IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 14, 2021, accepted March 8, 2021, date of publication March 18, 2021, date of current version March 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3067245

An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients

FERDA ERNAWAN[1], DHANI ARIATMANTO[2], AND AHMAD FIRDAUS[1]

[1]Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, Pekan 26600, Malaysia
[2]Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Yogyakarta 55283, Indonesia

Corresponding author: Ferda Ernawan (ferda@ump.edu.my)

This work was supported by the Fundamental Research Grant Scheme (FRGS), Ministry of Education under Grant FRGS/1/2018/ICT04/UMP/02/2 and Grant RDU190117.

ABSTRACT Digital images can be easily copied or manipulated by irresponsible persons. The right property needs to be secured and protected from illegal copies and piracy. Digital watermarking is one of the solutions to protect the intellectual property of digital images. This paper proposed the adaptive scaling factor based on selected DWT-DCT coefficients of its image content. The adaptive scaling factor was generated based on the role of selected DWT-DCT coefficients against the average value of DWT-DCT coefficients. The watermark image was embedded by using a proposed set of rules that consider the adaptive scaling factor. The experimental results showed that the proposed scheme achieved high PSNR value of 47dB, SSIM value of about 0.987 and an embedded watermark resistance to several attacks in the watermarked image.

INDEX TERMS Image watermarking, adaptive scaling factor, DWT-DCT watermarking, embedding technique, flexible scaling factor.

I. INTRODUCTION

The rapid growth of internet technology has increased the amount of multimedia data being transferred over the internet. Transferring multimedia data through the internet networks requires copyright protection [1]. Some issues, such as manipulation, authentication, and illegal distribution can lead to a loss of valuable multimedia data to the owner [2]. People can share data, such as video, image, audio, and documents through internet network. Therefore, the protection of multimedia data is essential to save the distribution of intellectual property [3], [4]. Digital watermarking is an alternative solution to protect the intellectual property from illegal users. A watermark logo is inserted into the host image, whereby the watermark can be visible or invisible [5].

The embedding and extracting watermark can be done in spatial and frequency domains. The embedding watermark in spatial domain has been widely used for tamper detection and authentication [6]. The watermark is inserted directly into the host image by modifying image pixels. This technique can produce high imperceptibility, while the embedding watermark can be destroyed under various attacks [7]. Image watermarking based on frequency domain able to achieve high resistance to various attacks [8]. A scheme by Ariatmanto and Ernawan [9] presented modifying selected DCT coefficient to generate adaptive scaling factor for image watermarking. The scheme examined the impact of selected coefficients against average coefficients of its image block. The results showed that the scheme can produce a high degree of imperceptibility and robustness of a watermarked image. While, the results of the scheme have potential to be improved by using hybrid method based image watermarking.

The hybrid method is formed by combining two or more transform domains that aims to address individual modified domain defects. Researchers have presented hybrid methods to enhance watermarking performance in terms of imperceptibility and robustness. A scheme by Vo *et al.* [10] demonstrated a robust hybrid image watermarking scheme based on DCT-SVD for stereo images. The watermark was embedded in the singular value of DCT-SVD. The scheme produced a good robustness of the watermarked image against different types of attack. While, the embedding watermark into singular value of SVD produced false positive problem in the extracting watermark image.

The hybrid methods also can be presented by using three transform domains. A scheme by He and Hu [11] presented a watermarking algorithm using DWT-DCT-SVD. The scheme used a trade-off between invisibility and robustness as an embedding strength in the watermarked image. However, a trade-off between imperceptibility and robustness does not

The associate editor coordinating the review of this manuscript and approving it for publication was Mansoor Ahmed.

suitable for all image blocks. The embedding strength should consider for each image content.

This research proposed an adaptive scaling factor based on DWT-DCT for different image contents. The adaptive scaling factor was developed based on DWT-DCT coefficients of the image content itself. DWT-DCT coefficient in the middle frequency was selected since it could preserve good robustness and imperceptibility as compared to other frequencies. This study analysed the impact of selected DWT-DCT coefficients against the average DWT-DCT coefficients. The impact of DWT-DCT coefficients was used to generate an adaptive scaling factor for embedding watermark.

This research is organized as follows. Section II presents related work of embedding watermark. Section III discusses the methods in watermarking scheme. Section IV presents the proposed embedding watermark. The experimental results are shown in Section V and Section VI concludes the paper.

II. RELATED WORKS

Kumar *et al.* [12] presented the recent survey on image watermarking techniques. The hybrid transform domain techniques can enhance the imperceptibility, robustness and avoid false positive effect by SVD. The hybrid methods were able to improve robustness of the extracted watermark under image processing attacks. However, the success of hybrid schemes is to achieve the desired goals based on appropriate transform domains.

A scheme by Pandey *et al.* [13] presented embedding watermark-based DWT-SVD in image watermarking. Their scheme used an adaptive value of embedding strength generated from the perceptual tuning of the host image contents and watermark image contents. Their scheme was able to maintain the robustness and imperceptibility of the watermarked image.

A scheme by Yadav and Singh [14] presented image watermarking using the adjustable strength factor based on DWT. Their scheme provided flexibility of its strength factor that can be adjusted based on the level of image quality. Their scheme was able to achieve good robustness under various attacks. Therefore, the adaptive scaling factor gave a significant impact to the quality and robustness of the watermarked image. The usage of adaptive scaling factor is suitable for different image inputs to achieve high robustness and invisibility. Further investigation for this research is to enhance robustness while maintaining the host image quality after watermark insertion, which is generated by adaptive embedding strengths.

Another scheme by Ahmadi *et al.* [15] presented an image watermarking scheme based on DWT-SVD-PSO. The scheme utilised PSO to find the best optimal scaling factors based on the attacks test results and predefined objective function. The PSO is used for balancing the trade-off between imperceptibility and robustness. The scheme also used edge entropy and entropy for choosing embedding block regions with higher imperceptibility. The scheme achieved good imperceptibility on the watermarked image. However, the scheme robust under certain attacks such as cropped image, Gaussian filter and Gaussian noise.

Kang et al [16] presented hybrid of DCT-SVD-DWT image watermarking with optimal embedding. The cover image was split into four sub-bands using DWT. The LL sub-band is divided into 8 × 8 non-overlapping blocks. Each block is then transformed by DCT, the selected eight DCT coefficients are re-arranged into modulation matrix with two rows and two columns. The matrix is computed by SVD, then the watermark is embedded by modifying the largest singular values. The scheme achieved a good robustness of the extracted watermark against noise attacks and Gaussian filter. However, the imperceptibility performance of the scheme for the average of eight images produced PSNR value of 38.63 dB and SSIM value of 0.9662. In another word, the scheme produced significant distortion to the quality of watermarked image.

A scheme by Taha et al [17] presented adaptive watermarking algorithm using perceptual mapping model. The scheme used integer-based lifting wavelet transform to create perceptual mapping model. The scheme achieved fast embedding watermark by execution time of 1.06 second. While, the scheme produced less imperceptibility of the watermarked image with the average PSNR value of 36.31 dB and SSIM value of 0.96 for fifteen images.

