

Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection

Ferda Ernawan

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Malaysia

Article Info

Article history:

Received Sep 9, 2018

Revised Dec 20, 2018

Accepted Jan 18, 2019

Keywords:

Edge entropy

Human visual characteristics

Image edge

Tchebichef moments

Tchebichef watermarking

ABSTRACT

Easy creation and manipulation of digital images present the potential danger of counterfeiting and forgery. Watermarking technique which embeds a watermark into the images can be used to overcome these problems and to provide copyright protection. Digital image watermarking should meet requirements, e.g. maintain image quality, difficult to remove the watermark, quality of watermark extraction, and applicable. This research proposes Tchebichef watermarking along the edge based on YCoCg-R color space. The embedding region is selected by considering the human visual characteristics (HVC) entropy. The selected blocks with minimum of HVC entropy values are transformed by Tchebichef moments. The locations of $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$ of the matrix moment are randomly embedded for each watermark bit. The proposed watermarking scheme produces a good imperceptibility by average SSIM value around 0.98. The watermark recovery has greater resistant after several types of attack than other schemes.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Ferda Ernawan,

Faculty of Computer Systems & Software Engineering,

Universiti Malaysia Pahang,

Lebuhraya Tun Razak, Gambang, Kuantan, 26300, Malaysia.

Email: ferda@ump.edu.my

1. INTRODUCTION

The distribution and duplication of digital images are rapidly growing due to the advancement of multimedia technologies and computer networks [1]. The advanced media (e.g. image, video, and audio) can be altered effortlessly by assailants who can then claim its possession. In this way, owners, creators, distributors, and suppliers of that media, are hesitant to allow the conveyance of their records. This leads to scientists toward the development of multimedia protection schemes against illegal duplication, and redistribution. A new approach to secure and maintain the quality of the digital multimedia becomes the primary target of scientists in digital watermarking.

Most of watermarking schemes are performed in the frequency domains. The issues need to be addressed in image watermarking are imperceptibility, robustness, security and applicable. Image watermarking based on Singular Value Decomposition (SVD) can achieve a good robustness and maintain the quality of the watermarked image. In fact, watermarking based on SVD produce high computational complexity. Furthermore, Discrete Wavelet Transform (DWT) has been widely applied in image watermarking [2], [3], DWT provides excellent spatial localization and multi-resolution [4]. While, image watermarking based on DWT may not be implemented in any devices due to high computational cost during watermark insertion and extraction. Therefore, DWT is not popular technique in the commercialization and communication. Image watermarking based on Discrete Cosine Transform (DCT) may suitable for devices due to its high robustness and low estimated cost. Lai's scheme [5] presented DCT-SVD based on the human visual characteristics. The human visual characteristic can be measured by calculating the entropy and edge

entropy of image pixels. This scheme can maintain the quality of watermarked image and it can achieve a good robustness. Furthermore, it can be seen from the limited works on [5], Lai's scheme does not sufficiently consider the optimal threshold as a trade-off between robustness and imperceptibility. The robustness of Lai's scheme may need to be improved against noise additions.

This paper proposes Tchebichef watermarking along the image edge using YCoCg-R color space. YCoCg-R color space is used to obtain the decorrelation of image pixels. In order to provide additional security, a watermark is scrambled by Arnold transform before watermark embedding. Embedding regions are determined based on the human visual characteristic entropy by measuring the entropy and edge entropy of image pixels. Selected blocks based on the human visual characteristic entropy are transformed using Tchebichef moment transform (TMT). TMT is an alternative solution to improve DCT performance in image watermarking with low computational cost using matrices. This paper also reveals an optimal threshold as a trade-off between imperceptibility and robustness. An optimal threshold is obtained by measuring SSIM and NC values against JPEG compression. JPEG compression is employed for finding an optimized threshold of Tchebichef watermarked images. Our scheme is designed to achieve high robustness and minimum distortion of the watermarked image.

2. PRELIMINARIES

2.1. YCoCg-R color space

Most of watermarking schemes are performed using YUV, RGB [6], and YCbCr color spaces [7]. YCbCr has been widely used in image compression [8]-[11], this color space is able to achieve a good decorrelation of the color image. Selecting color space in digital watermarking is an important element when we implemented on the color image. This research proposes YCoCg-R to obtain decorrelation colors. The conversion from RGB to YCoCg-R can be defined as:

$$\begin{aligned} Co &= R - B \\ t &= B + (Co/2) \\ Cg &= G - t \\ Y &= t + (Cg/2) \end{aligned} \quad (1)$$

The inverse of YCoYg-R color space is defined as

$$\begin{aligned} t &= Y - (Cg/2) \\ G &= Cg + t \\ B &= t - (Co/2) \\ R &= B + Co \end{aligned} \quad (2)$$

The YCoCg color space consist of three components Luminance (Y), Chrominance orange (Co) and Chrominance green (Cg). In [12], the YCoYg-R color space has been applied to maintain the image quality and reversibility of image watermarking.

