

A Digital Watermarking Scheme using Multi-watermark Logos Embedding and Adaptive Prediction Algorithm

Komwit Surachat, Wanicbut Wattanamatiphot

*Information and Communication Technology Programme, Faculty of Science,
Prince of Songkla University, Thailand
Email: komwit.s@psu.ac.th, wanicbut.w@psu.ac.th*

Abstract

a digital watermarking scheme using multi-watermark logo embedding is proposed in this paper. In order to enhance the accuracy of the extraction process, we suggest increasing more number of watermark signals for embedding into the original image. We then section the host image into subsection by dividing all area to sixteen parts. The random number is then generated as a secret key for embedding in the individual section. In the extraction process, we retrieve the signal from each subsection individually and use the majority voting principle to conclude the final result. In addition, we propose a new adaptive mean filter to increase the retrieval performance by creating a criterion for separating data into small group and cut some peak bits out of the prediction equation. We have proved how our proposed results work by comparing with the previous algorithm. Seven types of geometric attacks are applied to the watermarked image. The recovered results of both algorithms are compared in terms of normal correlation value (NC) and readability of the results. The obtained results from the proposed method perform better than the previous method almost 0.12 in terms of NC in case if no attack is applied. Also, the proposed method result after cropping image more than fifty percent of image is still readable and returned a high NC (0.9223) when only 25 % of image left for prediction.

Manuscript received September 5, 2014; revised September 9, 2014.

This work was supported by the Information and Communication Technology Programme, Faculty of Science, Prince of Songkla University.

Corresponding author email: komwit.s@psu.ac.th.

doi:10.12720/jcm.v.n.p-p

Index Terms—digital watermarking scheme, multi-watermark logo embedding, adaptive mean filter, cropping attack

I. INTRODUCTION

The copyright protection and the security of digital multimedia information has become an important topic today. Many new technologies support and facilitate human to do anything easily. It also happens with digital media data that can be easily copied, unlimited transferring, immediate uploading to anywhere without losing any quality. The old traditional way to provide the security of digital data is to apply the cryptography functions by encrypting and decrypting using mathematical methods. Recently, the digital watermarking became popular for protecting the original data. Many researches have been proposed and discussed based on new techniques nowadays as the digital watermarking provide many applications in certification, distribution and protection.

The watermarking schemes are classified into frequency domain and spatial domain based watermarking. The processess of each domain based watermarking are quite different. In frequency domain, the process is more complex because the original image must be transformed from the time domain to the frequency domain first and then the transformed values called coefficients are edited for being embedded a signal into. For example, Shaofeng *et al.* [1] presented a computation structure for 2-D DCT watermarking in their research. They employed a single DCT-block instead of using many block in DCT-watermarking system. Also, Zheng *et al.* [2] proposed a scheme for embedding a watermark signal by using DCT-based watermarking. The proposed algorithm provided more capacity of watermark signal for envying. Not only with DCT approach, there are many researchers proposed the watermarking algorithm based on DWT. For instance, Zhang *et al.* [3] presented a robust watermarking scheme based on singular value of decomposition in DWT domain. The original image was transformed by DWT and SVD and the watermarking signal was then processed by Arnold transform and SVD. Their results were claimed that the algorithm has a very high feasibility, and has a good robustness. Also, [4], [5], [6] and [7] proposed the DWT-based watermarking together with SVD in their work. The robustness against the compression attacks were claimed and discussed. However, the frequency domain based approach was not robust enough against geometrical attacks, e.g. cropping and rotation attack.

In addition, there is another way to embed a watermark signal without using any frequency transformation. The watermark logo can be embedded into image easily by editing pixel values of the original image directly in the spatial domain. For instance, Nasir *et al.* [8] presented an idea on a new robust scheme for colored image. The original image has the embedded watermark signal by modifying the intensities of non-overlapping block of 8x8 of blue component. Furthermore, [9], [10] proposed a watermarking scheme in time domain using three-dimensional triangle meshes and Fresnel transform, respectively. The experimental results demonstrated that the proposed schemes provided good robustness against different kinds of common attacks. In addition, a method for embedding a watermark logo into an original image

by modifying the pixel was presented by Kutter *et al.* [11]. They proposed to edit the pixel by using either additive or subtractive depending on the watermark bit, and proportional to the luminance of embedding bit. The HVS theory was applied for the proposed method by using the blue color channel to envy the information because this channel is least sensitive to human eye. Then, Amornraksa *et al.* [12] developed a further technique to improve the performance of the extraction process. They proposed to balance the watermark bits before embedding process started. The strength of embedding watermark was tuned by nearly luminance and reduced the bias in the prediction of the original image. However, this proposed method encountered a deficiency when implemented with a high frequency image.

In this paper, we propose a new watermarking scheme based on the previous method [12] by using a new sectioning technique before the embedding process is being applied. Also, we proposed a more efficient way to retrieve the watermark logo by using an adaptive mean filter. The descriptions of the proposed are given as follows. The digital watermarking based on the modifications of image was given in the next section. Then, section 3 describes our proposed techniques. In section 4, the experimental results are shown and discussed. Finally, the conclusion is drawn in section 5.

II. THE PREVIOUS WATERMARKING METHOD [12]

In the previous work [12], the watermarking method was processed in the spatial domain by embedding a watermark signal in the blue channel of RGB color space. The proposed embedding algorithm was given as follows;

1. The watermark bits from the watermark signal are switched from $\{0,1\}$ to $\{1,-1\}$ by converting only the zero bits to one bits.
2. The security of the proposed algorithm was improved by using the XOR operation to balancing the watermarking bits with a pseudo-random bit-stream.
3. The watermark strength was adjusted by using the scaling factor s together with the modification of the luminance value $G_{(i,j)}$ [12] of each embedding pixel. The watermark embedding equation can be expressed by

$$I'_{(i,j)} = I_{(i,j)} + w_{(i,j)}sG_{(i,j)} \quad (1)$$

where $I_{(i,j)}$ is the image pixel in blue channel at coordinate (i,j) and $I'_{(i,j)}$ is the result of either additive or subtractive depending on the sign of watermark bit $w_{(i,j)}$ and $G_{(i,j)}$.