Ernawan & Kabir [18] presented a watermarking scheme by modifying selected DCT coefficients with a certain rule. The coefficient pairs are modified with a threshold by considering a certain rule. The scheme finds the embedding location by using human visual characteristic. The modified entropy is used to determine the large redundant location. The watermark bits are encrypted by using Arnold chaotic map for additional security. The scheme achieved a good imperceptibility with minimum distortion. The scheme also produced high robustness performance under image processing attacks and geometrical attacks. While, the modified coefficient pairs with a threshold value may not optimal for all frequency blocks of image. The adaptive scaling factor is needed to achieve the optimal imperceptibility and robustness for different image signals.

III. METHODS

A. VARIANCE PIXELS

The experiments utilised variance pixel value to choose the embedding locations. The scheme selected embedding regions based on the highest variance pixels. The highest variance pixels indicate a high complex texture of the image, whereby the complex texture of image becomes more invisible to the human visual system [19]. The variance pixel is defined by:

$$S^2 = \sum_{i=1}^{v} \left(V_i - \bar{V}\right)^2 \frac{n_i}{N} \tag{1}$$

where v is a sequence numbers of pixels on the selected block, V_i denotes every pixel value in selected block, $\overline{V}$ denotes the average value of the selected block, n represents number

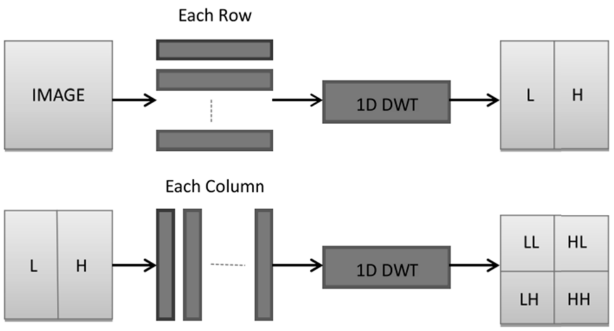

FIGURE 1. One-level decomposition of 2D DWT.

of pixels in level i and N denotes total pixel number. The variance pixel values of image blocks are sorted by descending order. The image blocks with highest variance pixels are selected by considering the length of watermark bits. x and y coordinates of selected blocks are saved into a database for extracting reference.

B. ARNOLD'S CAT MAP

The watermark needs to be secured from unauthorised users or attackers. Arnold transform provides simplicity, periodicity, and secrecy in the encryption process. Arnold's cat map is defined by [20]:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} \bmod N \tag{2}$$

where, N is the number of iterations x_{n-1} and y_{n-1} are the position of watermarks, x_n and y_n are the transformed coordinates of the scrambled image, p and q are the positive integer. The period of iterations in the Arnold transform can be utilised as a private key to scramble the watermark. By adding a secret key, it would be difficult to identify the encrypted watermark. To recover the watermarked image, the inverse Arnold transform needs the same key. Arnold transforms provides less computational time in the encryption process than other traditional ones [21].

C. DISCRETE WAVELET TRANSFORM

The DWT is a technique to transform the spatial domain into wavelets signals [22]. DWT consists of four sub-bands, in which LL is low pass approximation where is contains of the signal information, LH and HL are the vertical and horizontal detail coefficients and HH is diagonal detail coefficients. The DWT can provide perfect image reconstruction. The decomposition of a single level of two-dimensional DWT as shown in Figure 1.

D. DISCRETE CONSINE TRANSFORM

The selected blocks of DWT coefficients on the LL sub-band were computed by DCT. The DCT was defined by [23]:

$$B_{pq} = \partial_p \beta_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} \cos \frac{\pi\,(2m+1)_p}{2M} \cos \frac{\pi\,(2n+1)_q}{2N} \tag{3}$$

for p = 0, 1, 2, . . . , M − 1 and q = 0, 1, 2, . . . , N − 1 where

$$\partial_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \frac{2}{\sqrt{M}}, & p > 0 \end{cases} \quad \beta_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \frac{2}{\sqrt{N}}, & q > 0 \end{cases} \tag{4}$$

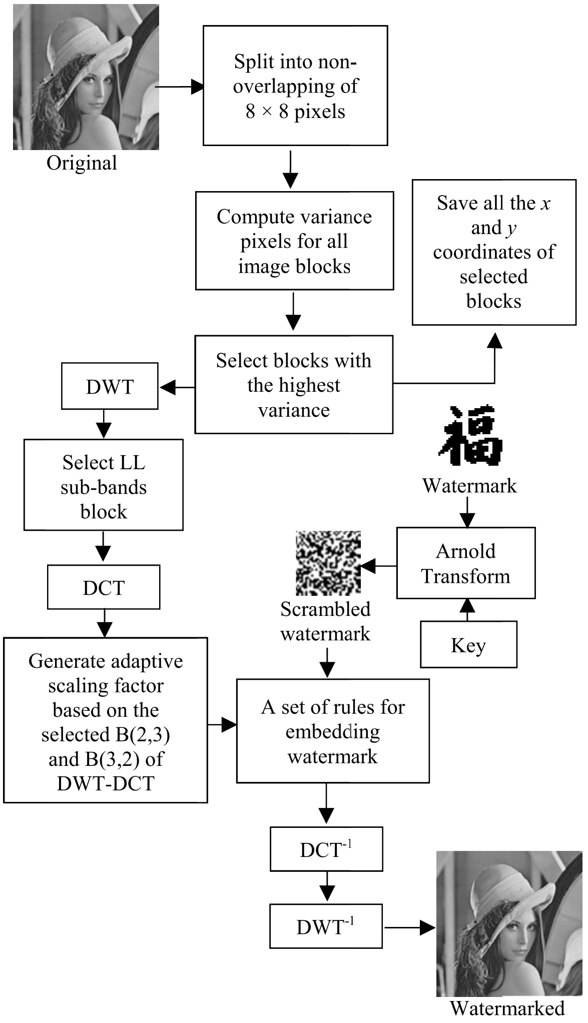
Original
Split into non-overlapping of 8 × 8 pixels
Compute variance pixels for all image blocks
Save all the x and y coordinates of selected blocks
Select blocks with the highest variance
DWT
Select LL sub-bands block
福
Watermark
Arnold Transform
Scrambled watermark
Key
DCT
Generate adaptive scaling factor based on the selected B(2,3) and B(3,2) of DWT-DCT
A set of rules for embedding watermark
DCT-1
DWT-1
Watermarked

FIGURE 2. The block diagram of the proposed embedding watermark.

IV. PROPOSED EMBEDDING WATERMARK

A. PROPOSED EMBEDDING WATERMARK

The proposed block diagram of image watermarking scheme is visualized in Figure 2.

First, a host image is split into non-overlapping blocks of 8 × 8 pixels. Each block was computed by variance pixels, the image blocks with highest variance value are selected for embedding watermark. The purpose of selecting image block with high variance pixels is to obtain the image block that less sensitive to the human eyes. The selected image blocks considered the watermark size.

The number of selected image blocks are equal to 1024 image blocks because the experiments used a binary watermark with the size of 32 × 32 pixels. The number of selected image blocks are equal to length of binary watermark bits. The coordinates of x and y of selected image blocks are saved for extracting references. The selected image blocks are transformed by one-level decomposition of discrete wavelet transform. LL sub-band of DWT coefficients was selected to be transformed by two-dimensional DCT. The embedding watermark bits were performed by using a set of embedding rules as follows:

Rules 1: calculate $P(i)$ defined by:

$$P(i) = \frac{\overline{L}(i)}{\alpha(i)} \tag{5}$$

$$\alpha(i) = \frac{\left(\left(\frac{B_{(2,3)}+B_{(3,2)}}{n}\right) + \overline{L}_{(i)}\right) \cdot n}{\overline{L}_{(i)}} \tag{6}$$

where $P(i)$ represents the value for the rules for embedding process, n is 16, $\overline{L}(i)$ represent the average of the DWT-DCT block on the LL sub-band and $\alpha(i)$ denotes the adaptive embedding strength of its image block.

