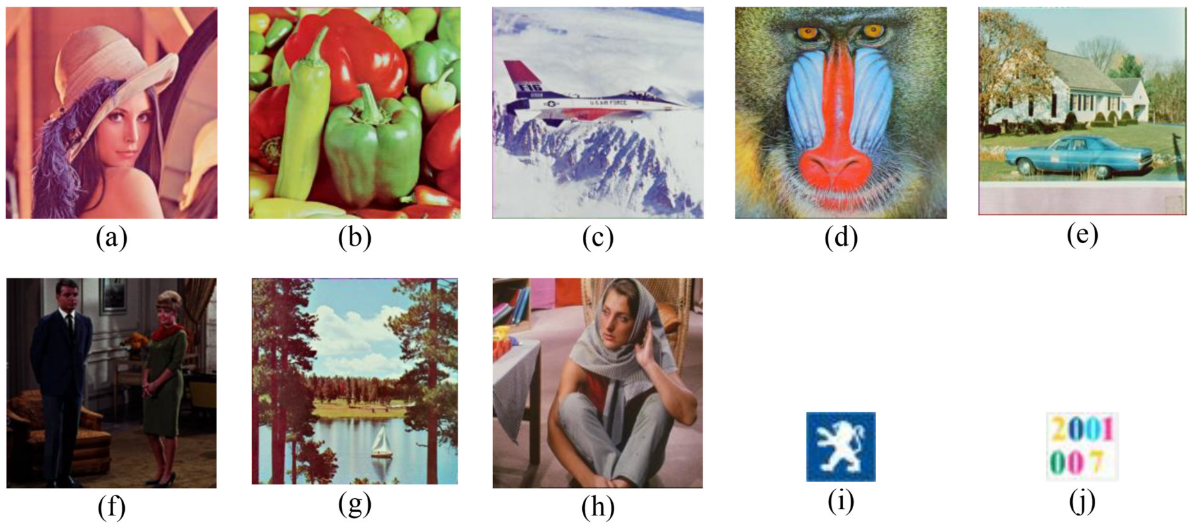


Fig. 3. Original host images: (a) Lena, (b) Peppers, (c) F-16, (d) Baboon, (e) House, (f) Couple, (g) Sailboat, (h) Barbara; Original watermark logo: (e) Peugeot, (f) 8-color watermarks.

Table 2. The SSIM value obtained from the embedding on the *U* orthogonal of Schur decomposition in 4×4 block selection.

Image	$CC(U_1, U_2)$	$CC(U_1, U_3)$	$CC(U_1, U_4)$	$CC(U_2, U_3)$	$CC(U_2, U_4)$	$CC(U_3, U_4)$
Lena	0.993	0.989	0.989	0.988	0.996	0.991
Peppers	0.977	0.967	0.967	0.965	0.984	0.966
F16	0.990	0.986	0.986	0.980	0.996	0.986
Baboon	0.974	0.963	0.963	0.957	0.981	0.962
House	0.996	0.994	0.994	0.994	0.998	0.995
Couple	0.929	0.905	0.905	0.898	0.968	0.910
Sailboat	0.990	0.984	0.984	0.981	0.996	0.983
Barbara	0.991	0.984	0.984	0.980	0.995	0.984
Average	0.980	0.971	0.971	0.968	0.989	0.972

Chen [15]. The SSIM value of the proposed scheme is listed in Table 3.

5.2. Robustness performance under various attacks

In the experiments, the watermarked images are tested under various types of attack. The proposed scheme is tested for two watermark logos. The image of “Lena” is tested with different types of attack to measure the robustness performance. Table 4 shows the robust performance of the proposed scheme for two different watermark logos.

