A Robust Blind Watermarking Scheme Based On Stationary Wavelet Transform

Zahra Shokrollahi

Department of Electrical and Computer Engineering Shiraz University Zand St., Shiraz, Iran shokrollahi89@gmail.com

Mehran Yazdi

Department of Electrical and Computer Engineering Shiraz University Zand St., Shiraz, Iran yazdi@shirazu.ac.ir

Received July, 2016; revised February, 2017

ABSTRACT. Image watermarking is being used for proving the authenticity of images and videos. Concerning web applications, image watermarking is increasingly used to attest the ownership of images distributed on the web, however, it needs lightweight and robust watermarking methods for inserting and extracting watermarks. Recently, the stationary wavelet transform (SWT) which is linear, shift-invariant, redundant and undecimated shows a better performance in image watermarking. This paper presents a robust watermarking algorithm based on SWT which uses all subband decompositions of the image to embed the watermark from all subbands. The proposed algorithm has been compared with the more recent algorithm which uses SWT for image watermarking and the results using NCC and PSNR as evaluation metrics show a significant improvement in the presence of various attacks.

Keywords: Stationary wavelet transform; Blind watermarking; Robustness; PSNR and NCC.

1. Introduction. With rapid growth of technology and increase in use of internet, it is so easy to transfer digital data such as image, audio and video, but there are still many challenges in this issue. Some people do not consider copyright and they transfer the data without any license from the owner, creator or distributor. Therefore, there is an increasing demand for using better secure techniques to protect copyright and prevent illegal copying and distributing.

Fortunately, watermarking can be used as an alternative for many previous techniques in this field. A digital watermark is a kind of mark covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications [8].

Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and banknote authentication. So Watermarking is a process of secure data from threats of piracy and copyright, in which owner identification (watermark) is merged with the digital media at the sender end, and at the receiver end this owner identification is used to recognize the authentication of data [2].

The important technical issue is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly [6].

The process of watermarking can be divided into two parts:

a) Embedding of watermark into host image

The process of image watermarking is done at the source end. In this process watermark is embedded in the host image by using any watermarking algorithm. The whole process is shown in Fig. 1, [2].

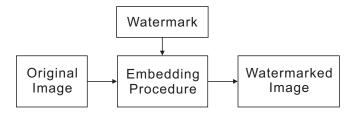


FIGURE 1. Embedding process of image watermarking

b) Extraction of watermark from image

This is the process of extracting watermark from the watermarked image by reverse the embedding algorithm. The whole process is shown in Fig. 2, [2].

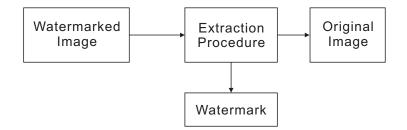


FIGURE 2. Extraction process of watermark

1.1. Watermark Classification. Digital watermarking techniques are classified into different types. This classification is based on several criteria which are: Watermark Type (noise, image); Robustness (fragile, semi-fragile, robust); Domain (spatial, frequency); Perceptivity (visible watermarking, invisible watermarking); Host Data (image, text, audio, video); Data Extraction (blind, semi-blind, non-blind).

Requirements for image watermarking contain imperceptibility, robustness to common signal processing operations, and capacity. Common signal processing operations which the watermark should survive include compression (such as JPEG), filtering, rescaling, cropping, A/D and D/A conversion, geometric distortions, and additive noise [7]. Capacity refers to the amount of information (or payload) that can be hidden in the host image and detected reliably under ordinary operating circumstances [7].

1.2. Related Work. Watermarking can be done in the spatial domain and frequency domain. Some techniques in spatial domain are LSB method, PVD method, GLM method and Parity Checker method [8]. In frequency domain there are a number of transforms including DCT, DFT, DWT and SWT.

A robust blind digital image watermarking method is proposed in [11] based on SVD in wavelet domain. First, the DWT is applied to the host image. Then, the SVD transform is applied to each sub-band of the transformed image and the singular values of each sub-band and the singular values of the watermark image are converted to semibinary arrays. Finally, the bits of the singular values of the watermark image are inserted into the selected bits of the singular values of decomposed host image's sub-bands. The experimental results show that the proposed method is robust against different geometric and non-geometric attacks and the watermarked image looks visually identical to the original one.

The proposed method in [12] is implemented using DWT and DCT. Watermark image is inserted in the LL sub-band of the host image by dividing it using DWT. 8×8 block DCT is applied to LL sub-band and watermark is embedded into the last pixel of each block. On the basis of watermark pixel value, the pixel value of host image is affected. Finally the reverse process of embedding is applied to extract exact watermark image.