2.2. Arnold transform

A watermark image is scrambled by Arnold transform before embedding watermark. Arnold transform changes randomly the pixel position of an image using modulo operation [13]. Arnold scrambling transformation is given by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (3)$$

where $\begin{pmatrix} x' \\ y' \end{pmatrix}$ represents the vector position after shifting, $\begin{pmatrix} x \\ y \end{pmatrix}$ denotes the original vector position before shifting, *mod* represents the modulus operation and *N* denotes the period of scrambling. In this paper, *N* is used as a key for embedding and extraction of scrambled watermark image. The inverse Arnold transformation is defined as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \quad (4)$$

2.3. Tchebichef moment

This section discusses a briefly review of Tchebichef polynomials and moments. Tchebichef moments are computed using a set of orthogonal polynomials [14]. The Tchebichef moment can be defined by:

$$T_{mn} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{r=0}^2 \frac{t_m(x)}{\rho(m, M)} f(x, y) \frac{t_n(y)}{\rho(n, N)} \quad (5)$$

where $f(x, y)$ denotes image pixels, M, N represent row and column size and $m, n = 0, 1, 2, \dots, N-1$. The set $\{t_n(x)\}$ represents the recursive relation. The inverse Tchebichef moments is given as follows:

$$\tilde{f}(x, y) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \sum_{r=0}^2 \frac{t_m(x)}{\rho(m, M)} T_{mn} \frac{t_n(y)}{\rho(n, N)} \quad (6)$$

where $\tilde{f}(x, y)$ denotes image reconstruction. The kernel of TMT can be defined by:

$$K_x = \frac{t_m(x)}{\rho(m, M)}, K_y = \frac{t_n(y)}{\rho(n, N)} \quad (7)$$

The Tchebichef moments of the original image can be computed by:

$$T = K^T F K \quad (8)$$

where F is original image. The inverse TMT can be computed by:

$$G = K T K^T \quad (9)$$

where G is reconstructed image. The first four Tchebichef polynomials are given in Figure 1.

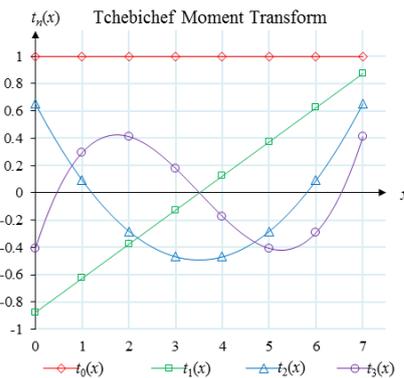


Figure 1. Discrete tchebichef polynomials $t_n(x)$

3. PROPOSED SCHEME

This section discusses the proposed embedding and extracting watermark. The watermark insertion and extraction steps are discussed in Sub-sections 3.1 and 3.2 respectively.

3.1. Proposed embedding scheme

Step 1: An image is splitted into 8×8 block pixels.

Step 2: The binary watermark is scrambled using Arnold transform.

Step 3: Each image block is computed by human visual characteristics entropy:

$$HVS_E = -\sum_{i=1}^n p_i \log_2(p_i) + \sum_{i=1}^n p_i \exp^{-p_i} \quad (10)$$

p_i denotes the occurrence probability of i -th pixel with $0 \leq p_i \leq 1$ and $\sum_{i=1}^n p_i = 1$. Furthermore, the values obtained of HVS entropy are sorted in ascending order. Select blocks that have the lowest HVS entropy value for embedding watermark. The human visual characteristic entropy has been used in the previous experiment in [15], [16] and gyrator domain [17]. This method can improve the imperceptibility of the watermarked image.

Step 4: TMT is applied on each selected block.

Step 5: Select $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$ coordinates on each selected block. These locations have potential to maintain the image quality and a good robustness. The Tchebichef moment of these locations are added value with watermark weight.

$$Q(i) = T \cdot W_Q \quad (11)$$

where T denotes by an optimal threshold, if the scrambled watermark bit W is 1, then $W_Q = 1$. Otherwise, $W_Q = -1$. If the embedded scrambled watermark bit W is 1, then the moment is added by Q . Otherwise, the moment is subtracted by Q .

Step 6: Generate the sequence random numbers using mersenne twister with a secret key. The watermark is randomly embedded in the locations of $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$.

