# Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels

## Ferda Ernawan<sup>1</sup>, Dhani Ariatmanto<sup>2</sup>

<sup>1</sup>Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Malaysia <sup>2</sup>Faculty of Computer Science, Universitas Amikom Yogyakarta, Indonesia

Article Info	ABSTRACT
Article history:	With the era of rapid technology in multimedia, the copyright protection is very important to preserve an ownership of multimedia data. This paper
Received Aug 9, 2018 Revised Dec 2, 2018 Accepted Dec 30, 2019	proposes an image watermarking scheme based on Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD). The binary watermark is scrambled by Arnold transform before embedding watermark. Embedding locations are determined by using variance pixels. Selected
Keywords:	blocks with the lowest variance pixels are transformed by IWT, thus the LL sub-band of $8 \times 8$ IWT is computed by using SVD. The orthogonal U matrix
Embedding technique Image watermarking Integer wavelet transform Singular value decomposition Variance pixels	component of $U_{3,1}$ and $U_{4,1}$ are modified using certain rules by considering the watermark bits and an optimal threshold. This research reveals an optimal threshold value based on the trade-off between robustness and imperceptibility of watermarked image. In order to measure the watermarking performance, the proposed scheme is tested under various attacks. The experimental results indicate that our scheme achieves higher robustness than other scheme under different types of attack.
	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 26300 Gambang, Kuantan Pahang Darul Makmur, Malaysia. Email: ferda@ump.edu.my

## 1. INTRODUCTION

With rapid growth of internet technology, copyright and security are the major issues towards multimedia distribution. Digital watermarking technique is an alternative solution to provide multimedia protection. Image watermarking technique embeds the copyright information which maintains the quality of the host image. Image watermarking can be performed in spatial and frequency domains. In spatial domain, the watermark is direcly embedded into the image pixels. This scheme provides low computational cost and it is easy to be implemented [1]. This technique can achieve high imperceptibility of the watermarked image. However, this scheme provides weak robustness against noise attacks and JPEG compression. Image watermarking based on transformed-domain produces a good robustness against several attacks. The transformed-domains such as Discrete Cosine Transform (DCT) [2]-[5], Discrete Wavelet Transform (DWT) [6], [7], Integer Wavelet Transform (IWT) [8] have been widely used in image watermarking schemes.

Most of watermarking schemes applied hybrid scheme between SVD and transform domains to improve robustness of the watermarked image. watermarking schemes. Lai [9] presented DCT-SVD watermarking scheme based on human visual characteristics. Lai presented the embedding watermark technique by examining the first column of orthogonal U matrix. Lai's scheme can achieve a good imperceptibility of the watermarked image. However, Lai's scheme provides weak robustness against speckle and Gaussian noises. Makbol *et al.* [10] presented DWT-SVD watermarking technique that consider the

human visual characteristic. The embedding process was examined orthogonal U matrix of DWT-SVD. Their scheme has adopted Lai's scheme for the embedding watermark. Makbol's scheme achieves higher robustness and imperceptibility respectively than Lai's scheme. While, DWT filter performs the transformation in the floating point. It may loose perfect reconstruction during the conversion from integer image pixels to floating point and from floating point to integer image pixels [11]. It leads round-off errors that give effect to the quality of the watermarked image.

This paper proposes image watermarking based on IWT-SVD with variance pixels. The embedding locations are determined based on the variance pixels on each block. Blocks with the lowest variance pixels are selected for embedded watermark. The number of selected blocks are similar to the number of watermark bits. The binary watermark bits are scrambled before embedding in order to provide additional security. Each selected block is transformed using  $8 \times 8$  IWT, then LL sub-band is computed using SVD. The orthogonal *U* matrix of IWT-SVD is modified using some rules with an optimal threshold. The proposed watermarking scheme may improve the imperceptibility and robustness performance compare to other schemes. The rest of this paper is organized as follows. The brief preliminaries of variance pixels, Arnold transform, IWT and SVD are discussed in Section 2. The proposed embedding and extracting watermark are presented in Section 3. The experimental setup of the proposed watermarking scheme is discussed in Section 4. Section 5 presents the experimental results. Finally, Section 6 concludes the contribution of this paper.