In [13], an optimal watermarking scheme based DWT and QR decomposition is presented. Before embedding the watermark, information was firstly encrypted to enhance the security and robustness. Then LL subband is blocked 8×8 after DWT transformation. When each of them is QR decomposed, the watermark is embedded in the first row elements of R matrix. The experimental results show that the algorithm has high robustness, invisibility and high embedding capacity.

Thongkor *et al.* [14] proposes a digital image watermarking based on DWT. In the embedding process, the blue component of the original host image is decomposed by the Discrete Wavelet Transform (DWT) to obtain the coefficients in LL subband, and some of them are used to carry the watermark signal. In the extraction process, an original coefficients prediction in the LL sub-band based on mean filter is employed to extract the embedded watermark. The experimental results show that the performance of their proposed method in term of average NC is superior to the previous ones.

In [9] a kind of watermark inserting and extracting algorithm based on stationary wavelet transform was proposed. At first, the digital watermark was transformed randomly (Arnold transformation), then encrypted by logistic. The coded watermark was transformed to one-dimensional row vector, and the pixel value was sorted. The coefficient of one-dimensional of original image of stationary wavelet transformation was sorted too, then inserted sorted watermark to the sorted low frequency, and turned it to two dimensional data. Then the image is reconstructed with coefficients of high-frequency. The process of watermark detection is the inversion of the process of watermark embedding. Experimental results indicate that this algorithm not only enables the watermarking to have the good invisibility, but also makes the watermarking have the strong robustness to the general image attacks, such as noise, filter, rotation, compression and so on.

A digital watermarking method is proposed in [10] basing on the stationary wavelet transform to embed the digital watermark in the original DEM images and withdraw the watermark from the watermarked DEM images. Considering the characteristic of the DEM images, the embedding position is chosen in the relatively gentle terrains by analyzing the slope of the *DEM* image. The embedding intensity is optimized by an optimization model, of which the objective function is defined as the similarity between the original watermark and the extracted watermark. The optimization model is then resolved with ant colony optimization algorithm, by which the robustness are guaranteed. Simultaneously, the disturbance of the image is unnoticeable by human eyesight and the hiding of the watermark is also guaranteed.

In this paper the proposed method is based on Stationary Wavelet Transform (SWT) as introduced by [1], with some modifications in watermarking algorithm that is led to better results against various attacks such as signal and non-signal processing attacks.

In the next section a brief introduction to SWT is presented. In section 3, the embedding and extraction parts of the proposed method are explained, and in section 4 the results between proposed method and the reference paper method are compared. Section 5 is dedicated to conclusion.

2. Stationary Wavelet Transform. The Discrete Wavelet Transform is not a time invariant transform. The way to restore the translation invariance is to average some slightly different DWT, called un-decimated DWT, to define the stationary wavelet transform (SWT). It does so by suppressing the down-sampling step of the decimated algorithm and instead up-sampling the filters by inserting zeros between the filter coefficients. Algorithms in which the filter is up-sampled are called "à trous ", meaning "with holes "[4].

The stationary wavelet transform is linear, shift-invariant, redundant and undecimated. It has been discovered independently several times for divergent purposes and under different titles such as shift/translation invariant wavelet transform, undecimated wavelet transform or redundant wavelet transform. The main point is that it is redundant, shift invariant, and it contributes a denser approximation to the continuous wavelet transform than the approximation provided by the orthonormal discrete wavelet transform.

As matrix point of view, the stationary wavelet transform can be considered as a matrix multiplication.

$$Y = Wy \tag{1}$$

Where y is a $1 \times N$ input vector, W is an $(L+1)N \times N$ matrix, L is the number of decomposition levels, and Y is the $(L+1)N \times 1$ output vector.

$$W = [W_1, W_2, ..., W_L, W_{L+1}]^T$$
(2)

Where W_i is an $N \times N$ matrix, and the columns of W_i are circularly shifted versions of a single vector W_i , which is the ordinary discrete wavelet transform (DWT) basis at i_{th} scale, and W_{L+1} is the scaling function at the largest scale.

There are many inverse transforms, and one of them, which is balanced is given by:

$$M = \left[\frac{1}{2}W_1, \frac{1}{2^2}W_2, \dots, \frac{1}{2^L}W_L, \frac{1}{2^L}W_{L+1}\right]$$
(3)

Where, the factors, $(\frac{1}{2}, \frac{1}{2^2}, ..., \frac{1}{2^L}, \frac{1}{2^L})$, are needed to offset the rising redundancy of the SWT when the scale becomes larger.