Step 7: The selected blocks are computed by inverse TMT.

Step 8: Generate the watermarked image.

In this experiment, the location of embedding watermark has determined in $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$ of the matrix moment based on TMT. These locations have significantly less error reconstruction and the watermarked image can achieve high imperceptibility using YCoCg-R color space. Due to improving the security level, we use Arnold transform to scramble the watermark and the embedding watermark locations are randomized based on a secret key.

3.2. Proposed extraction scheme

Step 1: We use x and y coordinates to identify the embedded regions. Divide the selected region into non-overlapping block of 8×8 pixels.

Step 2: Each selected block is transform by TMT.

Step 3: Generate the random numbers using the same secret key. The sequence random numbers are used to identify extracting watermark location of $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$.

Step 4: Compute the correlation coefficients:

$$\rho = X \cdot X^* \quad (12)$$

where X represents the watermarked image and X^* denotes the sequence of watermark extraction. The watermark bit is 1, if the correlation result is greater than a threshold. otherwise, the vise versa.

Step 5: Inverse Arnold transform to restore the watermark binary image.

Step 6: Generate the watermark recovery.

3.3. An optimal threshold

In order to investigate the trade-off between robustness and invisibility, the watermarked image is compressed by JPEG compression. We increase the threshold by one at a time for embedding watermark, thus we apply JPEG compression. The invisibility of watermarked image is assessed by SSIM and the resistant of extracted watermark after different attacks is measured by NC. The relationship between imperceptibility and robustness from JPEG compression is shown in Figure 2(a) Lai's scheme [5] and Figure 2(b) proposed scheme.

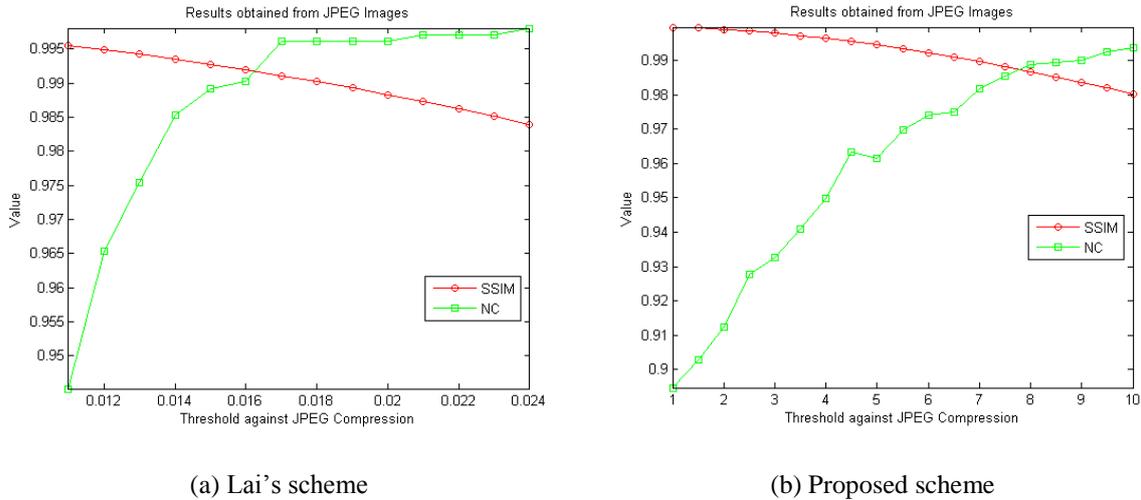


Figure 2. The optimal threshold for (a) Lai's scheme, (b) the proposed scheme

Referring to Figure 2, the experimental results show that the optimal value can be achieved using the tradeoff between resistant and invisible of watermarked image against JPEG compression. The proposed watermarking scheme can achieve the tradeoff between invisibility and resistant with the scale factor of 8 for the weighted watermarked images. However, the optimal threshold of Lai's scheme is 0.016 as presented in Figure 2(a).

4. EVALUATIONS

This section describes the evaluation of the proposed watermarking scheme to demonstrate the watermarking performance against different types of attack. The proposed watermarking scheme is tested into eight color images with 512×512 pixels as shown in Figure 3. Eight images are selected to test the proposed algorithm named as: "Lena", "Pepper", "Car", "Airplane", "Lake", "Tiffany", "Baboon" and "Sailboat". The binary watermark with size of 32×32 pixels is shown in Figure 4.