# 2. PRELIMINARIES

## 2.1. Variance image pixels

The variance function has been implemented in [12], it has been used to determine the selected blocks of embedding watermark. The variance pixels indicate the most complex blocks of the image. Its locations are suitable for embedding watermark in order to improve the invisibility of the watermarked image. The variance pixels are defined by:

$$S^{2} = \frac{\sum_{i=1}^{n} (V_{i} - \overline{V})^{2}}{n - 1}$$
(1)

where *n* represents the number of image pixels on each block,  $V_i$  denotes each pixel and  $\overline{V}$  represents the average pixel value on each image block.

#### 2.2. Arnold transform

Arnold transform is performed using modulo operation [13]. This technique changes the pixel position in order to scramble the binary watermark. The period the scramble watermark is used as a secret key. Attacker will difficult to identify the information of the embedded watermark even the attacker successful to extract the watermark. Arnold transform can be defined by:

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

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 and mod denotes the modulus operation after division with N. The inverse Arnold transformation is defined as:

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

#### 2.3. Integer wavelet transform

Integer wavelet transform uses a lifting scheme to perform the integer to integer wavelet transform [11]. This technique is used to avoid rounding off errors during the conversion from image pixels to the transformed coefficients. The lifting scheme may produce perfect reconstruction image watermarking. The lifting wavelet transform can be done in three stages e.g. split, predict and update. The block diagram of the lifting and inverse lifting operation is shown in Figure 1.



Figure 1. Lifting and inverse lifting operations

First stage is split, the signals are divided into even *fe* and odd *fo* values. The next stage is predict, the odd sequence values are predicted with the even sequence in the predictor. Third stage is update operation, a new even values are obtained by merging the predicted odd value and original even value based on updater. The predicted odd value represents high frequency coefficients and even value as low frequency coefficients. The inverse lifting operation can be done by merge operation.

## 2.4. Singular value decomposition

Block image with the size of  $N \times N$  can be decomposed using singular value decomposition. The SVD of an image A can be defined by [14]:

$$A = USV^{T}$$
<sup>(4)</sup>

where U and V represent the orthogonal matrices and S is the diagonal matrix that contain non-negative value.

## 3. PROPOSED SCHEME

This section discuss the proposed watermarking scheme based on IWT-SVD with variance pixels. The embeding and extracting procedures are discussed in the next sub-sections.

## **3.1. Embedding procedure**

In this procedure, the selected regions are determined by lowest variance pixel values of each block. Each selected block is transformed by IWT-SVD. The  $U_{3,1}$  and  $U_{4,1}$  coefficients of orthogonal U matrix are modified for embedding watermark. The watermark embedding scheme is illustrated in Figure 2. The proposed embedding algorithm is presented in Algorithm 1.