In short, besides its advantages, there are some drawbacks which are the lack of orthogonality, the increased computational complexity, and the large size of the outputs [3]. 3. **Proposed Method.** The proposed method is based on stationary wavelet transform (SWT) or undecimated wavelet transform. Moreover, discrete wavelet transform is also used in order to digest necessary information for extraction. In this approach, SWT is applied to host image to obtain LL, LH, HL and HH subbands. Then parameter T is calculated for each subband according to equation 4. This is followed up by obtaining a pattern for each subband using equation 5. By applying inverse of discrete wavelet transform on patterns, a key is achieved. This key is used in extraction process in order to extract watermark.

Stationary Wavelet Transform has a better performance because of its special property, which is shift invariant. This property causes more resistivity against different kinds of attacks.

3.1. Embedding Procedure.

- 1. The image is decomposed into four sub-bands after applying the SWT.
- 2. All four subbands are considered for embedding the watermark.
- 3. Compute the mean value of each subband as follow.

$$T = \frac{1}{N} \sum_{i=1}^{N} a_k(i)$$
 (4)

Where a(i) is the SWT coefficients of the original image. k indicates a specific subband which can be LL, LH, HL or HH.

4. Compare the SWT coefficients a(i) and value T for each subband.

$$p_k(i) = \begin{cases} 1, & \text{if } a_k(i) \ge T\\ 0, & \text{if } a_k(i) < T \end{cases}$$

$$\tag{5}$$

 p_k is a determiner for obtained and appropriate pattern. Consider the watermark w(i) with size of 64×64 .

5. Perform XOR operation for $p_k(i)$ and w(i),

$$S_k(i) = p_k(i) \bigoplus w(i) \tag{6}$$

Hereby, $S_{LL}(i)$, $S_{LH}(i)$, $S_{HL}(i)$ and $S_{HH}(i)$ are achieved. (\bigoplus is the XOR sign.)

6. Apply IDWT on $S_{LL}(i)$, $S_{LH}(i)$, $S_{HL}(i)$ and $S_{HH}(i)$ to obtain S(i) (see Fig. 3). This key is used in the extraction process.

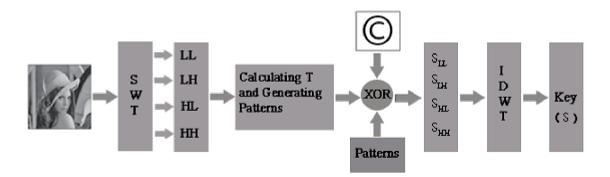


FIGURE 3. Embedding Diagram

3.2. Extraction Procedure.

- 1. Apply SWT to decompose the watermarked image into four subbands.
- 2. Take each subband and compute its mean value separately.

$$\hat{T}_k = \frac{1}{N} \sum_{i=1}^{N} \hat{a}_k(i)$$
(7)

Where $\dot{a}_k(i)$ are frequency coefficients of watermarked image in each of four subbands. 3. Compare SWT coefficients $\dot{a}_k(i)$ and \dot{T}_k .

$$\dot{p}_k(i) = \begin{cases} 1, & \text{if } \dot{a}_k(i) \ge \dot{T}_k \\ 0, & \text{if } \dot{a}_k(i) < \dot{T}_k \end{cases}$$
(8)

- 4. Perform DWT on S to get S_{LL} , S_{LH} , S_{HL} and S_{HH} .
- 5. Apply XOR operation on $p'_k(i)$ and $S_k(i)$.

$$\dot{w}_k(i) = \dot{p}_k(i) \bigoplus S_k(i) \tag{9}$$

Where \dot{w}_k is the extracted watermark from each subband.

6. Add \dot{w}_{LL} , \dot{w}_{LH} , \dot{w}_{HL} and \dot{w}_{HH} to obtain the watermark (see Fig. 4).

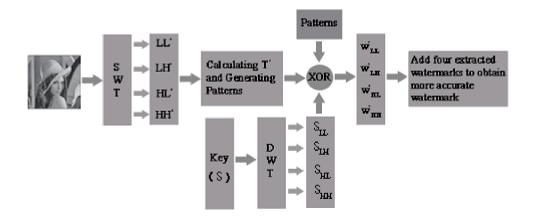


FIGURE 4. Extraction Diagram

4. **Results.** The proposed method was simulated on MATLAB 8.2.0 platform using two original images, Lena and Baboon which are shown in Fig. 5.