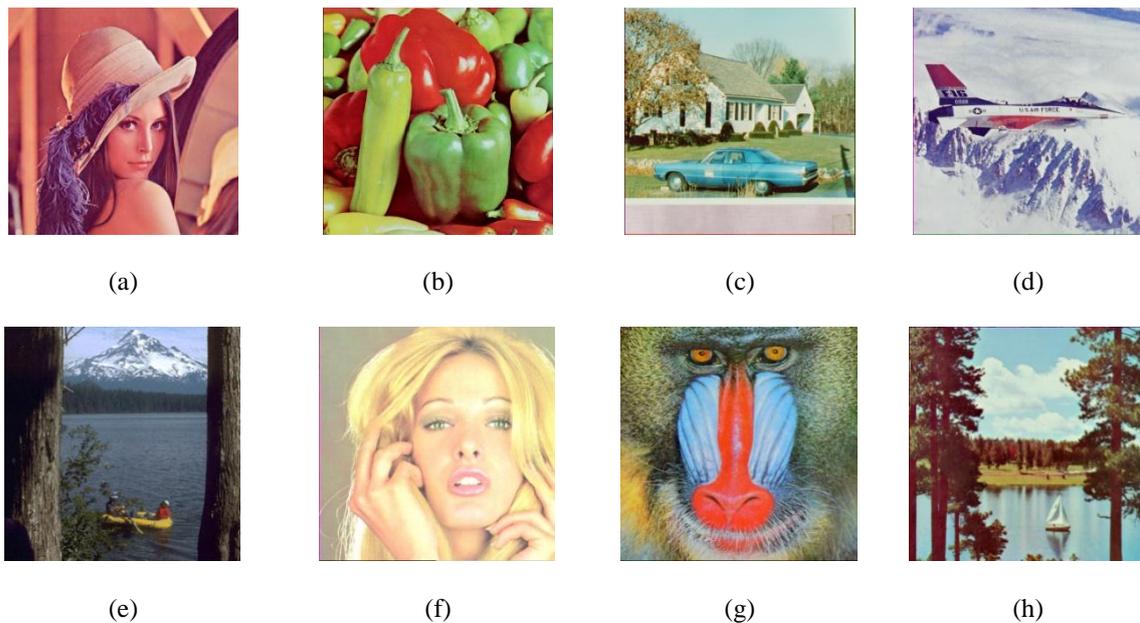


Figure 3. Host images: (a) Lena, (b) Pepper, (c) Car, (d) Airplane, (e) Lake, (f) Tiffany, (g) Baboon and (h) Sailboat

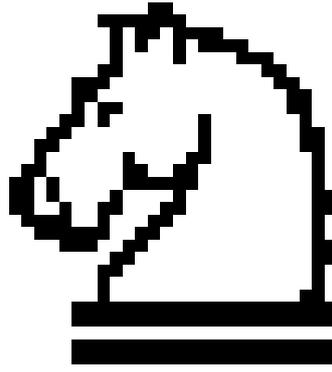


Figure 4. Watermark image

4.1. Imperceptibility evaluation

The imperceptibility of watermarked image is estimated by Structural SIMilarity (SSIM) index. SSIM is defined by [18]:

$$SSIM(x, y) = \frac{(2xy + c_1)(2\sigma_{xy} + c_2)}{(x^2 + y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (13)$$

where x and y represent the image pixel coordinates of the original and watermarked images, respectively. Two constants $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are taken to stabilize the division with weak denominator, where L is the dynamic range of a pixels, which is 255 for 8 bits per pixel and $k_1 = 0.01$ and $k_2 = 0.03$.

4.2. Robustness evaluation

Robustness of extracted recovery is estimated by Normalized Cross-Correlation (NC) and Bit Error Rate (BER). NC and BER are given as [19]:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i, j) \cdot W^*(i, j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W(i, j)^2 \sum_{i=1}^M \sum_{j=1}^N W^*(i, j)^2}} \quad (14)$$

$$BER = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i, j) \oplus W^*(i, j)}{M \times N} \quad (15)$$

where \oplus denotes the exclusive OR operation. M and N represent the number of rows and number of columns of the watermark, $W^*(i, j)$ denotes watermark extraction and $W(i, j)$ represents the original binary watermark.

4.3. Attacks

To evaluate the proposed watermarking scheme, our scheme is tested under various attacks. The consequences of the different image attacks are listed in Table 1.