Figure 2. Block diagram of embedding watermark

Algorithm 1. Embedding Algorithms					
Input: Host image; watermark;					
Pre-processing:					
An image is divided into non-overlapping blocks of 8×8 pixels					
Step 2: The variance of each block is calculated, then the blocks with the lowest variance value are selected for embedding watermark. The selected blocks are equal to the number of watermark bits.					
Step 3: Save <i>x</i> and <i>y</i> coordinates of each selected block with the lowest variance value.					
Step 4: The binary watermark is scrambled using Arnold transform.					
Embedding watermark:					
Step 5: Each selected block is transformed using $8 \times 8$ IWT. Thus, LL sub-band is transformed by SVD to generate orthogonal $U$ , $S$ , and $V$ matrices.					
<ul> <li>Step 6: Calculate the average absolute value of component matrix U<sub>3,1</sub> and U<sub>4,1</sub> coefficient: b = ( U<sub>3,1</sub> + U<sub>4,1</sub> )/2 (5) Embed each binary watermark bit by modifying orthogonal U matrix with rules: Rule 1: If U<sub>k,1</sub> is a negative value, set a = -1 and µ = -R else a = 1 and µ = R, for k = 3, 4 and R represents the optimal parameter trade-off between robustness and imperceptibility. The optimal threshold R is discussed in detail as presented in Section 3.3. Rule 2: If the binary watermark bit = 1, then update U<sub>k,1</sub> by the formula: U<sub>k,1</sub> = a*b + (-1)<sup>k</sup> µ/2 (6)</li> </ul>					
Rule 3: If the binary watermark bit = 0, then update $U_{k,1}$ by the formula $U_{k,1} = a^*b - (-1)^k \mu/2$ (7)					
$U_{k,1} = a^*b - (-1)^k \mu/2$ (7) where $\mu$ is a threshold value of the optimal parameter <i>R</i> , either is a negative or positive value. If $U_{k,1}$ is negative, then we set <i>a</i> and $\mu$ as negative and vice versa.					
Post-processing:					
Step 7: The modified selected blocks are performed by inverse SVD, then we implement inverse IWT.					
Step 8: Combine all the modified selected blocks to generate the watermarked image.					
Output: Watermarked image					

## **3.2.** Extracting procedure

The block diagram of watermark extraction is illustrated in Figure 3. Step-by-step algorithm of the extracted watermark is discussed in Algorithm 2. The binary watermark image can be extracted by measuring the different absolute value of  $U_{3,1}$  and  $U_{4,1}$  coefficients that obtained from IWT-SVD. The extracted watermark is recovered by applying inverse Arnold transform.



Figure 3. Watermark extraction

Borrow	
Input: Wate	rmarked image; x and y coordinates of each selected block;
Pre-process	ing:
Step 1:	x and $y$ coordinates are used to determine the embedded regions. The selected regions are divided into non-
	overlapping of 8×8 pixels.
Step 2:	Apply $8 \times 8$ IWT for each selected block.
Step 3:	Apply SVD on the first level of LL sub-band of IWT coefficients.
Watermark	extraction:
Step 4:	Calculate the different absolute value of $U_{3,1}$ and $U_{4,1}$ coefficients from orthogonal U matrix of IWT-SVD on each
	selected block. If its different value is greater than 0, the extracted watermark bit =1 and vice versa.
Post-process	sing:
Step 5:	The extracted watermark bits are computed by inverse Arnold transform to restore the watermark image.
Output: Rec	covered Watermark

#### **Algorithm 2. Extraction Algorithms**

#### **3.3.** An optimal threshold

A threshold value or weight of embedding watermark give a significant effect to imperceptibility and robustness of the watermarking scheme. A large threshold can achieve high robustness, while at the same time it produces large distortion and vice versa. An optimal threshold based on a trade-off between robustness and imperceptibility is important to give a balance for maintaining image quality and resistant against several attacks. Lai's scheme [9] and Makbol's scheme [10] presented various thresholds; e.g. 0.02, 0.012, and 0.04. These thresholds are in tend to produce more robustness or imperceptibility based on the amount of threshold value. They did not sufficiently consider the optimal threshold value as a trade-off between imperceptibility and robustness. Therefore, based on these issues, we perform experiments to find the optimal trade-off between robustness and imperceptibility for the Lai's scheme [9], Makbol's scheme [10] and our scheme against JPEG compression. JPEG compression has been widely used in the most of digital applications [15]-[24] and it is a standard attack to measure the image watermarking performance [25]-[28].

Figure 4 shows a trade-off between NC and SSIM values for Lai's scheme [9], Makbol's scheme [10] and our scheme against JPEG compression. In order to generate the optimal threshold, the trade-off value is used as a parameter threshold R. The parameter threshold R is incremented with the rate of 0.001. The threshold for Lai's scheme [9] is 0.016, Makbol's scheme [10] is around 0.027 and our proposed scheme is 0.017. The parameter threshold R is set as the optimal threshold for embedding watermark.