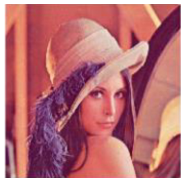
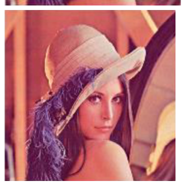
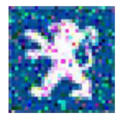
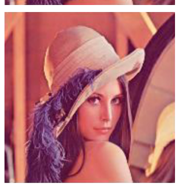
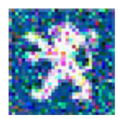
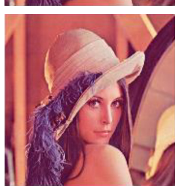
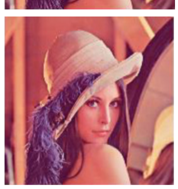
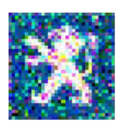
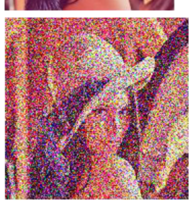
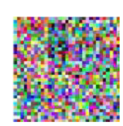
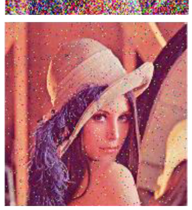
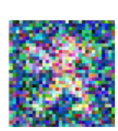
5.3. Computational time

The experiments were conducted on the computer with the processor Apple M2, memory of 8GB, OS Ventura 13.5, and software MATLAB R2023b. The

Table 3. The SSIM value obtained from the embedding on the *U* orthogonal of Schur decomposition in 8×8 block selection.

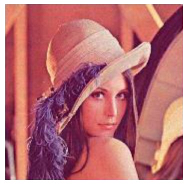
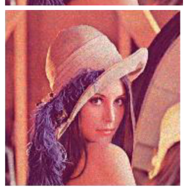
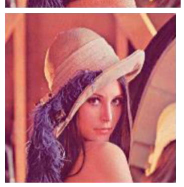
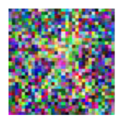
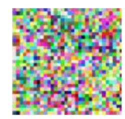
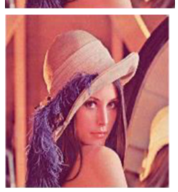
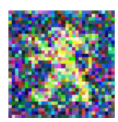
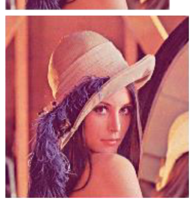
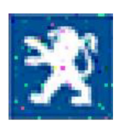
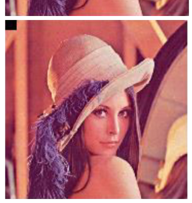
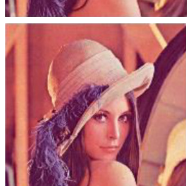
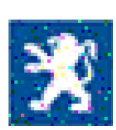
Image	$CC(U_2, U_3)$	$CC(U_2, U_4)$	$CC(U_2, U_5)$	$CC(U_2, U_6)$	$CC(U_3, U_4)$	$CC(U_3, U_5)$
Lena	0.9982	0.9981	0.9989	***0.9990***	0.9973	0.9974
Peppers	0.9881	0.9883	0.9862	***0.9890***	0.9883	0.9877
F16	0.9992	0.9990	0.9988	***0.9996***	0.9992	0.9991
Baboon	1.0000	1.0000	1.0000	***1.0000***	1.0000	1.0000
House	0.9992	0.9997	0.9988	***0.9998***	0.9993	0.9998
Couple	0.9605	0.9638	0.9709	***0.9733***	0.9648	0.9725
Sailboat	1.0000	1.0000	1.0000	***1.0000***	1.0000	1.0000
Barbara	1.0000	1.0000	1.0000	***1.0000***	1.0000	1.0000
Average	0.9932	0.9936	0.9942	***0.9951***	0.9936	0.9946

Table 4. The visual extracted watermark under various attacks.