Table 1. Abbreviation of the geometrical attacks used for robustness analysis

| Abbreviation | Attack's Description | Abbreviation | Attack's Description |
|--------------|---|--------------|--------------------------------------|
| NA | No Attack | RC1 | Rescaling (2, 0.5) |
| GLPF | Gaussian Low Pass Filter (3,3), sigma=1.5 | RC2 | Rescaling (0.5, 2) |
| PSN1 | Pepper and Salt Noise, density 0.001 | HE | Histogram equalization |
| PSN2 | Pepper and Salt Noise, density 0.005 | CROP1 | Cropping (rows 25%) |
| PSN3 | Pepper and Salt Noise, density 0.02 | CROP2 | Cropping (middle 25%) |
| GN1 | Gaussian Noise, variance=0.0001 | CROP3 | Cropping (columns 25%) |
| GN2 | Gaussian Noise, variance=0.0005 | CROP4 | Cropping off (rows and columns, 25%) |
| GN3 | Gaussian Noise variance=0.02 | CROP5 | Cropping off (rows and columns, 50%) |
| SN1 | Speckle Noise 0.0001 | JPEG10 | JPEG (Q=10) |
| SN2 | Speckle Noise 0.0005 | JPEG30 | JPEG (Q=30) |
| SN3 | Speckle Noise 0.02 | JPEG50 | JPEG (Q=50) |
| MF | Median Filter 3×3 | JPEG70 | JPEG (Q=70) |
| AF | Average Filter 3×3 | JPEG80 | JPEG (Q=80) |
| PN | Poisson Noise | JPEG90 | JPEG (Q=90) |
| IS | Image Sharpening | | |

5. EXPERIMENTAL RESULTS

The comparison of the watermarking performance is discussed in terms of robustness and imperceptibility. The imperceptibility of the watermarked image is measured by SSIM values. The SSIM value from the different watermarked images are depicted in Figure 5.

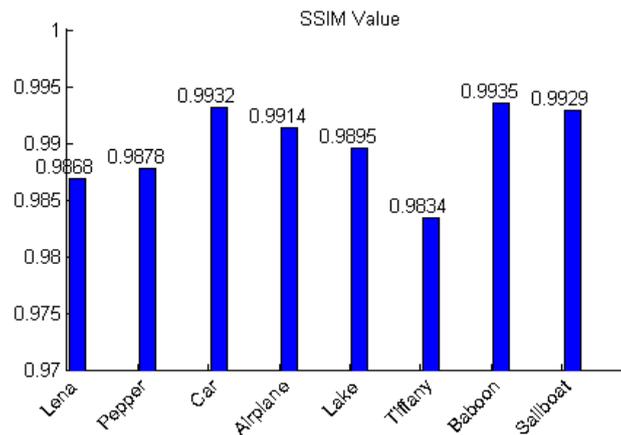


Figure 5. Comparison of SSIM values for eight watermarked images

Table 2. Comparison of NC Values from watermarked Lena image after different types of attack

| Image Processing Attack | Lai [5] | Zhang et al. [20] | Proposed |
|----------------------------|---------------|----------------------|---------------|
| | $T=0.016$ | $T=0.016$ | $T=8$ |
| No attack | 0.9724 | 1 | 1 |
| PSN1 | 0.9288 | 0.9923 | 0.9981 |
| PSN2 | 0.8008 | 0.9566 | 0.9925 |
| GN1 | 0.9097 | 0.9693 | 0.9981 |
| GN2 | 0.7681 | 0.7099 | 0.9919 |
| SN1 | 0.9373 | 0.9944 | 0.9994 |
| SN2 | 0.8664 | 0.8379 | 0.9969 |
| MF | 0.8238 | 0.9386 | 0.9622 |
| AF | 0.8165 | 0.8641 | 0.9511 |
| IS | 0.8371 | 0.9724 | 0.9819 |
| JPEG70 | 0.8371 | 0.9793 | 0.9919 |
| JPEG80 | 0.8345 | 0.9986 | 0.9950 |
| JPEG90 | 0.9265 | 1 | 0.9950 |
| RC1 | 0.9541 | 1 | 0.9919 |
| RC2 | 0.9541 | 0.9538 | 0.9680 |
| CROP1 | 0.7809 | 0.7828 | 0.9157 |
| CROP2 | 0.9500 | 0.7083 | 0.7559 |
| CROP3 | 0.8477 | 0.7297 | 0.9704 |

Figure 5 shows the SSIM values of all watermarked images. It can be checked that SSIM varies between 0.983 and 0.993 with different watermarked images. The average SSIM values obtained from proposed method is about more than 0.98. The SSIM value of watermarked Baboon image is 0.993. In Table 2, We observe that NC values are highest for the proposed technique. However, the second largest values occur for Zhang’s scheme. Zhang’s scheme produces better NC values against JPEG compression than our scheme. In summary, the proposed method outperforms other schemes for all cases implying that our method is more robust than another scheme. The proposed technique outperforms the other scheme under noise addition and filter attack. Moreover, Zhang’s performance is better than Lai’s scheme. However, for cropping centered 25%, Lai’s scheme performs better than the other schemes. The comparison of robustness under different types of attack is shown in Figure 6. NC values of extracted watermark from Lai’s scheme and proposed scheme are listed in Table 3 for comparison.