Figure 4. Trade-off between SSIM and NC values: (a) the Lai's scheme [9], (b) Makbol's scheme [10]



Figure 4. Trade-off between SSIM and NC values: (c) the proposed scheme

## 4. EXPERIMENTAL SETUP

In this research, we test the proposed scheme in the seven grayscale images with the size of  $512 \times 512$  pixels. The experiments use a binary watermark image with the size of  $32 \times 32$  pixels. Seven host images and a watermark logo are shown in Figure 5.





Figure 5. (a) Lena, (b) Pepper, (c) Baboon, (d) Sailboat, (e) Lake, (f) Car, (g) Airplane, (h) watermark image

## 4.1. Imperceptibility measurement

The perceptual quality of watermarked image can be measured by Structure SIMilarity (SSIM) index. SSIM is defined by:

$$SSIM(\mathbf{x}, \mathbf{y}) = \frac{(2xy + c_1)(2\sigma_{xy} + c_2)}{(x^2 + y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$
(8)

where x and y represent the image pixels in the host and embedded images, respectively. Two constants  $c_1 = (k_1 L)^2$  and  $c_2 = (k_2 L)^2$  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 measurement

The robustness performance can be measured by Normalized Cross-Correlation (NC) and Bit Error Rate (BER). NC and BER values are measured after watermarked images are tested under different types of attack. NC and BER are defined by:

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

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

where  $W^{*}(i, j)$  is the extracted watermark and W(i, j) is the original watermark. *M* and *N* denote the row and column sizes. Several attacks are applied to the proposed watermarking scheme as listed in Table 1. Tabel 1 shows the attack's abbreviation and the attack's description. These attacks are also implemented to the other watermarking schemes.

	Table 1. Abbieviation of the A	macks for the Ro	oustiless Analysis
Abbreviation	Attack's description	Abbreviation	Attack's description
SPN	Salt and Pepper Noise, density $= 0.001$	HE	Histogram Equalization
GN	Gaussian Noise, density $= 0.0005$	JPEG50	JPEG with quality factor $= 50$
GLF	Gaussian Low pass Filter [5 5] $\sigma = 1.2$	JPEG70	JPEG with quality factor $= 70$
SN	Speckle noise, density $= 0.005$	JPEG90	JPEG with quality factor $= 90$
MF	Median Filter [3 3]	JPEG2000-9	JPEG2000 with compression ratio $= 9$
AF	Average Filter [3 3]	JPEG2000-15	JPEG2000 with compression ratio $= 15$

JPEG2000-21

JPEG2000 with compression ratio = 21

Table 1. Abbreviation of the Attacks for the Robustness Analysis

#### 5. EXPERIMENTAL RESULTS

Sharpening

Cropping row off 25%

SH

CR

This section presents the experimental results of the proposed watermarking scheme and the comparison to other schemes. The SSIM results obtained from Lai's scheme, Makbol's scheme and the proposed scheme are shown in Figure 6.



Figure 6. Comparison of SSIM values for Lai's scheme, Makbol's scheme and proposed scheme from different watermarked images

Figure 6 shows the SSIM values of the proposed scheme for seven images. It is noted that our scheme can achieve higher SSIM values than the other scheme for Baboon watermarked image. Furthermore, the rest images present slightly lower SSIM value than Lai's scheme. However, the other scheme is worse than the proposed scheme. The robustness comparison of Lai's scheme [9], Makbol's scheme [10], Zhang *et al.*'s scheme [29] and proposed scheme is shown in Table 2.

Table 2 shows the NC values between original watermark and extracted watermark after performing various attacks on the watermarked image. As can be seen, our scheme achieves high NC values against speckle noise, Gaussian noise, average filter and compression, which mean high robustness. Based on our observation, Makbol's scheme produces higher NC value against salt & pepper noise, sharpening and median filter than other schemes. While, the other schemes are worse than our scheme. The comparison of NC values under noise additions, image filters, cropping and compression attacks is shown in Figure 7.