The extraction of watermark signal process steps for estimating the embedded watermark bit at coordinate (i,j) are given as follows;

1. Each original image pixel in the blue channel is predicted from its surrounding watermarked image pixels. The predicted original image pixel $I''_{(i,j)}$ is determined by

$$I''_{(i,j)} = \frac{1}{8} \left(\sum_{m=-1}^1 \sum_{n=-1}^1 I'_{(i+m,j+n)} - I'_{(m_{\max}n_{\max})} \right) \quad (2)$$

where $I'_{(m_max, n_max)}$ is a neighboring pixel around (i,j) that most differs from $I'_{(i,j)}$ and $I''_{(i,j)}$ is the predicted original image pixel at coordinate (i,j) .

2. The equation to determine the embedded watermark bit $w'_{(i,j)}$ at coordinate (i,j) can be expressed as follow

$$w'_{(i,j)} = I'_{(i,j)} - I''_{(i,j)} \quad (3)$$

where $w'_{(i,j)}$ is the prediction of the embedded watermark w around (i,j) .

3. The result from equation (3) is changed to be either 1 or -1 by using $w'_{(i,j)} = 0$ as a threshold. The inverted permutation balancing and the inverted modification of luminance value are then applied. The watermark signal is finally extracted after this process completed.

III. THE PROPOSED METHOD

In this research, we propose to section the original into sixteen areas before embedding a watermark signal as shown in Fig. 1.



Fig. 1 The sectioned original image

The random sequence R is then generated for using as a position set in embedding process. The value of R can be set before the embedding process is started by inputting the number of desired logo for embedding n . For example, n is set to 3 and R is then randomized to $\{3, 5, 16\}$. Set R will be used in the next process for embedding in position 3, 5 and 16 as shown in Fig. 1. Random sequence R can be expressed by following equation:

$$R_n = \{R_n \mid 1 \leq n \leq 16, 1 \leq n \leq 16, R = \text{Random}(\text{Seed}_n)\} \quad (4)$$

The proposed method description is given as follows:

1. The process is started by resizing the watermark logo from the original size $m \times n$ pixels into $\frac{m}{8} \times \frac{n}{8}$ pixels. Then, the security of the embedding process is improved by using XOR operation and Gaussian Distribution to balance the watermark bit $w_{(i,j)}$.

2. Number of position for embedding is then initiated to generate random sequence R with equation (4).
3. Due to HVS theory, the blue channel is used to embed the watermark signal in this research. The embedding process is being run by using sequence R for defining the position. The embedding equation is expressed by

$$B'_{(i,j)} = B_{(i,j)} + w_{(i,j)}^s \tag{5}$$

4. After all positions from sequence R is processed, B pane is then replaced by B' pane for using as the watermarked image.

In the extraction process, we propose to use different prediction equation to identify the watermarking bits. We first define individual criterion of own prediction window to analyze the statistical deviation from the error in embedding process. The standard deviation is then calculated for determining which equation should be used. The equation can be expressed as follow:

$$\sigma = \sqrt{\frac{1}{m \times n} \sum_{i=1}^M \sum_{j=1}^N (w'_{(i,j)} - u_x)^2} \tag{6}$$

where u_x is the mean value of prediction window $m \times n$ and can be calculated by the following equation:

$$u_x = \sqrt{\frac{1}{m \times n} \sum_{i=1}^M \sum_{j=1}^N (w'_{(i,j)})} \tag{7}$$

We set only three criterions for selecting the prediction equation. Criterion C_1 and C_2 is defined by n times of the calculated SD. The first prediction equation is determined by using the simple mean filter. This equation is summoned when the absolute value of the difference between center pixel and the mean value is less than one time of SD (locate in C_1 criterion). The equation of this case can be expressed by

$$B''_{(i,j)} = \frac{1}{9} \left(\sum_{m=-1}^1 \sum_{n=-1}^1 B'_{(i+m,j+n)} \right) \tag{8}$$

If the absolute value of the difference between center pixel and the mean value is more than one time of SD but less than two times of SD, we propose to use the surrounding pixels only as defined in equation (9).

$$B''_{(i,j)} = \frac{1}{8} \left(\sum_{m=-1}^1 \sum_{n=-1}^1 B'_{(i+m,j+n)} - B'_{(i,j)} \right) \tag{9}$$