Attack	Watermarked Image	Extracted Watermark Image (Peugeot)	NC	Extracted Watermark Image (8-color)	NC
No attack			0.9985		0.0073
Median Filtering 3*3			0.9657		0.2689
Median Filtering 5*5			0.9387		0.3464
Wiener Filtering 3*3			0.9729		0.2495
Wiener Filtering 5*5			0.934		0.3671
Gaussian Noise 0.1			0.8052		0.4851
Gaussian Noise 0.3			0.7625		0.4822
S&P Noise 0.02			0.9467		0.3577
S&P Noise 0.1			0.8501		0.4597

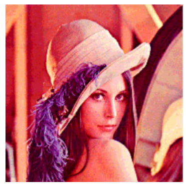
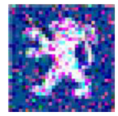
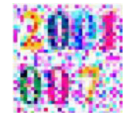
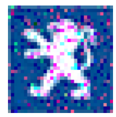
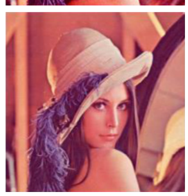
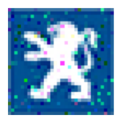
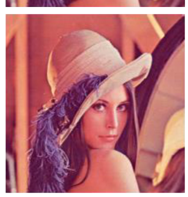
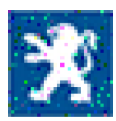
(*continued on next page*)

Table 4. Continued.

Attack	Watermarked Image	Extracted Watermark Image (Peugeot)	NC	Extracted Watermark Image (8-color)	NC
Speckle Noise 0.001			0.9991		0.0079
Speckle Noise 0.005			0.9989		0.0115
JPEG Compression 25			0.7614		0.4813
JPEG Compression 50			0.8259		0.4392
Resize Image *2*0.5			0.9946		0.0645
Resize Image *2*0.25			0.9951		0.057
Cut 64*64 pixel			0.9963		0.0133
JPEG2000:5			0.9987		0.0126
JPEG2000:10			0.9901		0.1135

(*continued on next page*)

Table 4. Continued.

Attack	Watermarked Image	Extracted Watermark Image (Peugeot)	NC	Extracted Watermark Image (8-color)	NC
Histogram Equation 10			0.9317		0.3154
Histogram Equation 20			0.9678		0.2184
Motion Blur 0.2			0.9919		0.103
Motion Blur 0.6			0.9919		0.103

experiments used images with a size of 1024×1024 pixels. Table 5 shows an average computational time for embedding and extracting watermark. The proposed scheme required a computational time of 0.3 second for embedding process and 0.26 second for extracting the watermark.

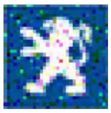
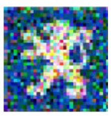
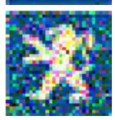
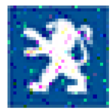
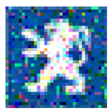
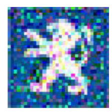
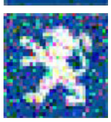
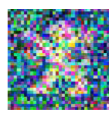
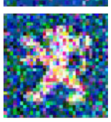
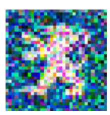
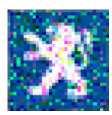
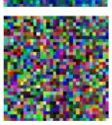
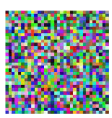
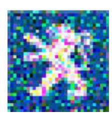
The experimental result was compared to the existing scheme in terms of robustness performance. The robustness comparisons among existing schemes by Su et al. [18] and Su & Chen [15] are shown in Table 6. The visual comparison of the extracted watermark and NC value of the extracted watermark under various attacks are listed in Table 6. In this comparison, the watermark image of "Peugeot" is used to visualize under six types of attack. The proposed method shows a high robustness performance compared to the existing schemes especially under median filter and compression.

According to Table 6, the proposed scheme achieved a highest NC value of about 0.9982 under JPEG2000 compression. It indicated that the embedded watermark has stronger resistance than the existing watermarking schemes. However, the proposed scheme slightly lower of NC value under noise addition, such as salt & pepper. The proposed scheme showed a significant improvement on the extracted watermark when the watermarked image was attacked by median filter. The proposed scheme has shown significant visual quality of the extracted watermark under median filter. The proposed scheme can achieve higher NC value of about 0.96 than the scheme by Su et al. [18] and Su & Chen [15]. Furthermore, it demonstrates that the proposed scheme effectively preserves the visual integrity of the retrieved watermark, ensuring that the watermark information remains dependable even when subjected to different types of attack. The proposed

Table 5. Computational time for embedding and extracting watermark.