Reffering to Figure 6, it is clear that our scheme shows better performance in terms of NC values than Lai's scheme and Makbol's scheme. It is noted that our scheme is more resistant against noise additions, image filters and compression attacks. The visual watermark extractions of the Lai's scheme, Makbol's scheme and proposed scheme are shown in Figure 4. It can be observed that the proposed scheme produces higher quality of the extracted watermark under severe JPEG2000 compression than the existing schemes. As expected, our scheme has clearly visual quality of the extracted watermark after noise addition. However, as can be seen from Table 3, Lai's scheme shows worse distortion of visual extracted watermark against Gaussian noise and speckle noise. It can be noticed that our scheme also provides distortion of extracted watermark after median and average filter attacks.

Table 2. NC Values of the Extracted Watermark for Lena Image under Different Types of Attack

able 2. INC Values of the Extracted	watermark r	U		<b>7</b>
Image Processing Attack	Lai [9]	Makbol [10]	Zhang <i>et al</i> . [29]	Proposed
Intage I focessing Attack	T=0.016	T=0.027	T=0.016	T=0.017
No attack	0.9961	1	1	1
Pepper and Salt Noise 0.001	0.9754	0.9941	0.9923	0.9883
Pepper and Salt Noise 0.005	0.8774	0.9550	0.9566	0.9467
Gaussian Noise 0.0001	0.8444	1	0.9693	0.9990
Gaussian Noise 0.0005	0.6929	0.9772	0.7099	0.9922
Speckle Noise 0.0001	0.9021	1	0.9944	1
Speckle Noise 0.0005	0.8040	1	0.8379	1
Median Filter [3×3]	0.8272	0.9467	0.9386	0.9327
Average Filter [3×3]	0.8223	0.5234	0.8641	0.9285
Image Sharpening	0.8653	1	0.9724	0.9833
JPEG (Q=70)	0.8729	0.9990	0.9793	1
JPEG (Q=80)	0.9452	1	0.9986	1
JPEG (Q=90)	0.9452	1	1	1
Rescaling (2, 0.5)	0.9635	1	1	1
Rescaling (0.5, 2)	0.8252	0.9812	0.9538	0.9068
Cropping (row off 25%)	0.8014	0.8060	0.7828	0.8601
Cropping (Centred 25%)	0.9941	0.9990	0.7083	0.9662
Cropping (column off 25%)	0.8658	0.8703	0.7297	0.8814



Figure 7. Comparison of NC values for Lai's scheme, Makbol's scheme and proposed scheme under different types of attack