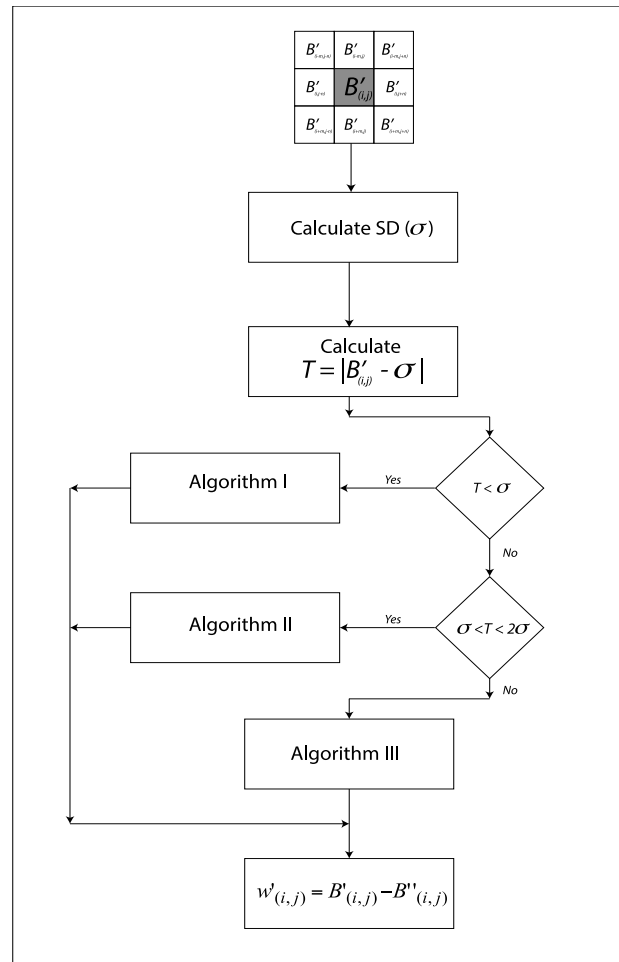


Fig. 2 The Diagram of prediction selection

Finally, we apply original equation (2) from [12] in the outbound case by

$$B''(i,j) = \frac{1}{8} \left(\sum_{m=-1}^1 \sum_{n=-1}^1 B'(i+m, j+n) - B'(m_{\max}, n_{\max}) \right) \quad (10)$$

As shown in Fig. 2, the diagram illustrates the selection process based on the difference value between the center pixel and the SD from all pixel in the prediction window. Algorithm I, II and III represents by equation 8, 9 and 10, respectively.

Then, the embedded watermark bit $w'(i,j)$ at coordinate (i,j) can be defined as follow

$$w'(i,j) = B'(i,j) - B''(i,j) \quad (11)$$

The $w'(i,j)$ is then determined by the calculated sign from equation 11. If $w'(i,j)$ is less than zero, the value will be converted to zero. In contrary, if $w'(i,j)$ is more than or equal to zero, the value will be converted to one bit.

IV. EXPERIMENTAL SETTING AND RESULTS

In the experiments, five standard color images namely ‘Lena’, ‘Birds’, ‘Tower’, ‘House’ and ‘Peppers’ were used to test the performance of interesting parameters, with the size of 256×256 pixels as the original images. Also, the 64×64 pixels black & white image containing a logo ‘Robot’ was used as a watermark signal in all experiments as shown in Fig. 3. In addition, the black color pixels were considered as -1 and the white color pixels as +1 in our proposed method.

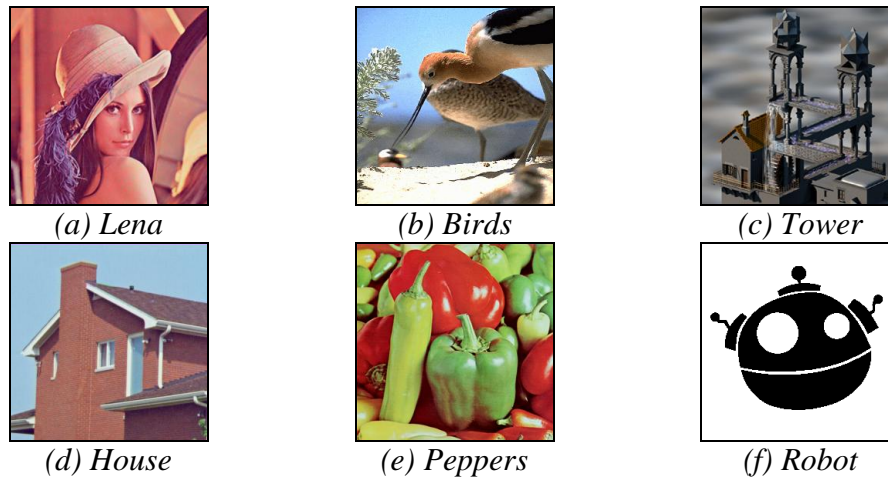


Fig. 3 The original testing images and the watermark logo

A. Evaluation Methods

The quality of watermarked image was evaluated by measuring its PSNR (Peak Signal-to-Noise Ratio) in all experiments. The PSNR value can be defined by the following equation [13]:

$$PSNR(dB) = 20 \log_{10} \frac{255\sqrt{3MN}}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (I'(i,j) - I(i,j))^2}} \tag{12}$$

where M and N represent the numbers of row and column of the images; $I(i,j)$ and $I'(i,j)$ are the original host image bit and the extracted watermark image bit at coordinate (i,j) .

In addition, Normal Correlation (NC) [14] value was measured to evaluate the quality of extracted watermark. The calculation of NC value can be expressed by:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N w(i,j)w'(i,j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (w(i,j))^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N (w'(i,j))^2}} \tag{13}$$

where M and N represent the number of row and column in the testing images, respectively. $w(i,j)$ and $w'(i,j)$ are the original and the retrieved watermark bits at pixel (i,j) , respectively.

B. Suitable Window Size of Mean Filter

A suitable $m \times n$ window size of the mean filter was first determined to achieve the highest performance of NC value. The window sizes were set as 3×3 , 5×5 , 7×7 , 9×9 and 11×11 , respectively. At PSNR = 40, the performance in term of average NC value of the proposed digital watermarking method at five different widow sizes are illustrated and compared.

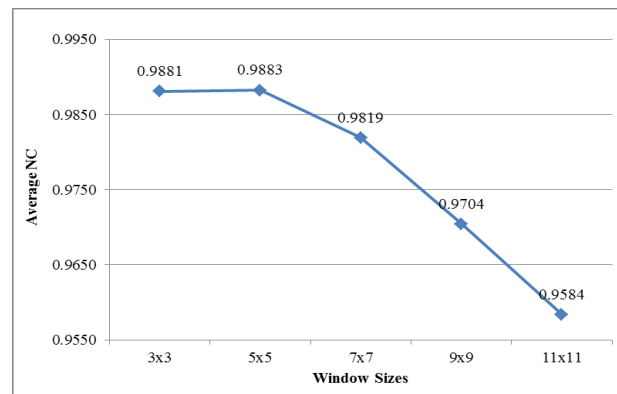


Fig. 4 Average NC from watermark extraction at PSNR 40 with different mean widow sizes

As shown in the figure, the highest performance was obtained from the 5×5 window size while 3×3 , 7×7 , 9×9 and 11×11 was a little bit lower, respectively. From this experiment, the mean filter of 5×5 pixels window size was then selected for using and testing in all remaining experiments.