Rules 2: Embedding watermark by using following algorithm:

Algorithm 1: Embedding Watermark

```
Input: $P$, $\alpha$, $B(i) = \{B_{(2,3)}, B_{(3,2)}\}$
u = 0;
for $i = 1:2$
    if $u \le size\_wm$ && $(P(i) - B(i)) > \alpha(i)$ &&
        $wt(u) == 0$ then
        $Q(i) = P(i) - \alpha(i)$;
        $u = u + 1$;
    else if $u \le sw$ && $(B(i) - P(i)) > \alpha(i)$ &&
        $wt(u) == 1$ then
        $Q(i) = P(i) + \alpha(i)$;
        $u = u + 1$;
    else
        $Q(i) = B(i)$;
    end (if)
end (for)
Output: The inserted binary logo in the watermarked
        image
```

where, Q denotes the modified DWT-DCT coefficients, B denotes the selected DWT-DCT coefficients, wt represents the watermark, $size\_wm$ denotes as watermark size and α is adaptive scaling factors.

In order to generate adaptive scaling factor, the selected pairs of DWT-DCT coefficients are chosen to calculate the impact of those coefficients against its image block. The selected $B(2,3)$ and $B(3,2)$ of DWT-DCT coefficients contributed less distortion to the image reconstruction. Therefore, the modifying the selected pair of $B(2,3)$ and $B(3,2)$ of DWT-DCT coefficients are suitable for embedding watermark. The watermark image is encrypted by Arnold transform before embedding watermark. The adaptive embedding strength for its image block is given in Equation (6).

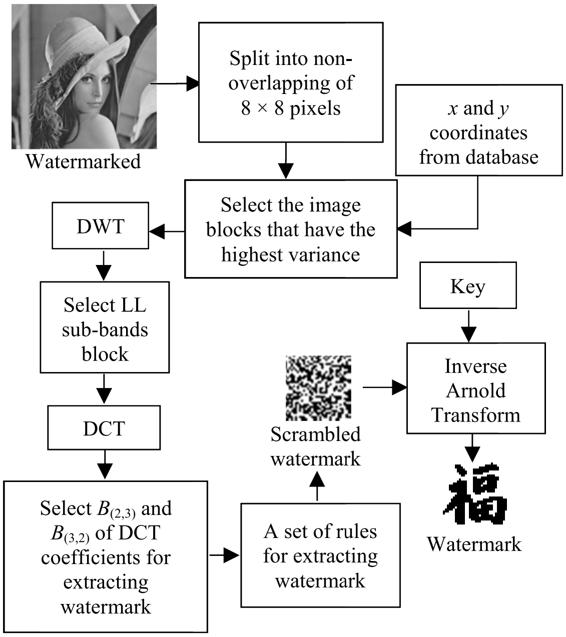
Watermarked
Split into non-overlapping of 8 × 8 pixels
x and y coordinates from database
DWT
Select the image blocks that have the highest variance
Key
Select LL sub-bands block
Inverse Arnold Transform
DCT
Scrambled watermark
Watermark
Select $B_{(2,3)}$ and $B_{(3,2)}$ of DCT coefficients for extracting watermark
A set of rules for extracting watermark

FIGURE 3. Extracting procedure.

If $P(i)$-$B(i)$ is greater than adaptive scaling factor $\alpha(i)$ of its image block and watermark bit equal to 0, $B(i)$ of DWT-DCT coefficient is replaced by value of $P(i) - \alpha(i)$. Else if $B(i)$-$P(i)$ is greater than adaptive scaling factor $\alpha(i)$ of its image block and watermark bit equal to 1, $B(i)$ of DWT-DCT coefficient is replaced by value of $P(i) + \alpha(i)$. Else the $B(i)$ of DWT-DCT coefficient is maintained. Watermark is inserted accordingly embedding rule and length of watermark bits.

B. WATERMARK EXTRACTION

The extracting watermark is visualized in the block diagram as shown in Figure 3. First, the watermarked image is split non-overlapping into 8 × 8 pixels. x and y coordinates from database are used to choose the image blocks. The selected image blocks are transformed by DWT. LL sub-band of DWT are transformed by two-dimensional DCT.

Select pair coefficient $B(2,3)$ and $B(3,2)$ of DWT-DCT in order to extract watermark image. The extracted watermark is obtained from a set of rules by considering selected pair coefficient. The watermark bits were recovered by using a set of rules as follows:

Rules 1: Calculate $P_w(i)$ defined by:

$$P_w(i) = \frac{\overline{L}_w(i)}{\alpha_w(i)} \tag{7}$$

where $P_w(i)$ represents the value for the extraction rules of the watermarked image, $\overline{L}_w(i)$ represent the average of the DWT-DCT block of the watermarked image and $\alpha_{\mathrm{w}}(i)$ denotes the adaptive embedding strength.

Rules 2: Extract the watermark using Algorithm 2 as follows:

Algorithm 2: Extracting Watermark

```
Input: $B_w(i) = \{B_{(2,3)}, B_{(3,2)}\}, P_w(i)$
u = 0;
for $i = 1 : 2$
    if $u \leq size\_wtm$ then
        if $B_w(i) > P_w(i)$ then
            $wt\ (u) = 1$
            $u = u + 1;$
        else
            $wt\ (u) = 0;$
            $u = u + 1;$
        end (if)
    end (if)
end (for)
Output: Extracted watermark
```

TABLE 1. The abbreviation of various attacks.

Abbreviation	Attacks description
CC25%	Center cropping 25%
CC50%	Center cropping 50%
GF 3×3	Gaussian low-pass filter with a kernel size of 3×3
GF 5×5	Gaussian low-pass filter with a kernel size of 5×5
GN 0.03	Gaussian noise by mean 0 and variance of 0.03
GN 0.003	Gaussian noise by mean 0 and variance of 0.003
HE	Histogram Equalization
JPEGQ40	JPEG compression with quality of 40
JPEGQ50	JPEG compression with quality of 50
MF 3×3	Median filter with a kernel size of 3×3
PN	Poisson noise
SH	Sharpening
SN 0.03	Speckle noise with density 0.03
SN 0.3	Speckle noise with density 0.3
SPN 0.002	Salt & pepper noise with density of 0.002

TABLE 2. Imperceptibility of the proposed watermarking scheme for ten images.

Host image	ARE	PSNR	SSIM
Lena	0.527	47.176	0.987
Sailboat	0.535	46.918	0.985
Baboon	0.517	46.116	0.990
Airplane	0.530	47.024	0.984
Pepper	0.528	47.158	0.987
House	0.520	47.300	0.985
Boat	0.512	47.404	0.986
Barbara	0.520	47.352	0.989
office	0.541	47.365	0.989
stadium	0.516	47.311	0.984
Average	0.525	47.112	0.987

where B represents the selected DWT-DCT coefficients, the watermark bits denotes by *wt* and *size_wtm* represents the length of watermark bits.