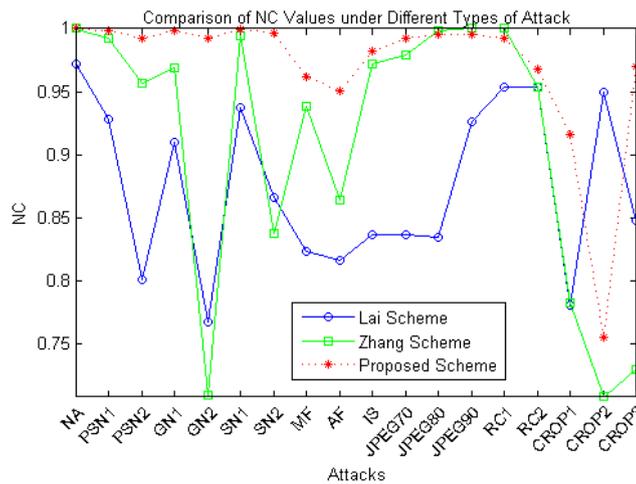


Figure 6. Comparison of robustness performance for Lai’s scheme, Zhang’s scheme and the proposed scheme

Table 3. Comparison of NC Values for Lai’s Scheme and the Proposed Scheme under Image Processing Attacks

| Attack | Lai [5] T=0.016 | Proposed T=8 | Attack | Lai [5] T=0.016 | Proposed T=8 |
|--------|--------------------|-----------------|--------|--------------------|-----------------|
| NA | 0.9837 | 1.0000 | RC1 | 0.9863 | 0.9919 |
| PSN1 | 0.9621 | 0.9981 | RC2 | 0.9605 | 0.9680 |
| PSN2 | 0.8667 | 0.9925 | CROP1 | 0.7827 | 0.9157 |
| PSN3 | 0.7307 | 0.9621 | CROP2 | 0.9588 | 0.7559 |
| GN1 | 0.9440 | 0.9981 | CROP3 | 0.8626 | 0.9477 |
| GN2 | 0.8482 | 0.9919 | CROP4 | 0.7668 | 0.9704 |
| GN3 | 0.6522 | 0.9143 | CROP5 | 0.6817 | 0.8627 |
| GLPF | 0.9642 | 0.9544 | PN | 0.7577 | 0.9800 |
| SN1 | 0.9602 | 0.9994 | HE | 0.9679 | 0.9907 |
| SN2 | 0.9082 | 0.9969 | JPEG10 | 0.5799 | 0.7631 |
| SN3 | 0.6621 | 0.9621 | JPEG30 | 0.8155 | 0.9660 |
| MF | 0.9605 | 0.9622 | JPEG50 | 0.8570 | 0.9888 |
| AF | 0.9593 | 0.9511 | JPEG70 | 0.8333 | 0.9919 |
| IS | 0.8491 | 0.9819 | JPEG90 | 0.9570 | 0.9950 |

In Figure 6, at the same Lena image, the proposed method achieves higher NC value than another schemes except the watermarked image was cropped 25% in the middle. As listed in Table 3, the proposed watermarking scheme produces high robustness of watermark extraction compared to Lai’s scheme. The proposed method achieves average NC value of 0.9 above on Lena image under different types of attack, while for the same image, the Lai’s scheme produces NC value less than 0.9. The proposed watermarking scheme can produce high NC value when the watermarked images was added by noise attacks. For the same image, Lai scheme decrease NC values if the watermarked image was compressed by JPEG compression. The visual comparison of the extracted watermarks are shown in Table 4 after different types of attack. Visually, the proposed method can extract the watermark more clearly than the other schemes.

Table 4. Extracted watermark under different Image Processing Attacks for the Lai’s Scheme and the Proposed Scheme

| Attack | Lai [5] $T=0.016$ | Proposed $T=8$ | Attack | Lai [5] $T=0.016$ | Proposed $T=8$ |
|--------|----------------------|-------------------|--------|----------------------|-------------------|
| NA | | | AF | | |
| PSN1 | | | IS | | |
| PSN2 | | | RC1 | | |
| PSN3 | | | RC2 | | |
| GN1 | | | CROP1 | | |
| GN2 | | | CROP2 | | |
| GN3 | | | CROP3 | | |
| GLPF | | | CROP4 | | |
| SN1 | | | CROP5 | | |
| SN2 | | | PN | | |
| SN3 | | | HE | | |
| MF | | | | | |

Table 4 shows the extracted watermark that has been attacked. In the proposed scheme. the watermark extraction visually less distortion, withstands severe attacks and minimum false watermark extraction than others. Our scheme produces less resistant under cropping 25% on the middle. Overall, the proposed method can achieve robustness and the watermark visually resistant against severe attacks. The watermarked images are also tested under JPEG2000.