C. Suitable Numbers of Watermark Logo

The proposed algorithm supports various amounts of the watermark logos for embedding in the original image. We can first initiate the numbers before the process starts.

Thus, the comparison of different numbers of embedding logo was tested at the different PSNR values. We varied PSNR range from 28 to 44 and obtained the result from embedding 4, 8, 12 and 16 signals, respectively. At the same PSNR value of every comparison points, 16 watermark logos embedding has given the best performance as shown in Fig. 5. The results at PSNR value 28-32 was achieved nearly $NC \approx 1$, the highest possible normal correlation of extracted signal. On the other hand, 12, 8 and 4 logos embedding were slightly lesser than 16 logos embedding, respectively. As a result, sixteen was set to be used with all experiments.

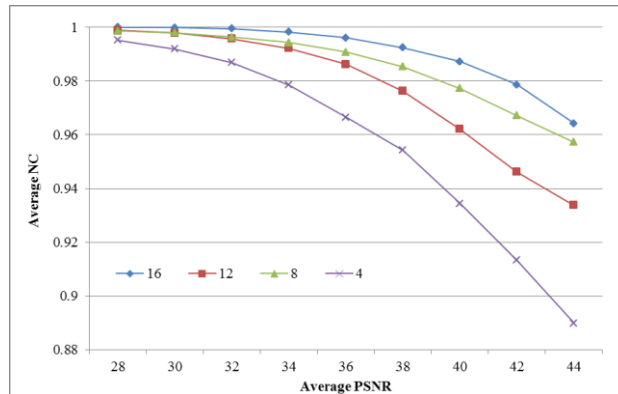


Fig. 5 The NC comparison of different logo amount embedding at different averaged PSNR values

D. Performance Comparison

In this experiment, the performance of our proposed watermarking method was evaluated and compared with the previous method [12]. Note that, the *NC* value obtained from each method was measured at the equivalent image quality, *PSNR* \approx 40 dB with the difference of less than 0.001 dB, in order to archive a fair comparison.

Different versions of the watermarked images ‘Lena’ and their extracted watermark with two different methods are illustrated in Fig. 6. From the figure, we can hardly see the difference between two versions of ‘Lena’ image. The watermarked images quality was undoubtedly comparable to the original host images. In addition, the result from the extraction process of our proposed method and previous method [12] were 0.9968 and 0.8648, respectively.

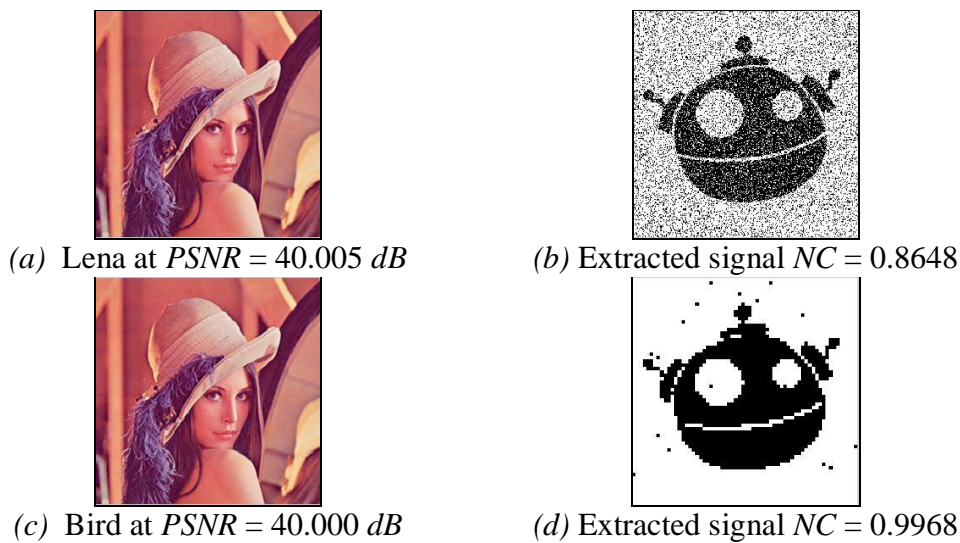


Fig. 6 The resultant watermarked image ‘Lena’ (a)-(b) and its extracted watermark at (c)-(d) with different methods

It can be obviously seen that the performance of our proposed method outperformed the previous method in [12], judge from the highest NC value at all fixed PSNR value (Range from 28 to 44). As shown in the figure below, the improvements of our proposed method were about 0.079, 0.123 and 0.142 at fixed PSNR 30, 36 and 40, respectively as shown in Fig. 7.

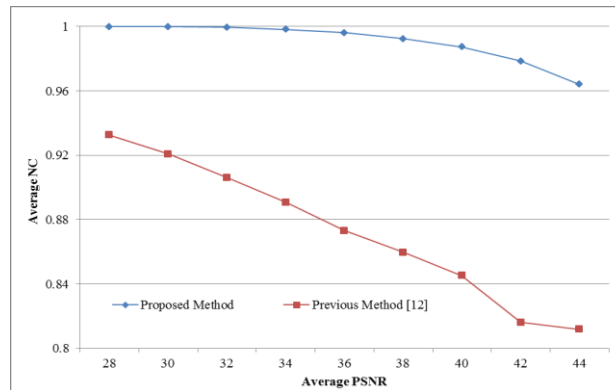


Fig. 7 Comparison between two watermarking methods at different PSNRs

E. Robustness against Attacks

We finally showed the evaluation results of our proposed watermarking method to compare with the previous method [12] in this section. Seven different kinds of common attack were chosen for proving and testing our concept. We started the experiment by embedding the watermarked signal into all chosen host images and fixing both methods with the PSNR value to 40 *dB*. Then, each attack was applied individually per one time.