The imperceptibility was evaluated by a quantitative measurement in the watermarked image. Imperceptibility means a change in the watermarked quality and the distortion of the host image after embedding a watermark image These experiments used SSIM, ARE, MSE, and PSNR to evaluate the imperceptibility of the embedding watermark. The SSIM was used to evaluate the similarity between the original host image and the watermarked image [24]. The SSIM index is defined by the following [25]:

$$SSIM(x, y) = [l(x, y)]^{\alpha} \cdot [c(x, y)]^{\beta} \cdot [s(x, y)]^{\gamma} \tag{8}$$

where $\alpha > 0$, $\beta > 0$, $\gamma > 0$. ARE was used to evaluate the reconstruction error of the embedding watermark. ARE is defined by [26], [27]:

$$ARE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{i=1}^{N} |f(k, l) - g(k, l)| \tag{9}$$

where f denotes as original image and g represents the watermarked image, and M, N denote as the row and column size of the image. The extracted watermark image under various attacks is measured by bit error rate (BER). The BER was used to measure the error rate of decoded watermark bits [28]. BER is defined as the ratio of incorrect bits to correct bits and it was determined by comparing the obtained bits with the original embedded bits after watermark extraction. The BER is defined by [29], [30]:

$$BER = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i, j) \oplus W^*(i, j)}{M \times N} \tag{10}$$

where, $W^*(i, j)$ is the watermark recovery and $W(i, j)$ is the original watermark. M and N denote the row and column sizes of the watermark image. The proposed watermarking scheme was tested under various image processing attacks e.g. Gaussian low-pass filter (GLF), median filter (MF), average filter (AF), wiener filter (WF), Gaussian noise (GN), salt & pepper (SP), speckle noise (SN), histogram equalisation (HE) and sharpening (SH). The proposed scheme was also tested under geometrical attacks e.g. cropping centered (CC), cropping row (CR), cropping column (CCL) and scaling (SC). The watermarked image was also compressed by JPEG and JPEG2000 compression. The abbreviation of various attacks is listed in Table 1.

V. THE EXPERIMENTAL RESULTS

The experiments test on eight grayscale images from USC-SIPI image database [31] and two real images taken by DSLR Nikon D7200. The visual ten grayscale images and a watermark image are shown in Figure 4.

The proposed watermarking scheme was performed using MATLAB R2014a, Intel®Core$^{\text{TM}}$i7-7700 CPU @ 3.60 GHz, memory 16GB. The imperceptibility performance of the proposed watermarking scheme is shown in Table 2.

The experiments used fourteen grayscale images with size of 512 × 512 pixels to evaluate the proposed watermarking

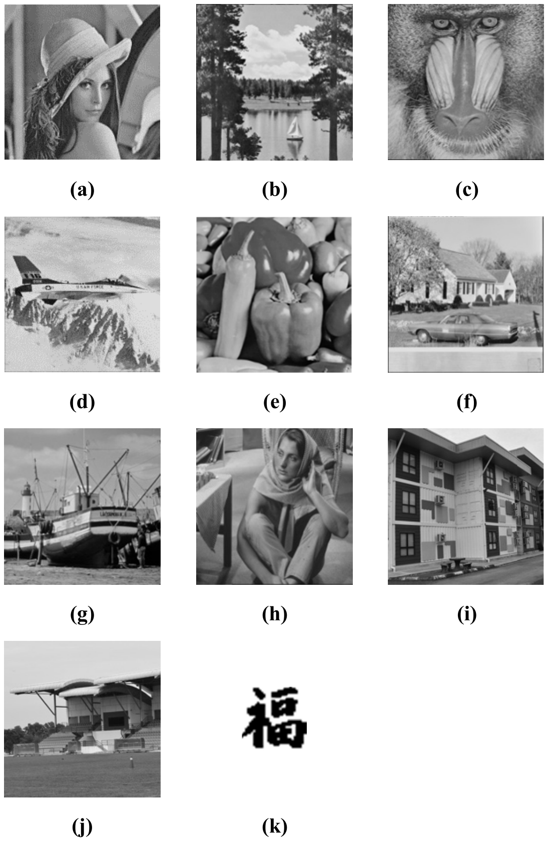

FIGURE 4. (a) Lena, (b) Sailboat, (c) Baboon, (d) Airplane, (e) Pepper, (f) House, (g) Boat, (h) Barbara, (i) office, (j) Stadium, (k) watermark image.

TABLE 3. Comparison of NC values under various attacks.

Image attacks	Lena			Sailboat		
	Ernawan and Kabir [18]	Ahmadi et a [15]	Proposed scheme	Ernawan and Kabir [18]	Ahmadi et a [15]	Proposed scheme
No Attack	1.000	1.000	**1.000**	1.000	1.000	**1.000**
GF 3×3	0.995	0.998	**1.000**	0.998	0.985	**1.000**
GF 5×5	0.995	**1.000**	0.966	**0.998**	0.972	0.942
GN0.003	0.783	0.818	**0.886**	0.765	0.861	**0.877**
GN0.03	0.527	**0.846**	0.669	0.517	**0.843**	0.638
SH	1.000	1.000	**1.000**	1.000	0.995	**1.000**
SPN0.002	0.951	0.922	**0.976**	**0.976**	0.924	0.975
MF 3×3	0.985	0.998	**0.999**	0.988	0.985	**1.000**
MF 5×5	0.648	0.851	**0.953**	0.652	0.835	**0.942**
HE	1.000	1.000	**1.000**	0.999	0.982	**1.000**
JPEGQ40	0.577	0.992	**1.000**	0.539	0.970	**1.000**
JPEGQ50	0.509	0.998	**1.000**	0.503	0.985	**1.000**
JPEGQ60	0.806	0.995	**1.000**	0.765	0.990	**1.000**
SN 0.03	**1.000**	0.866	0.723	**0.941**	0.909	0.676
SN 0.3	**0.977**	0.686	0.702	**0.806**	0.618	0.669
PN	0.493	**0.980**	0.897	0.462	**0.980**	0.842
CC25%	0.541	**1.000**	0.995	0.561	**1.000**	0.912
CC50%	0.712	**1.000**	0.975	0.726	**1.000**	0.713

scheme. A binary watermark image with the size of 32×32 pixels is used to be inserted into the cover image. The proposed watermarking scheme produced the average SSIM values of 0.987. The proposed scheme also achieved higher the average PSNR values of 47.112 dB than Ahmadi et al [15] with the result of average PSNR value about 43.690 dB. The average reconstruction error of the watermarked image was about 0.525. The NC comparison among schemes by Ernawan and Kabir [18], Ahmadi et al [15] and the proposed scheme is shown in Table 3.

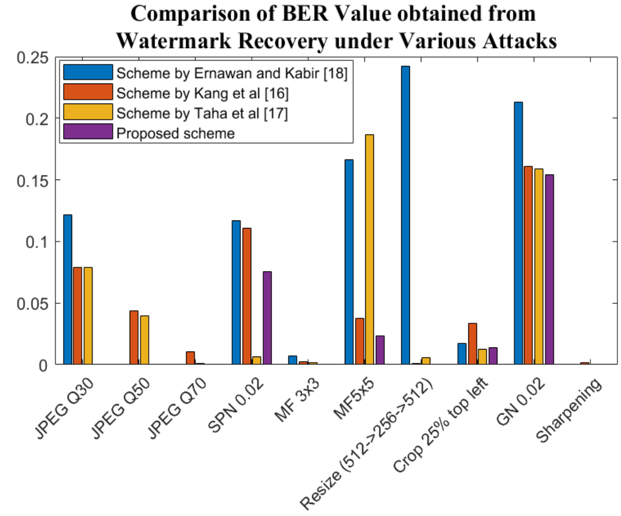

FIGURE 5. Comparison of BER value between schemes by Ernawan and Kabir [18], Kang et al [16], Taha et al [17] and proposed scheme.