Image	Embedding time (in seconds)	Extracting time (in seconds)
Lena	0.4268	0.2670
Peppers	0.3392	0.2631
F16	0.3374	0.2688
Baboon	0.3317	0.2745
House	0.3272	0.2623
Couple	0.3199	0.2573
Sailboat	0.3283	0.2659
Barbara	0.3541	0.2639

Table 6. Comparation NC and BER value of the existing scheme.

	Lena Image								
	Watermark Image			NC Value			BER Value		
Attacks	Su et al. [18]	Su & Chen [15]	Proposed	Su et al. [18]	Su & Chen [15]	Proposed	Su et al. [18]	Su & Chen [15]	Proposed
JPEG2000 (5:1)				0.9803	0.9867	**0.9982**	0.1918	0.1290	**0.0127**
JPEG2000 (10:1)				0.9081	0.9219	**0.9925**	0.4016	0.3856	**0.1135**
Salt and Peppers Noise(2%)				**0.9904**	0.9642	0.9493	**0.1147**	0.2949	0.3576
Salt and Peppers Noise(10%)				**0.9362**	0.8186	0.8478	**0.3312**	0.4476	0.4550
Median Filter (2×2)				0.8927	0.8891	**0.9612**	0.4316	0.4331	**0.2689**
Median Filter (3×3)				0.6479	0.7005	**0.9325**	0.4878	0.4879	**0.3464**

scheme demonstrates superior performance in terms of robustness and visual quality of watermark extraction, as evidenced by the comparative analysis with the existing scheme as listed in Table 6.

6. Conclusion

This study proposed an embedding watermark scheme by examining the relationship between orthogonal U on 8×8 of schur decomposition. This research has examined the possibility of embedding watermarks on the schur decomposition. An investigation has been conducted to investigate the correlation between the c-th column of the U matrix in Schur Decomposition. The embedding watermark by examining the relation between U_2 and U_6 of the schur decomposition. achieved the highest SSIM value of the watermarked image. The experiments have been tested under various image processing attacks, such as geometrical attacks, noise addition, median filter and JPEG compression to assess its resilience. The embedded watermark can be extracted without requiring the original cover image. The experimental results demonstrate that the proposed embedding watermark produces high imperceptibility of the watermark insertion and high resilience against various attacks. The suggested embedding watermark technique exhibits superior to the existing watermarking schemes when the watermarked image was compressed and filtered by median. In future study, the proposed approach can be applied to video watermarking.

Acknowledgement

The authors would like to thank the Ministry of Higher Education for providing financial support under Universiti Malaysia Pahang Al-Sultan Abdullah under Internal Research Grant RDU233003

Funding

UMPSA Internal Research Grant RDU233003.

Conflicts of interest

The author declares no conflict of interest.