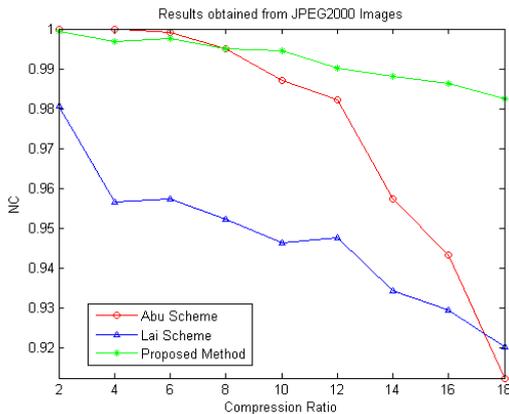


Figure 7. Comparison of NC values for Abu’s scheme [21], Lai’s scheme and proposed scheme against JPEG2000

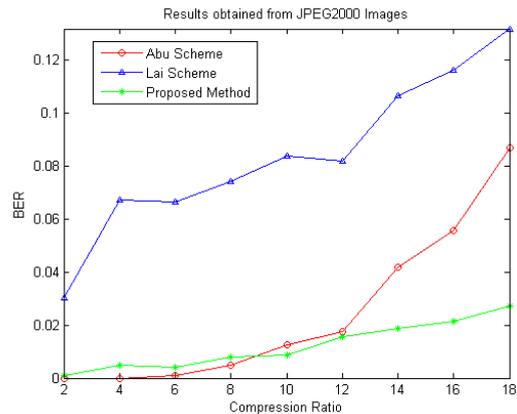


Figure 8. Comparison of BER values for Abu’s scheme, Lai’s scheme and proposed scheme against JPEG2000

According to Figure 7, the proposed method seems to degrade at higher compression ratio in JPEG2000. While our scheme is still better robustness than Lai's scheme [5] and Abu's scheme [21]. The proposed method presents highest NC values for different levels of compression ratio. The results obtained from JPEG2000 as shown in Figure 7 achieve high robustness when the compression ratio is greater than 8. At the same compression ratio, Lai's scheme is not necessarily able to withstand JPEG2000 compression. Lai's scheme seems to degrade fast at compression ratio 8-18 (NC value from 0.99 to 0.92). In Figure 8, BER values of the Abu's scheme seem to increase fast when the compression ratio is greater than 12. On the contrary, for the same image, Lai scheme produce higher bit error of watermark extraction compared to other methods. BER value of the proposed scheme is about less than 0.3, our scheme produces low bit error rates when the watermarked images are compressed by JPEG2000. BER values of the proposed method can achieve lower errors than another method. The proposed method presents resistant watermark extraction against severe JPEG2000 compression.

6. CONCLUSION

This paper presents a Tchebichef watermarking along the edge using YCoCg-R color space. YCoCg-R color space can effective increasing imperceptibility due to it has a good decorrelation of color pixel. In the proposed watermarking scheme, Human visual characteristic entropy is utilized for choosing the suitable blocks which has less sensitive to the human visual system. A binary watermark is scrambled by Arnold transform before inserting watermark as additional security. The watermark image has inserted randomly into $C_{(0,1)}$, $C_{(1,0)}$, $C_{(0,2)}$ and $C_{(2,0)}$ of the matrix Tchebichef moment. The scaling factor of inserting watermark for this scheme has been revealed to achieve a tradeoff between invisibility and robustness. In this experiments, the proposed scheme has been evaluated under various attacks. One of the significant findings from this study is that the watermarked image provides less distortion. The proposed watermarking scheme produces an improved robustness watermark against severe attacks than other schemes. Our results revealed that the proposed scheme can produce high quality of extracted watermark under JPEG2000 attacks with high compression ratio. Our scheme produces lower BER value than other methods for severe JPEG2000 compression.

ACKNOWLEDGEMENTS

The authors sincerely thank Universiti Malaysia Pahang, Malaysia for supporting this research work through UMP Research Grant Scheme (RDU180358).