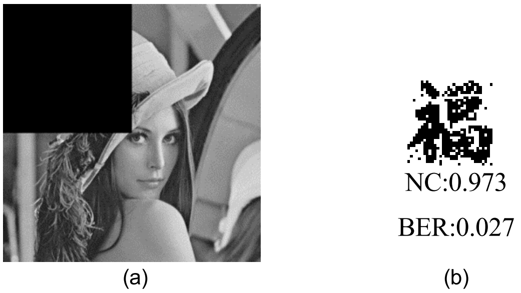

FIGURE 6. Result under cropping attack and extracted watermark (a) cropped watermarked image 25 %, (b) extracted watermark against 25% cropped watermarked image.

Referring to Table 3, the proposed scheme produced higher NC value compared with schemes by Ernawan and Kabir [18], Ahmadi et al [15] except under Gaussian filter [5,5], Gaussian noise 0.03, salt and pepper, and cropping attack. If the NC value was closer to 1, it means that the watermark recovery was closer to the original watermark image. The proposed scheme outperformed schemes by Ernawan and Kabir [18], Ahmadi et al [15] in terms of NC value under Gaussian filter [3,3], Gaussian noise 0.033, sharpening, median filter, histogram equalization and JPEG compression. The proposed scheme produced slightly less robustness under cropped image, but significant destroyed under salt & pepper, as listed in Table 3.

The proposed scheme was also compared to the other schemes by adding JPEG compression, salt & pepper (SPN), Median filter (MF), Resize image, Crop image, Gaussian noise (GN) and sharpening to the watermarked image. The visual bar of BER values obtained from the schemes by Ernawan and Kabir [18], Kang et al [16], Taha et al [17] and the proposed scheme is shown in Figure 5.

TABLE 4. Comparison of NC and BER Values under various image attacks between Scheme by Ernawan, kang and Proposed scheme.

Various image attacks	Lena						Peppers					
	Ernawan and Kabir [18]		Kang et al [16]		Proposed scheme		Ernawan and Kabir [18]		Kang et al [16]		Proposed scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
No Attack	1.000	0.000	1.000	0.000	**1.000**	**0.000**	1.000	0.000	1.000	0.000	**1.000**	**0.000**
JPEGQ20	0.706	0.501	0.850	0.207	**0.959**	**0.041**	0.706	0.497	0.884	0.164	**0.899**	**0.101**
JPEGQ30	0.777	0.243	0.887	0.158	**1.000**	**0.000**	0.780	0.221	0.933	0.098	**1.000**	**0.000**
JPEGQ50	0.999	0.001	0.945	0.079	**1.000**	**0.000**	0.999	0.001	0.983	0.025	**1.000**	**0.000**
JPEGQ70	1.000	0.000	0.986	0.021	**1.000**	**0.000**	1.000	0.000	0.997	0.009	**1.000**	**0.000**
JPEG2000 CR=2	1.000	0.000	0.998	0.003	**1.000**	**0.000**	1.000	0.000	0.999	0.001	**1.000**	**0.000**
JPEG2000 CR=4	1.000	0.000	0.989	0.016	**1.000**	**0.000**	1.000	0.000	0.991	0.014	**1.000**	**0.000**
JPEG2000 CR=8	0.988	0.012	0.949	0.073	**0.994**	**0.006**	**0.994**	**0.006**	0.956	0.065	0.991	0.009
Gaussian Filter (sigma=0.5)	1.000	0.000	1.000	0.000	**1.000**	**0.000**	1.000	0.000	1.000	0.000	**1.000**	0.000
Gaussian Filter (sigma=1.0)	1.000	0.000	0.991	0.013	**1.000**	**0.000**	**0.998**	**0.002**	0.994	0.009	0.997	0.003
Gaussian Filter (sigma=1.5)	0.903	0.098	0.965	0.052	**0.998**	**0.002**	0.885	0.116	0.961	0.058	**0.982**	**0.018**
Median Filter 3x3	0.985	0.015	0.997	0.005	**0.999**	**0.001**	0.989	0.011	0.977	0.034	**0.999**	**0.001**
Median Filter 5x5	0.648	0.332	0.949	0.075	**0.953**	**0.047**	0.609	0.357	0.907	0.137	**0.941**	**0.060**
Average Filter 3x3	0.995	0.005	0.964	0.052	**1.000**	**0.000**	0.992	0.008	0.972	0.040	**0.999**	**0.001**
Average Filter 5x5	0.685	0.290	0.901	0.143	**0.955**	**0.045**	0.646	0.321	0.893	0.153	**0.945**	**0.056**
Salt and Pepper Noise 0.01	0.847	0.155	0.882	0.165	**0.905**	**0.096**	0.865	0.133	0.894	0.149	**0.894**	**0.105**
Salt and Pepper Noise 0.02	0.727	0.275	0.839	0.222	**0.850**	**0.151**	0.765	0.235	**0.854**	0.201	0.832	**0.166**
Speckle Noise 0.01	0.714	0.284	**0.868**	0.183	0.818	**0.183**	0.765	0.232	**0.910**	**0.129**	0.848	0.152
Adaptive Histogram Equalization	1.000	0.000	0.996	0.006	**1.000**	**0.000**	1.000	0.000	0.999	0.001	**1.000**	**0.000**
Histogram Equalization	1.000	0.000	0.995	0.007	**1.000**	**0.000**	1.000	0.000	0.996	0.006	**1.000**	**0.000**
Adjustment Contrast	1.000	0.000	0.950	0.073	**1.000**	**0.000**	1.000	0.000	0.944	0.083	**0.999**	**0.001**
Sharpening	1.000	0.000	0.999	0.001	**1.000**	**0.000**	1.000	0.000	0.999	0.001	**1.000**	**0.000**
Crop upper left corner 25%	0.967	0.035	0.957	0.066	**0.973**	**0.027**	0.979	0.021	0.959	0.065	**0.983**	**0.017**
Crop upper left corner 50%	0.910	0.104	0.911	0.150	**0.914**	**0.087**	0.864	0.169	**0.909**	0.153	0.862	**0.137**
Resize (512--->256--->512)	0.549	0.484	0.999	0.002	**1.000**	**0.000**	0.498	0.513	0.999	0.002	**1.000**	**0.000**
Resize (512--->1024--->512)	1.000	0.000	1.000	0.000	**1.000**	**0.000**	1.000	0.000	1.000	0.000	**1.000**	**0.000**