We first tested our proposed method with added Gaussian distributed noise with zero mean at various variances. We varied the percentages of variance from 0.002 to 0.2. As shown in Fig. 8, the NC value of our proposed method was significantly higher than the previous methods in variance range from 0.002 to 0.01. On the other hand, the previous method was still better in small range (0.05 to 0.2).

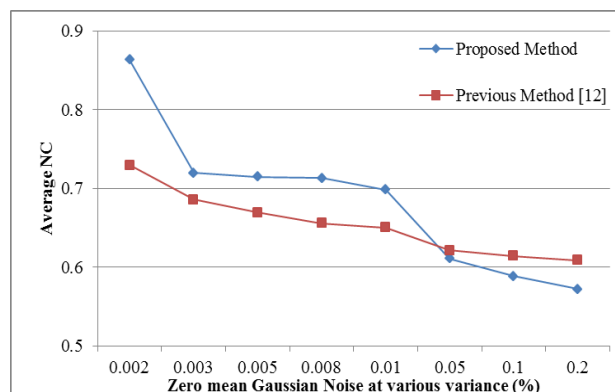


Fig. 8 Average NC values at various variances of Gaussian noise

We then added more noise testing case in our experiment. Salt and Pepper noise was implemented with different densities. Range of noise density was set from 0.01 to 0.06. We calculated numbers of inserted noise by multiplying number of pixel elements in the testing image with the density. Then, the pixels were randomly added noises as calculated quantity in the image. As shown in Fig. 9, at noise density = 0.02, our extracted signal NC value was 0.9812, while the previous method reached only 0.8583. Moreover, as shown in Fig. 10, our proposed method performed better than the previous method in all noise densities.

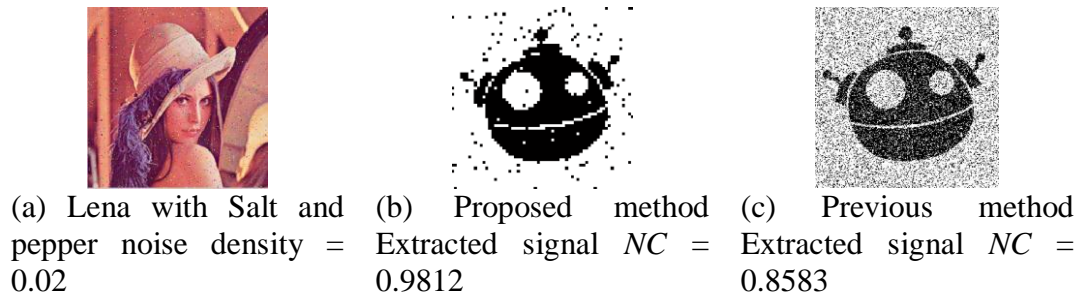


Fig. 9 The resultant of the attacked image and its extracted watermark

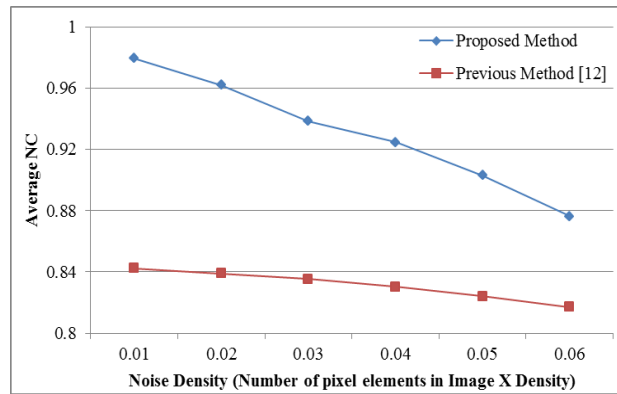


Fig. 10 Average NC values at various variances of Gaussian noise

In addition, the blurring attack was tested with both watermarking concepts. We applied motion blur to the watermarked images. The range of blurring pixels was set from 2 to 20 pixels per area. As shown in Fig. 11, the proposed method result was achieved higher performance in terms of normal correlation value. For example, at blurring pixels = 2, the average NC value of our proposed method and the previous method were 0.9053 and 0.7756, respectively.