Table 3	8. Watermar	k Recovery	under Ima	ge Processi		•
Image Processing	Lai	Lena Makbol			Pepper Makbol	
Attack	[9]	[10]	Proposed	Lai [9]	[10]	Proposed
	T=0.016	<u>T=0.027</u>	<u>T=0.017</u>	T=0.016	T=0.027	<u>T=0.017</u>
SPN	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		<b>4</b>		14	<b>A</b>
	100	161			143	100
		25	25		2.2	25
GN		10				
	1995			-6.4288		
GLF	2 <b>RS</b>		4 12	-5 SO		4.63
<u>GEA</u>		19	10	3 a T	<b>28</b>	163
	版物的		2.55	SHE CH	÷23323	2.52
SN	1. AL				2	<b>X</b> -1
	1999			223,000,00		
MF	- 1944 -	46				
WII <sup>*</sup>	13 G	10	10	440.0	44	100
			¥ 48*	1.44	4, 6	÷e%
AF	14 19 H	8		45 667	6 No. 8	
	4. S. F		162	48.4	e serre	
		26	26		26	260
SH		10	40	6 A.	40	1.
			38.900 S	3893		C-12-0-05
CR 1						, ĽА
	2 + 2		8		5	
	26. SA	1.5.4 C	$1 \leq i \leq k$	8 A 19	8 A 19	5 <b>-</b> S
CR 2				9 an 8		
				30. <b>1</b> . 1	(C	20,000
CR 3	10	10		10	in.	10
	16	161	167	74	767	<b>4</b> 0
	255	25	255	2.5	2.5	2.55
HE		Xa.				A
		104				
JPEG50	<u> (</u>	20	10	1.18		10
JI 1050	44.3	40	10	433	40	10
	20.00		1			1.2
JPEG70		10	10			2.0
	网络	14	144	2. C. J.	464	141
IDE COO	10	16	26	16	-26	26
JPEG90	A 163	40	40	100	40	40
	1. A. M.	A		10. 10.	16.435	
JPEG2000-9			10			1
	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	a	161	<u> </u>		761
JPEG2000-15		2. A 2		25		255
			Å.			
	8-4440/20 1910/2017	59. 50579 - 1 8219 - 1110	200 <b>- 200</b> 200 - 200	3290978 . Dogeđa	an a	en an
JPEG2000-21			10.00			<b>4</b> 2
	52.VP2					2 AR

## 6. CONCLUSION

This paper presents block-based watermarking based on  $8\times8$  IWT-SVD with variance pixels. The goal of this scheme is to improve the robustness and the imperceptibility of the watermarked image under different types of attack. The binary watermark image has been embedded into the selected blocks with lowest variance pixels. The relationship between  $U_{3,1}$  and  $U_{4,1}$  of orthogonal U matrix of  $8\times8$  IWT-SVD was examined for embedding watermark bits. The watermark bits are not directly embedded into  $U_{3,1}$  and  $U_{4,1}$ , while these coefficients are modified with certain rule conditions by considering watermark bits. The experimental results show that the proposed scheme produces a good imperceptibility around of 0.98. Our scheme is tested under image-processing and geometrical attacks e.g., noise additions, image filters and compression, scale and crop the images. Our scheme shows greater resistant under noise attacks and severe JPEG2000 compression than other watermarking schemes.