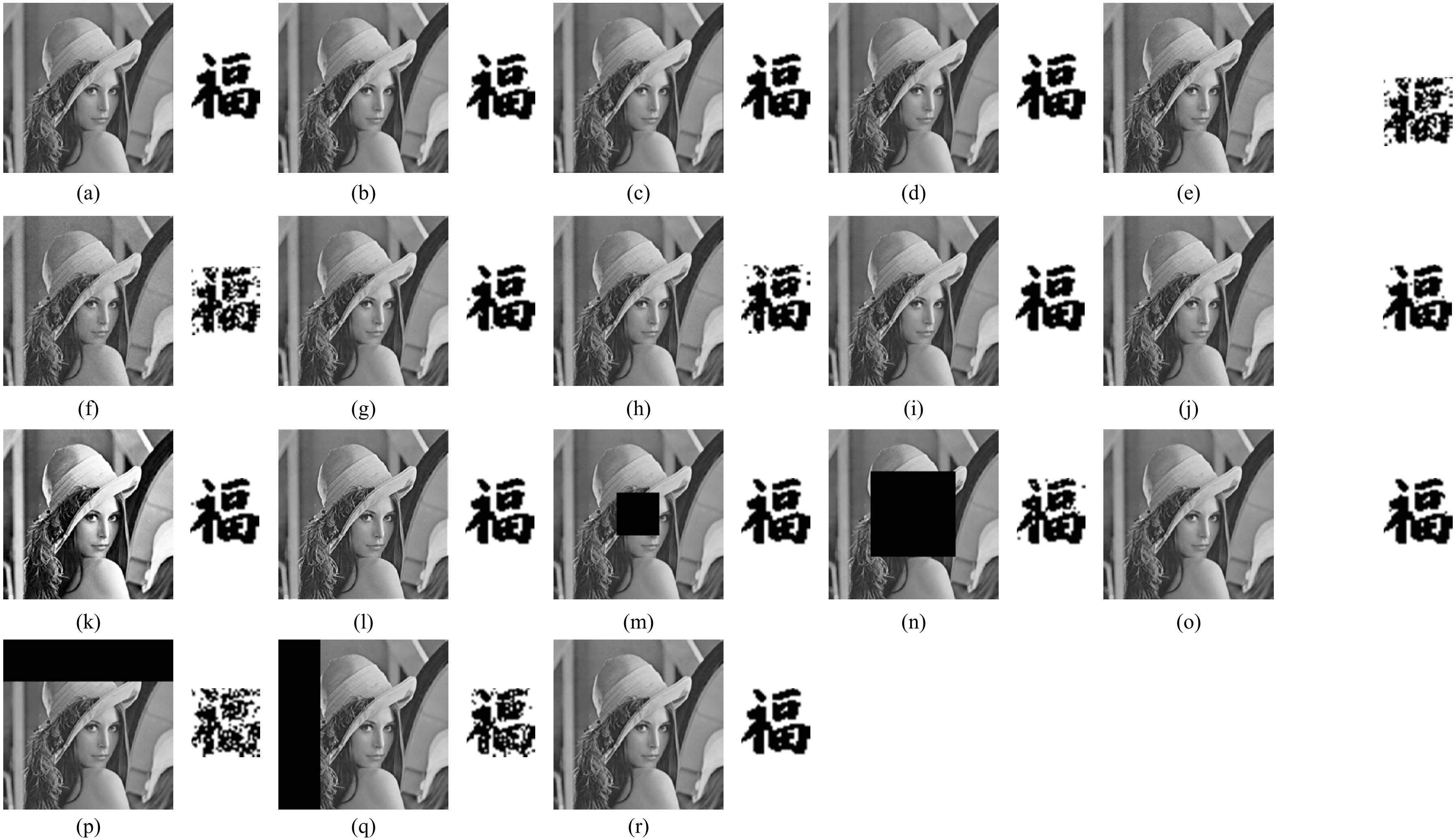

FIGURE 7. Result under various image attacks and recovered watermark from Lena image (a) GF 3 × 3 (b) MF 3 × 3 (c) AF 3 × 3 (d) WF 3 × 3 (e) GN0.001 (f) GN0.003 (g) SPN0.001 (h) SPN0.003 (i) SN0.001 (j) SN0.002 (k) HE (l) SH (m) CCO 12.5% (n) CCO 25% (o) SP0.001 and MF 3 × 3 (p) CRO 25% (q) CCLO 25% (r) SC 0.5.

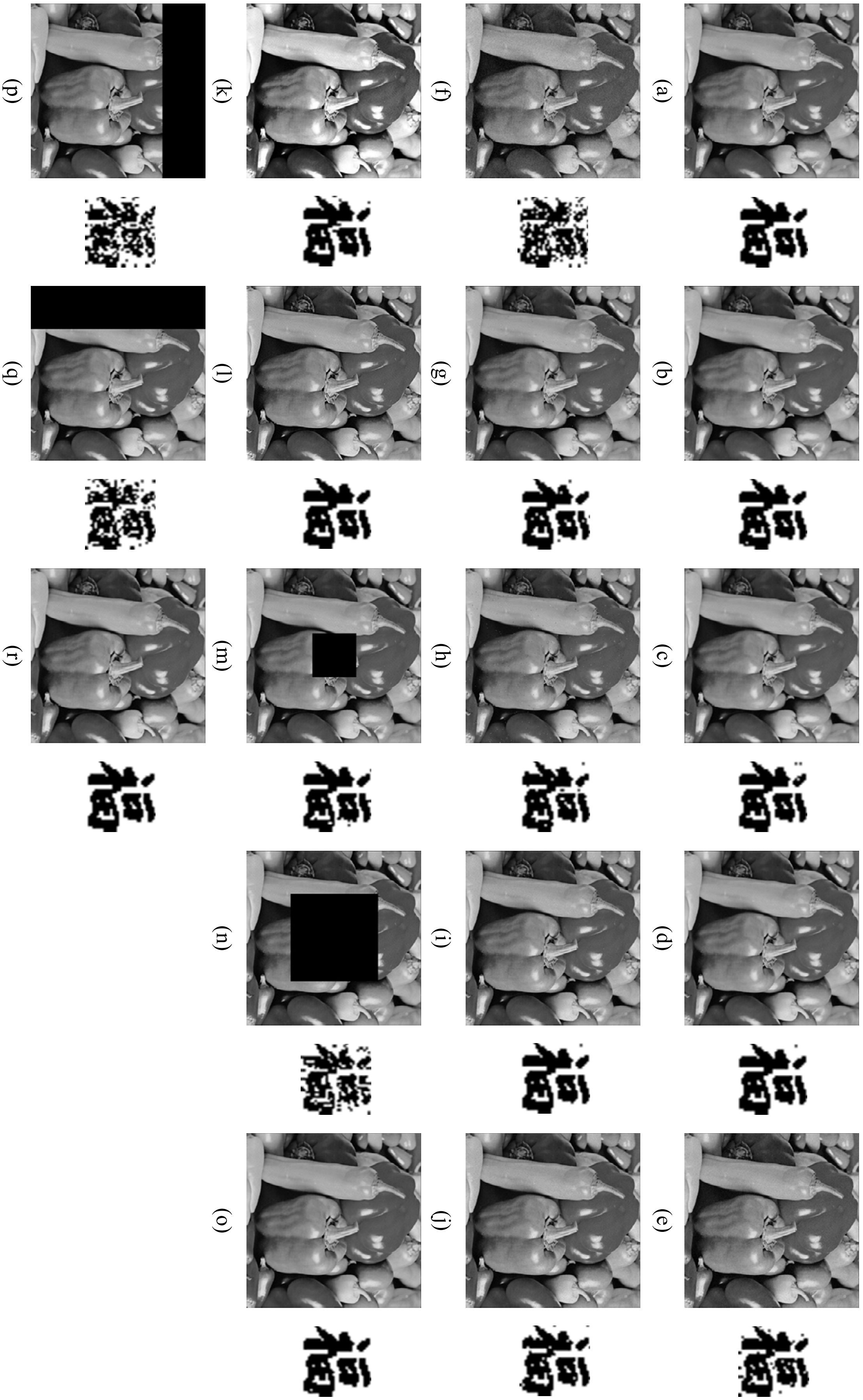

FIGURE 8. Result under various image attacks and recovered watermark from Lena image (a) GF 3 × 3 (b) MF 3 × 3 (c) AF 3 × 3 (d) WF 3 × 3 (e) GN0.001 (f) GN0.003 (g) SPN0.001 (h) SPN0.003 (i) SN0.001 (j) SN0.002 (k) HE (l) SH (m) CCO 12.5% (n) CCO 25% (o) SP0.001 and MF 3 × 3 (p) CRO 25% (q) CCLO 25% (r) SC 0.5.