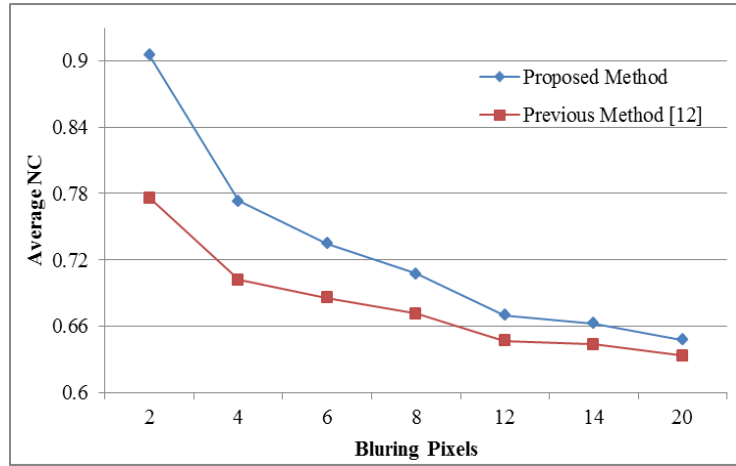


Fig. 11 Average NC values at various blurring pixels

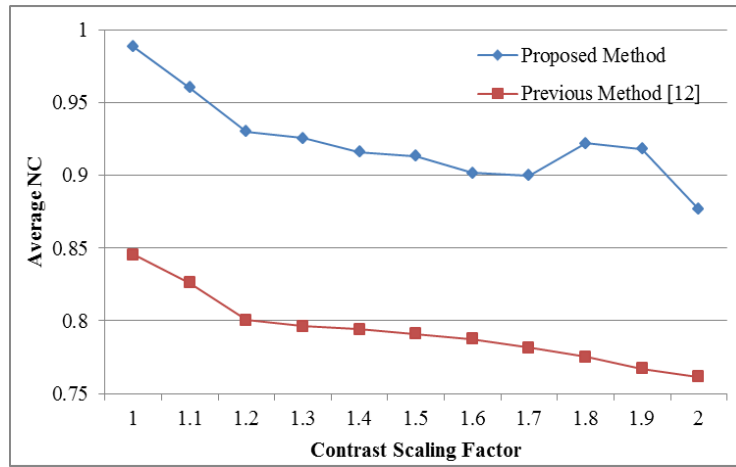


Fig. 12 Average NC values at various contrast scaling factors

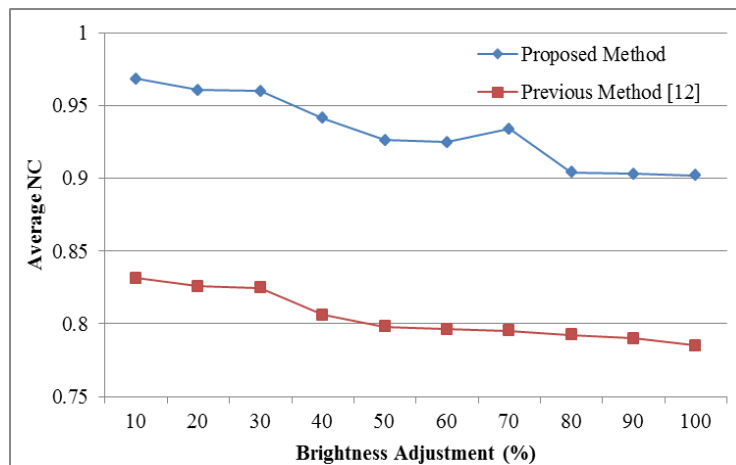


Fig. 13 Average NC values at various brightness adjustment percentage

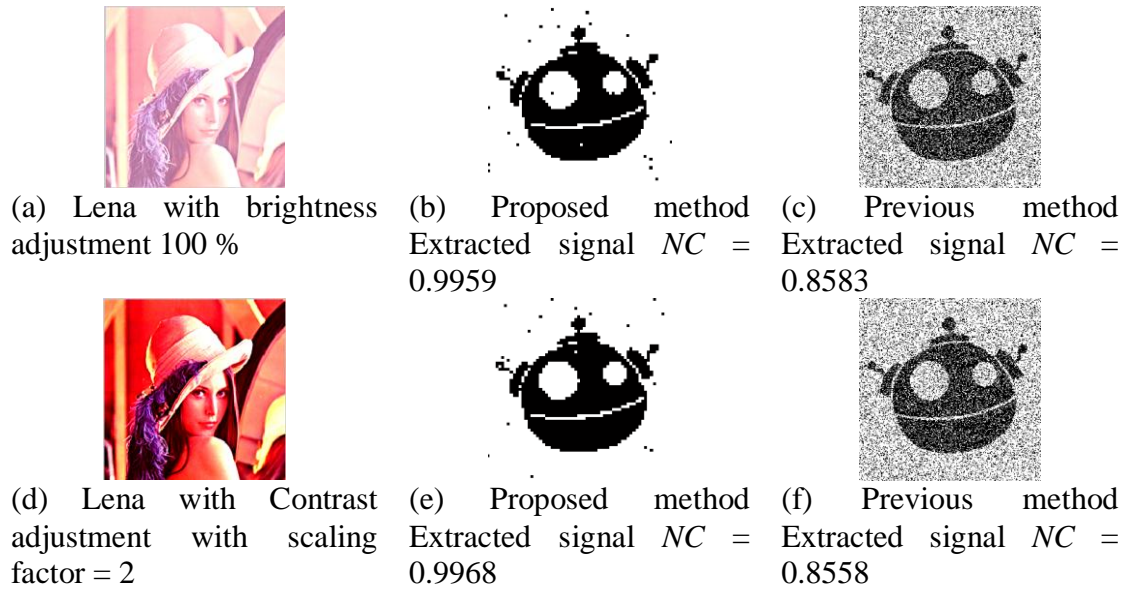


Fig. 14 The resultant of the attacked image with brightness and contrast adjustment images and its extracted watermark

Additionally, the contrast adjustment and the brightness adjustment were selected to generate the attack report. In contrast adjustment case, the chosen range was varied from 1 to 2 by increasing factor 0.1 time per once. Also, the brightness adjustment attack percentage was set from 10 to 100. As shown in Fig.12 and 13, the results obtained from our proposed method were better in all selected ranges. The extracted watermark signals from our proposed method were more readable and contained less noise than the previous method [12] as shown in Fig. 14.

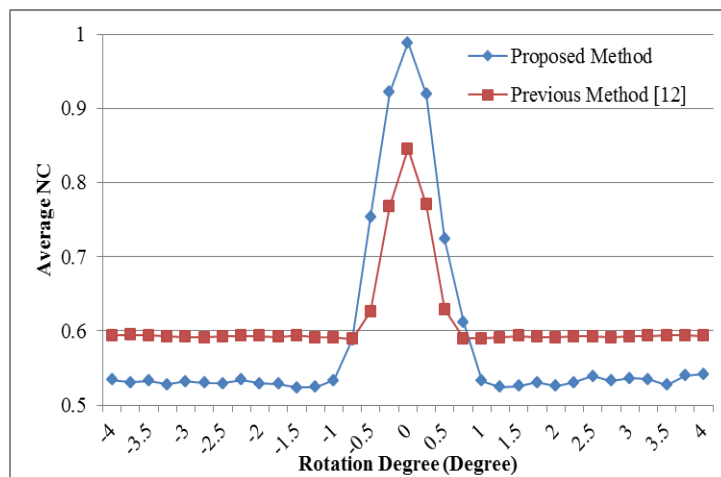


Fig. 15 Average NC values at rotation degree from -4 to 4

We then evaluated the performance of extracted watermark signal after applying rotation attack. We used full search to find the peak point of the retrieved signal. The rotation degree was varied from -4 to 4. As shown in Fig. 15, from -0.5 to 0.5 degree, our proposed method archived higher peak point than the previous method. At the rotation degree almost approach zero, the retrieved result almost reached $NC = 1$.