## ACKNOWLEDGEMENTS

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

#### REFERENCES

- [1] M. Khalili, "DCT-Arnold Chaotic based Watermarking using JPEG-YCbCr," *Optik International Journal for Light and Electron Optics*, vol/issue: 126(23), pp. 4367-4371, 2015.
- [2] L. Y. Hsu and H. T. Hu, "Robust Blind Image Watermarking using Crisscross Inter-Block Prediction in the DCT Domain," *Journal of Visual Communication and Image Representation*, vol. 46, pp. 33-47, 2017.
- [3] S. P. Singh and G. Bhatnagar, "A New Robust Watermarking System in Integer DCT Domain," *Journal of Visual Communication and Image Representation*, vol. 53, pp. 86-101, 2018.
- [4] F. Ernawan, et al., "An Improved Imperceptibility and Robustness of 4x4 DCT-SVD Image Watermarking with a Modified Entropy," *Journal of Telecommunication, Electronic and Computer Engineering*, vol/issue: 9(2-7), pp. 111-116, 2017.
- [5] F. Ernawan, *et al.*, "A Blind Multiple Watermarks based on Human Visual Characteristics," *International Journal of Electrical and Computer Engineering*, vol/issue: 8(4), 2018.
- [6] A. Benoraira, et al., "Blind Image Watermarking Technique based on Differential Embedding in DWT and DCT Domains," EURASIP Journal on Advances in Signal Processing, vol/issue: 2015(1), pp. 55, 2015.
- [7] I. A. Ansari and M. Pant, "Multipurpose Image Watermarking in The Domain of DWT based on SVD and ABC," *Pattern Recognition Letters*, vol. 94, pp. 228-236, 2017.
- [8] K. R. Chetan and S. Nirmala, "An Efficient and Secure Robust Watermarking Scheme for Document Images using Integer Wavelets and Block Coding of Binary Watermarks," *Journal of Information Security and Applications*, vol. 24-25, pp. 13-24, 2015.
- C. C. Lai, "An Improved SVD-based Watermarking Scheme using Human Visual Characteristics," *Optics Communication*, vol/issue: 284(4), pp. 938-944, 2011.
- [10] N. M. Makbol, et al., "Block-based Discrete Wavelet Transform-Singular Value Decomposition Image Watermarking Scheme using Human Visual System Characteristics," *IET Image Processing*, vol/issue: 10(1), pp. 34-52, 2016.
- [11] I. A. Ansari, et al., "Robust and False Positive Free Watermarking in IWT domain using SVD and ABC," Engineering Applications of Artificial Intellegence, vol. 49, pp. 114-125, 2016.
- [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. Loukhaoukha, et al., "Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *Journal of Electrical Systems and Information Technology*, vol/issue: 4(3), pp. 359-368, 2017.
- [15] F. Ernawan, et al., "Bit Allocation Strategy based on Psychovisual Threshold in Image Compression," Multimedia Tools and Applications, vol/issue: 77(11), pp. 13923-13946, 2018.
- [16] 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.
- [17] 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.
- [18] N. A. Abu and F. Ernawan, "A Novel Psychovisual Threshold on Large DCT for Image Compression," *The Scientific World Journal*, vol/issue: 2015(2015), pp. 001-011, 2015.
- [19] N. A. Abu and F. Ernawan, "Psychovisual Threshold on Large Tchebichef Moment for Image Compression," *Applied Mathematical Sciences*, vol/issue: 8(140), pp. 6951-6961, 2014.
- [20] F. Ernawan, et al., "TMT Quantization Table Generation Based on Psychovisual Threshold for Image Compression," International Conference of Information and Communication Technology, pp. 202-207, 2013.

- **D** 2195
- [21] F. Ernawan, et al., "Adaptive Tchebichef Moment Transform Image Compression using Psychovisual Model," Journal of Computer Science, vol/issue: 9(6), pp. 716-725, 2013.
- [22] F. Ernawan and S. H. Nugraini, "The Optimal Quantization Matrices for JPEG Image Compression from Psychovisual Threshold," *Journal of Theoretical and Applied Information Technology*, vol/issue: 70(3), pp. 566-572, 2014.
- [23] F. Ernawan, et al., "An Adaptive JPEG Image Compression using Psychovisual Model," Advanced Science Letters, vol/issue: 20(1), pp. 26-31, 2014.
- [24] F. Ernawan, et al., "An optimal Tchebichef Moment Quantization using Psychovisual Threshold for Image Compression," Advanced Science Letters, vol/issue: 20(1), pp. 70-74, 2014.
- [25] 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.
- [26] N. A. Abu, *et al.*, "Image Watermarking using Psychovisual Threshold over the Edge," *Information and Communication Technology*, vol. 7804, pp. 519-527, 2013.
- [27] F. Ernawan, "Robust Image Watermarking Based on Psychovisual Threshold," *Journal of ICT Research and Applications*, vol/issue: 10(3), pp. 228-242, 2016.
- [28] F. Ernawan, et al., "Block-based Tchebichef Image Watermarking Scheme using Psychovisual Threshold," International Conference on Science and Technology-Computer (ICST), pp. 6-10, 2016.
- [29] Zhang H., et al., "A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain," Future Internet, vol/issue: 9(45), pp. 1-16, 2017.

## **BIOGRAPHIES OF AUTHORS**



**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).



**D.** Ariatmanto is a Lecturer at Faculty of Informatics, University of AMIKOM Yogyakarta. He received the master's degree in Informatic Engineering from University of AMIKOM Yogyakarta. He is currently pursuing doctoral program at Universiti Malaysia Pahang. His research interests include image processing, digital watermarking and multimedia application.