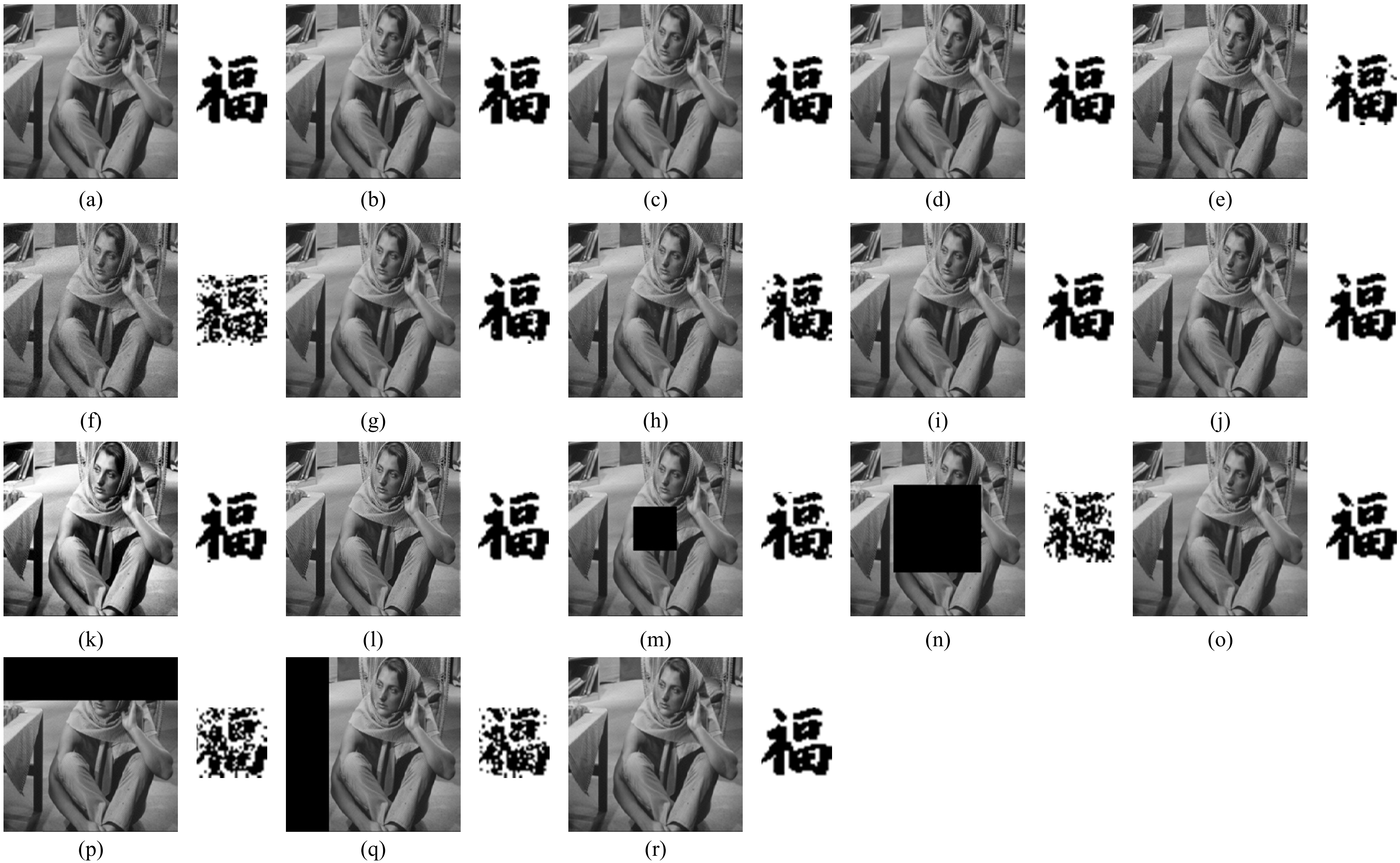

FIGURE 9. Result under various image attacks and recovered watermark from Lena image (a) GF 3 × 3 (b) MF 3 × 3 (c) AF 3 × 3 (d) WF 3 × 3 (e) GN0.001 (f) GN0.003 (g) SPN0.001 (h) SPN0.003 (i) SN0.001 (j) SN0.002 (k) HE (l) SH (m) CCO 12.5% (n) CCO 25% (o) SP0.001 and MF 3 × 3 (p) CRO 25% (q) CCLO 25% (r) SC 0.5.

The proposed scheme outperformed schemes by Ernawan and Kabir [18], Kang et al [16] and Taha et al [17] in terms of BER value under various attacks, except for salt and pepper noise (SPN) attack. It can be noticed that the proposed scheme produced lesser BER value than the existing schemes except under SPN 0.02. The watermark recovery obtained from the proposed scheme under SPN 0.02 produced higher BER value compare with Taha et al [17]. The visual croped image and it's watermark recovery are shown in Figure 6. Figure 6(a) shows that the watermarked image was cropped 25% by modifying the color image into black color. The proposed scheme produced slightly less robustness under cropped 25% of the image with NC value of 0.973 and BER value of 0.027. From Figure 6(b), it can be noticed that the watermark recovery still can be recognized by human eyes.

To investigate the robustness performance, the recovered watermarks under attacks were evaluated by NC and BER. Comparison between the scheme by Kang et al [16] and the proposed scheme is listed in Table 4. If the recovered watermark produced less BER value or high NC value, it indicates that the recovered watermark produced less distortion. If the NC value was closer to 1, it means that the watermark recovery was closer to the original watermark image.

Referring to Table 4, the proposed scheme produced majority smaller bit error rate of extracted watermark than the schemes by Ernawan and Kabir [18], Kang [25] under various attacks. The proposed scheme produced bit error rate of zero against JPEG compression with quality factor of 30, 50, 70, JPEG2000 with compression ratio of 2 and 4, Gaussian filter with sigma 0.5 and 1.0, histogram equaltization and sharpening. From Table 4, it also can be noticed that the proposed scheme produced significant improvement for NC value compared to the scheme by Kang et al [16] under JPEG compression, JPEG2000, Gaussian filter and median filter.

Moreover, the proposed scheme in this study achieved higher robustness for most image processing attacks. The visual extracted watermark under various attacks is shown in Figures 7-9. The results demonstrated that the proposed scheme able to generate good visual quality of extracted watermark under various attacks. Even the watermarked image was cropped 25%, the extracted watermark still can be recognized.