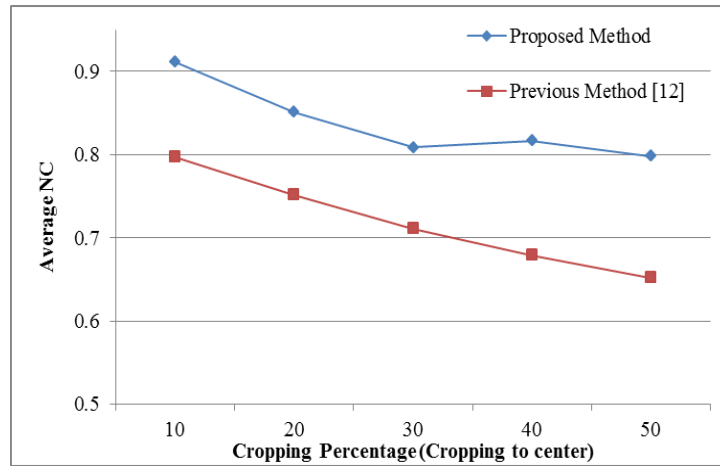


Fig. 16 Average NC values at various cropping percentage

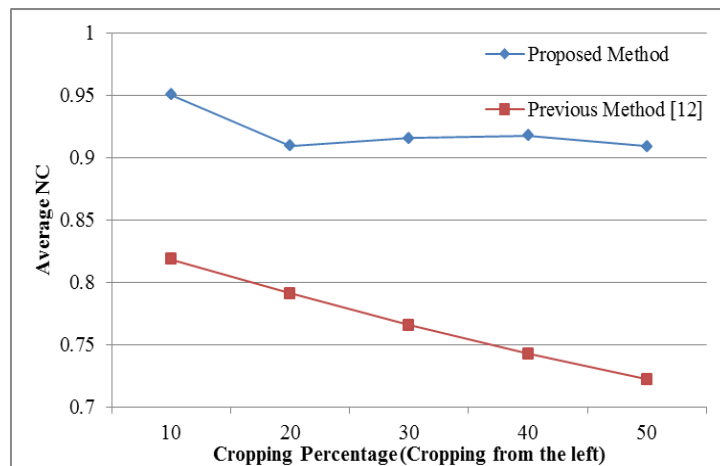


Fig. 17 Average NC values at various cropping percentage

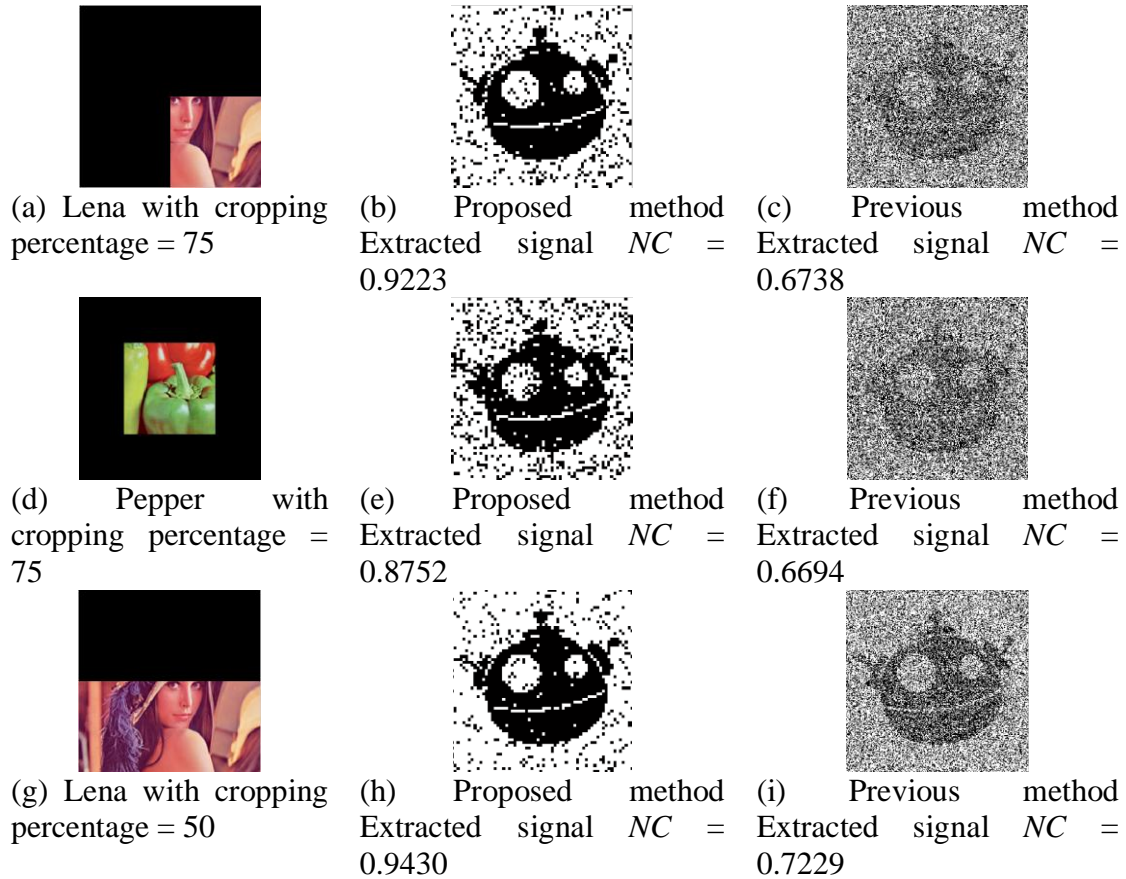


Fig. 18 The resultant of the attacked image with various cropping attack types its extracted watermark