References

1. F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *Vis. Comput.*, vol. 36, no. 1, pp. 19–37, 2020. doi: 10.1007/s00371-018-1567-x.
2. A. Alzahrani, "Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD," *Appl. Bionics Biomech.*, vol. 2022, pp. 1–13, 2022. doi: 10.1155/2022/5271600.
3. M. A. Ur Rahaman, M. Safoora Begum, J. N. Sai Krishna, A. Teja Mani Raju, R. K. Tata, and G. Swain, "Digital Watermarking Analysis Using Data Security," in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India: IEEE, Mar. 2023, pp. 486–489. doi: 10.1109/ICACCS57279.2023.10113111.
4. M. Ali, "Robust Image Watermarking in Spatial Domain Utilizing Features Equivalent to SVD Transform," *Appl. Sci.*, vol. 13, no. 10, p. 6105, May 2023. doi: 10.3390/app13106105.
5. M. A. Hameed, O. A. Abdel-Aleem, and M. Hassaballah, "A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 5, pp. 4639–4657, 2023. doi: 10.1007/s12652-022-04366-y.
6. X. Zhou, H. Zhang, and C. Wang, "A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 3, p. 77, 2018. doi: 10.3390/sym10030077.
7. H. Karajeh, T. Khatib, L. Rajab, and M. Maqableh, "A robust digital audio watermarking scheme based on DWT and Schur decomposition," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 18395–18418, 2019. doi: 10.1007/s11042-019-7214-3.
8. S. Singh, H. Singh, A. Gehlot, and J. Kaur, Gagandeep, "IR and visible image fusion using DWT and bilateral filter," *Microsyst. Technol.*, vol. 29, no. 4, pp. 457–467, 2023. doi: 10.1007/s00542-022-05315-7.
9. J. Wang, D. Wu, L. Li, J. Zhao, H. Wu, and Y. Tang, "Robust periodic blind watermarking based on sub-block mapping and block encryption," *Expert Syst. Appl.*, vol. 224, p. 119981, 2023. doi: 10.1016/j.eswa.2023.119981.
10. Y. Sun, Q. Su, S. Chen, and X. Zhang, "A double-color image watermarking algorithm based on quaternion Schur decomposition," *Optik*, vol. 269, p. 169899, 2022. doi: 10.1016/j.ijleo.2022.169899.
11. K. Fares, A. Khaldi, K. Redouane, and E. Salah, "DCT & DWT based watermarking scheme for medical information security," *Biomed. Signal Process. Control*, vol. 66, p. 102403, 2021. doi: 10.1016/j.bspc.2020.102403.
12. A. Tiwari and V. K. Srivastava, "Image watermarking techniques based on Schur decomposition and various image invariant moments: a review," *Multimed. Tools Appl.*, 2023. doi: 10.1007/s11042-023-16109-y.
13. S. Mehraj, S. Mushtaq, S. A. Parah, K. J. Giri, and J. A. Sheikh, "A robust watermarking scheme for hybrid attacks on heritage images," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 6, pp. 7367–7380, 2023. doi: 10.1007/s12652-022-04445-0.
14. W. Hao, R. Xie, Q. Du, J. Wang, and W. Zhang, "Large-capacity fragile watermarking scheme for color images based on prime number distribution theory," *Signal Image Video Process.*, vol. 18, no. 1, pp. 953–960, 2024. doi: 10.1007/s11760-023-02753-2.
15. Q. Su and B. Chen, "An improved color image watermarking scheme based on Schur decomposition," *Multimed. Tools Appl.*, vol. 76, no. 22, pp. 24221–24249, 2017. doi: 10.1007/s11042-016-4164-x.
16. L.-Y. Hsu and H.-T. Hu, "A Reinforced Blind Color Image Watermarking Scheme Based on Schur Decomposition," *IEEE Access*, vol. 7, pp. 107438–107452, 2019. doi: 10.1109/ACCESS.2019.2932077.
17. H. Karajeh and M. Maqableh, "An imperceptible, robust, and high payload capacity audio watermarking scheme based on the DCT transformation and Schur decomposition," *Analog Integr. Circuits Signal Process.*, vol. 99, no. 3, pp. 571–583, 2019. doi: 10.1007/s10470-018-1332-0.
18. Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimed. Tools Appl.*, vol. 72, no. 1, pp. 987–1009, 2014. doi: 10.1007/s11042-013-1653-z.
19. F. Ernawan and D. Ariatmanto, "An efficient adaptive scaling factor for 4×4 DCT image watermarking," *Multimed. Tools Appl.*, vol. 82, pp. 8603–8621, 2023. doi: https://doi.org/10.1007/s11042-022-14220-0.
20. F. Ernawan and D. Ariatmanto, "A recent survey on image watermarking using scaling factor techniques for copyright protection," *Multimed. Tools Appl.*, vol. 82, pp. 27123–27163, 2023. doi: https://doi.org/10.1007/s11042-023-14447-5.
21. F. Ernawan, "An improved hiding information by modifying selected DWT coefficients in video steganography," *Multimed. Tools Appl.*, vol. 83, pp. 34629–34645, 2024. doi: https://doi.org/10.1007/s11042-023-17113-y.
22. M. lebcir, S. Awang, and A. Benziane, "The optimal scaling factor based on Secant Method for image watermarking using the hybrid DTCWT-DCT domain", *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 1, pp. 237–262, 2024.