REFERENCES

- [1] F. Ernawan, "Robust Image Watermarking Based on Psychovisual Threshold," *Journal of ICT Research and Applications*, vol. 10(3), pp. 228-242, 2016.
- [2] T.-S. Nguyen, *et al.*, "A Reversible Image Authentication Scheme based on Fragile Watermarking in Discrete Wavelet Transform Domain," *AEU - International Journal of Electronics and Communications*, vol. 70, pp. 1055-1061, 2016.
- [3] S.-T. Chen, *et al.*, "Optimization-based Image Watermarking with Integrated Quantization Embedding in the Wavelet-Domain," *Multimedia Tools and Applications*, vol. 75, pp. 5493-5511, 2016.
- [4] J. Guo, *et al.*, "Secure Watermarking Scheme against Watermark Attacks in the Encrypted Domain," *Journal of Visual Communication and Image Representation*, vol. 30, pp. 125-135, 2015.
- [5] C.-C. Lai, "An Improved SVD-Based Watermarking Scheme using Human Visual Characteristics," *Optik - International Journal for Light and Electron Optics*, vol. 284(4), pp. 938-944, 2011.
- [6] S. Roy and A.K. Pal, "A Blind DCT Based Color Watermarking Algorithm for Embedding Multiple Watermarks," *AEU International Journal of Electronics and Communications*, vol. 72, pp. 149-161, 2017.
- [7] F Ernawan, *et al.*, "A Blind Multiple Watermarks based on Human Visual Characteristics," *International Journal of Electrical and Computer Engineering*, vol. 8(4), 2018.
- [8] F. Ernawan, *et al.*, "Bit Allocation Strategy based on Psychovisual Threshold in Image Compression," *Multimedia Tools and Applications*, pp. 1-24, 2017.
- [9] F. Ernawan, *et al.*, "An Efficient Image Compression Technique using Tchebichef Bit Allocation," *Optik - International Journal for Light and Electron Optics*, vol. 148, pp. 106-119, 2017.
- [10] N.A. Abu, *et al.*, "A Generic Psychovisual Error Threshold for The Quantization Table Generation on JPEG Image Compression," *9th International Colloquium on Signal Processing and its Applications*, pp. 39-43, 2013.
- [11] N.A. Abu and F. Ernawan, "A Novel Psychovisual Threshold on Large DCT for Image Compression," *The Scientific World Journal*, pp. 001-011, 2015.
- [12] M. Moosazadeh and G. Ekbatanifard, "An Improved Robust Image Watermarking Method using DCT and YcoCg-R color space," *Optik - International Journal for Light and Electron Optics*, vol. 140, pp. 975-988, 2017.

- [13] P. Singh, *et al.*, "Phase Image Encryption in The Fractional Hartley Domain Using Arnold Transform and Singular Value Decomposition," *Optics and Lasers in Engineering*, vol. 91, pp. 187-195, 2017.
- [14] K.M. Hosny, *et al.*, "Efficient compression of bio-signals by using Tchebichef moments and Artificial Bee Colony," *Biocybernetics and Biomedical Engineering*. vol. 38(2), pp. 385-398, 2018.
- [15] F. Ernawan & M. N. Kabir, "A Robust Image Watermarking Technique with an Optimal DCT-Psychovisual Threshold," *IEEE Access*, vol. 6, pp. 20464-20480, 2018.
- [16] F. Ernawan, *et al.*, "An Improved Imperceptibility and Robustness of 4x4 DCT-SVD Image Watermarking using Modified Entropy," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9(2-7), pp. 111-116, 2017.
- [17] S. Liansheng, *et al.*, "An optical Color Image Watermarking Scheme by using Compressive Sensing with Human Visual Characteristics in Gyrator Domain," *Optics and Lasers in Engineering*, vol. 92, pp. 85-93, 2017.
- [18] N.A. Abbas, "Image watermark detection techniques using quadrees," *Applied Computing and Informatics*, vol. 11(2), pp. 102-115, 2015.
- [19] A. Ansari, *et al.*, "Ownership Protection of Plenoptic Images by Robust and Reversible watermarking," *Optics and Lasers in Engineering*, vol. 107, pp. 325-334, 2018.
- [20] H. Zhang, *et al.*, "A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain," *Future Internet*, vol. 9(45), pp. 1-16, 2017.
- [21] N.A. Abu, *et al.*, "Image Watermarking using Psychovisual Threshold over the Edge," *Information and Communication Technology*, vol. 7804, pp. 519-527, 2013.

BIOGRAPHY OF AUTHOR



F. Ernawan is currently a Senior Lecturer at the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang. He received his Master in Software Engineering and Intelligence and Ph.D in image processing from Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka in 2011 and 2014 respectively. His research interests include image compression, digital watermarking and steganography (Scopus ID: 53663438800).