Finally, the robustness against cropping attack was presented. The cropping styles in this experiment were designed in three different ways. First, the common style of cropping attack was applied by replacing the original pixels with zero bits. As shown in Fig. 18(b), the black pixels were added into the original image from the bottom, top, left and right, respectively. We left only center area to extract the watermark logo to prove our proposed concept that robust enough to recover the signal. Fig. 18(e) and 18(f) illustrated the extracted result from the cropped image. Our retrieved watermark signal still resulted 0.8750 in terms of normal correlation and was readable by human eyes. In contrast, the previous method [12] returned only 0.6694 in terms of NC and hardly noticed by human eyes. Second, we implemented the different styles of cropping attack by replacing only pixels on the top approaching to the center as shown in Fig. 18(e) and replacing both top side pixel and left side pixel to the center as shown in Fig. 18(g). Our proposed method resulted 0.9430 and 0.9223 and the previous method [12] resulted 0.7229 and 0.6738, respectively. Moreover, more cropping percentage cases were tested. We generated the result by varying the cropping percentage from 10 to 50 with both cropping styles. As shown in

Fig. 16 and 17, our performances in terms of robustness against cropping attack performed better than the previous method [12] in all percentages.

V. CONCLUSIONS

A new digital watermarking scheme using multi-watermark logos embedding has been proposed in this research. In order to enhance the accuracy of the retrieved watermark and the robustness against different kind of attacks, a new technique was implemented by dividing image into subsections and generating random number sequence for embedding a watermark signal in the subsection. For example, the random sequence is 2, 6, 9, 10, 11 and 16. Those random numbers will be paired up with the subsection individually. We varied the quantity of embedded watermark logo in our experiment and the best result came from 16 logos embedding. In the extraction process, the adaptive mean filter has been presented to improve the accuracy of the extracted watermark signal. Finally, we provide more evidences to support our proposed concept by generating attack report from seven different types of attack namely, additive Gaussian distributed noise, the cropping attacks, the salt and pepper noise, the blurring attack, contrast adjustment, brightness adjustment and rotation attack. As a result, the proposed method archives higher performance in terms of normal correlation calculation and watermark readable than the previous method in [12]. Especially, the proposed method results against various styles of cropping attack are significantly improved. Even the watermarked image is cropped more than 50% of all area, the extracted signal is readable with high NC value.

REFERENCES

- [1] A. Shaofeng and C. Wang, "A computation structure for 2-D DCT watermarking," in *Proc. 52nd IEEE International Midwest Symposium on Circuits and Systems*, Cancun, 2009, pp. 577-580.
- [2] J. Y. Zheng, D. H. Ling and J. Z. Liang, M. Jin, "A DCT-based digital watermarking algorithm for image," in *Proc. International Conference on Industrial Control and Electronics Engineering*, Xi'an, 2012, pp.1217-1220.
- [3] L. Zhang and A. Li, "Robust watermarking scheme based on singular value of decomposition in DWT domain," in *Proc. Asia-Pacific Conference on Information Processing*, Shenzhen, 2009, pp. 19-22.
- [4] S. Mehta, R. Nallusamy, R.V. Marawar and B. Prabhakaran, "A study of DWT and SVD based watermarking algorithms for patient privacy in medical images," in *Proc. 2013 IEEE International Conference on Healthcare Informatics (ICHI)*, Philadelphia, 2013, pp. 287-296.
- [5] X. Kang, J. Huang, Y.Q. Shi and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Tran. on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 776-786, August 2013.

- [6] M. Chandra and S. Pandey, "A DWT domain visible watermarking techniques for digital images," in *Proc. 2010 International Conference On Electronics and Information Engineering (ICEIE)*, Kyoto, 2010, pp. V2-421 – V2-427.
- [7] V.R. Ayangar and S.N. Talbar, "A novel DWT-SVD based watermarking scheme," in *Proc. 2010 International Conference on Multimedia Computing and Information Technology (MCIT)*, Sharjah, 2010, pp.105-108
- [8] I. Nasir, Y. Weng and J. Jiang, "A new robust watermarking scheme for color image in spatial domain," in *Proc. Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, Shanghai, 2007, pp. 942-947.
- [9] M. Ashourian and R. Enteshary, "A new masking method for spatial domain watermarking of three-dimensional triangle meshes," in *Proc. Conference on Convergent Technologies for the Asia-Pacific Region (TENCON 2003)*, Bangalore, 2004, pp. 428-431.
- [10] J. Li, X. Zhang, S. Lui and X. Ren, "An Adaptive Secure Watermarking Scheme for Images in Spatial Domain Using Fresnel Transform," in *Proc. 1st International Conference on Information Science and Engineering (ICISE)*, Nanjing, 2009, pp. 1630-1633.
- [11] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of colour images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp.326-332, January 1997.
- [12] T. Amornraksa and K. Jantawongwilai, "Enhanced images watermarking based on amplitude modulation," *Journal of Image and Vision Computing*, vol. 24, no. 2, pp.111-119, Febuary 2006.
- [13] J. Korhonen and J. You, "Peak signal-to-noise ratio revisited: Is simple beautiful?," in *Proc. 2012 Fourth International Workshop on Quality of Multimedia Experience (QoMEX)*, Yarra Valley, 2012, pp. 37-38.
- [14] O. O. Khalifa, Y. B. Yusof and R.F. Olanrewaju, "Performance evaluations of digital watermarking systems," in *Proc. 2012 8th International Conference on Information Science and Digital Content Technology (ICIDT)*, Jeju Island, 2012, pp. 533-536.