The proposed scheme has limited embedding capacity with maximum watermark bits of about 4096 bits. The proposed scheme also applied Arnold transform to encrypt the original watermark image with a key. Before embedding process, the watermark image was scrambled by Arnold transform. A key is used to determine a period of iterations in the Arnold transform. The result obtained from the extracting watermark process is scrambled watermark recovery. The extracted watermark still cannot be recognized by human visual system; the watermark must be decrypted by inverse Arnold transform with a same key. Unauthorized persons who does not have a key are not able to recover the watermark image.

VI. CONCLUSION

This research presented an adaptive scaling factor for DWT-DCT image watermarking by considering its image content. A watermark image was embedded using a set of rules for selected DWT-DCT coefficients of the image content itself. The robustness of the proposed watermarking scheme was evaluated under various attacks, including added noise, filtered image, geometrical, and compression attacks. The proposed scheme was also verified in terms of imperceptibility of watermarked images. The experimental results demonstrated that the proposed scheme achieved average PSNR value of about 47 dB and SSIM value of about 0.987 than the other existing schemes. The results also showed the proposed scheme produced lowest BER value of the watermark recovery under various attacks. In a future, the optimization method for embedding watermark can improve the quality of the watermarked image.

REFERENCES

[1] N.-T. Le, "Invisible watermarking optical camera communication and compatibility issues of IEEE 802.15.7r1 specification," *Opt. Commun.*, vol. 390, pp. 144–155, May 2017.

[2] S. P. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 86–101, May 2018.

[3] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," *Int. J. Elect. Comput. Eng.*, vol. 9, no. 3, pp. 1850–1860, 2019.

[4] F. Ernawan and M. N. Kabir, "An improved watermarking technique for copyright protection based on tchebichef moments," *IEEE Access*, vol. 7, pp. 151985–152003, 2019.

[5] Z. Zheng, N. Saxena, K. K. Mishra, and A. K. Sangaiah, "Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications," *Future Gener. Comput. Syst.*, vol. 88, pp. 92–106, Nov. 2018.

[6] C. Qin, P. Ji, C.-C. Chang, J. Dong, and X. Sun, "Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery," *IEEE Multimedia Mag.*, vol. 25, no. 3, pp. 36–48, Jul. 2018.

[7] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik*, vol. 127, no. 2, pp. 964–972, Jan. 2016, doi: 10.1016/j.ijleo.2015.09.205.

[8] I. A. Ansari and M. Pant, "SVD watermarking: Particle swarm optimization of scaling factors to increase the quality of watermark BT," in *Proc. 4th Int. Conf. Soft Comput. Problem Solving*, 2015, pp. 209–218.

[9] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking," *J. King Saud Univ.-Comput. Inf. Sci.*, pp. 1–10, Feb. 2020.

[10] P.-H. Vo, T.-S. Nguyen, V.-T. Huynh, and T.-N. Do, "A robust hybrid watermarking scheme based on DCT and SVD for copyright protection of stereo images," in *Proc. 4th NAFOSTED Conf. Inf. Comput. Sci.*, Nov. 2017, pp. 331–335.

[11] Y. He and Y. Hu, "A proposed digital image watermarking based on DWT-DCT-SVD," in *Proc. 2nd IEEE Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, May 2018, pp. 1214–1218.

[12] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools Appl.*, vol. 77, no. 3, pp. 3597–3622, Feb. 2018.

[13] P. Pandey, S. Kumar, and S. K. Singh, "Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 723–748, Sep. 2014.

[14] N. Yadav and K. Singh, "Robust image-adaptive watermarking using an adjustable dynamic strength factor," *Signal, Image Video Process.*, vol. 9, no. 7, pp. 1531–1542, Oct. 2015.

[15] S. B. B. Ahmadi, G. Zhang, S. Wei, and L. Boukela, "An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics," *Vis. Comput.*, vol. 35, pp. 385–409, Feb. 2020.

[16] X.-B. Kang, F. Zhao, G.-F. Lin, and Y.-J. Chen, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13197–13224, Jun. 2018.

[17] T. B. Taha, R. Ngadiran, and P. Ehkan, "Adaptive image watermarking algorithm based on an efficient perceptual mapping model," *IEEE Access*, vol. 6, pp. 66254–66267, 2018.

[18] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," *IEEE Access*, vol. 6, pp. 20464–20480, 2018.

[19] F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *Int. J. Elect. Comput. Eng.*, vol. 9, no. 3, pp. 2185–2195, 2019.

[20] N. A. Abbas, "Image encryption based on independent component analysis and Arnold's cat map," *Egyptian Informat. J.*, vol. 17, no. 1, pp. 139–146, Mar. 2016.

[21] L. Sun, J. Xu, S. Liu, S. Zhang, Y. Li, and C. Shen, "A robust image watermarking scheme using Arnold transform and BP neural network," *Neural Comput. Appl.*, vol. 30, no. 8, pp. 2425–2440, Oct. 2018.

[22] S. Thakral and P. Manhas, "Image processing by using different types of discrete wavelet transform," in *Advanced Informatics for Computing Research*. 2019, pp. 499–507.

[23] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," *Multimedia Tools Appl.*, vol. 79, nos. 17–18, pp. 12041–12067, May 2020.

[24] P. Singh and B. Raman, "A secured robust watermarking scheme based on majority voting concept for rightful ownership assertion," *Multimedia Tools Appl.*, vol. 76, no. 20, pp. 21497–21517, Oct. 2017.

[25] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-Based optimization," *J. Inf. Secur. Appl.*, vol. 47, pp. 28–38, Aug. 2019.

[26] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," *J. Inf. Secur. Appl.*, vol. 44, pp. 144–156, Feb. 2019.

[27] S. Wang, X. Meng, Y. Yin, Y. Wang, X. Yang, X. Zhang, X. Peng, W. He, G. Dong, and H. Chen, "Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform," *Opt. Lasers Eng.*, vol. 114, pp. 76–82, Mar. 2019.

[28] A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8881–8900, Mar. 2017.

[29] F. Ernawan, S.-C. Liew, Z. Mustaffa, and K. Moorthy, "A blind multiple watermarks based on human visual characteristics," *Int. J. Elect. Comput. Eng.*, vol. 8, no. 4, pp. 2578–2587, 2018.

[30] F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," in *Proc. IEEE 14th Int. Colloq. Signal Process. Appl. (CSPA)*, Mar. 2018, pp. 221–226.

[31] *SIPI Image Database*. Accessed: Jan. 10, 2019. [Online]. Available: http://sipi.usc.edu/database/database.php

FERDA ERNAWAN received the master's degree in software engineering and intelligence and Ph.D. degree in image processing from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, in 2011 and 2014, respectively. He is currently a Senior Lecturer with the Faculty of Computing, Universiti Malaysia Pahang. His research interests include image compression, digital watermarking, and steganography.

DHANI ARIATMANTO was born in Jakarta, Indonesia, in 1980. He received the master's degree in informatic engineering from the University of AMIKOM Yogyakarta. He is a Lecturer with the Faculty of Informatics, University of AMIKOM Yogyakarta. He is currently pursuing Ph.D. degree with Universiti Malaysia Pahang. His research interests include image processing, digital watermarking, and multimedia application.

AHMAD FIRDAUS received the Master of Computer Science degree in networking from University Teknologi Mara, Malaysia, and the Ph.D. degree (Hons.) from the University of Malaya, Malaysia. He is currently a Senior Lecturer with the Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Malaysia. His research interests include mobile security, blockchain, and intrusion detection systems.