FIGURE 5. Host images: (a) Lena image as a low detailed image. (b) Baboon image as a high detailed image.

The watermark used in our work is a binary image shown in Fig. 6.

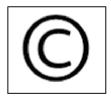


FIGURE 6. The watermark used for embedding procedure

The attacks which have been applied in our work are: Rotation, Scaling, Gaussian Noise, Jpeg2000 Compression, Shot Noise, Salt & Pepper Noise, Crop and Speckle Noise. To compare the results, *PSNR* (Peak Signal to Noise Ratio) and *NCC* (Normalized

Cross Correlation) are used as evaluation metrics as follows:

$$PSNR = 20 * \log_{10}\left(\frac{1}{\sqrt{MSE}}\right) \tag{10}$$

$$NCC = \frac{\bar{w} * w}{\sqrt{\bar{w}^2}\sqrt{w^2}} \tag{11}$$

In fact, *NCC* shows similarity between embedded watermark and extracted watermark after applying a specific attack.

Table 1 and 2 show the results of method introduced in [1] and our proposed method for the image of Lena and Baboon respectively. Furthermore, the extracted watermarks for Lena image are shown in table 3 for both methods. Table 4 is dedicated to show such results for Baboon image.

Based on the obtained results, we can conclude that much higher NCC and PSNR are obtained by proposed method. As can be also seen, visual quality of extracted watermarks is acceptable, however the extracted watermarks of our method show better performance compared to the method introduced in [1].

In order to illustrate the robustness of the proposed method, we compared our work with two recent works proposed by Singh *et al.* [15] and Xueyi *et al.* [16] who used different strategies for watermarking. Singh *et al.* [15] use the features of Discrete Cosine Transform (DCT) for the embedding of the watermark coefficients and use a pseudorandom sequence for selection of the DCT coefficients to embed the watermark. In [16], DWT, SVD and Zernike Moments are used in watermarking process. The comparisons have been performed based on NCC and applying different attacks.

Table 5 shows the results of Baboon image and the NCC values obtained by applying our proposed method and the method proposed by [15]. Table 6 shows the results of Lena image for our method and the method used in [16]. According to the NCC metric obtained in different cases, our algorithm demonstrates a better performance.

5. Conclusion. In this paper, we proposed a watermarking scheme based on stationary wavelet transform. In the proposed method, all subbands after wavelet decomposition were used to embed the watermark which makes the watermarking algorithm more robust against attacks. Indeed, some attacks can affect high frequency bands and some of them influence just low frequency bands, therefore when the watermark is extracted from all subbands, it has less sensitivity to way that an attack affect the host image. To prove this claim, various attacks have been implemented and applied in watermarked images and the results have been studied. Based on the experimental results, our proposed

	Results of [1]		Results of Our Algorithm	
Type of Attack	NCC	PSNR	NCC	PSNR
Rotation, Degree=10	0.4472	0.9688	0.9541	10.4769
Rotation, Degree=20	0.3160	0.4569	0.9409	9.4026
Rotation, Degree=30	0.2786	0.3510	0.9436	9.6011
Scaling, Ratio=2	0.9998	33.1133	1	inf
Gaussian Noise, M=0, V=0.01	0.9825	14.6007	0.9983	24.6623
Gaussian Noise, M=0, V=0.02	0.9701	12.3034	0.9960	20.9385
Gaussian Noise, M=0, V=0.03	0.9524	10.3143	0.9945	19.5915
Gaussian Noise, M=0, V=0.04	0.9411	9.4211	0.9931	18.6417
Gaussian Noise, M=0, V=0.05	0.9198	8.1233	0.9941	19.3112
JPEG2000 Compres- sion	0.9999	36.1236	1	inf
Shot Noise	0.9147	7.8693	0.9918	17.8629
Salt & Pepper Noise	0.9724	12.6406	0.9966	21.6520
Crop	0.9784	13.6932	1	inf
Speckle Noise	0.9801	14.0553	0.9974	22.9014

TABLE 1. The simulation results of Lena image for both methods of [1] and our proposed method.

method illustrated generally a better performance against different attacks compared to the previous method used SWT and other recent methods used different strategies.

REFERENCES

- Nagarjuna P.V., K. Ranjeet, Robust Blind Digital Image Watermarking Scheme Based on Stationary Wavelet Transform, *IEEE Sixth International Conference on Contemporary Computing*, pp. 451-454, 2013.
- [2] L.K. Saini, V. Shrivastava, A survey of digital watermarking techniques and its applications, International Journal of Computer Science Trends and Technology (IJCST), Volume 2, Issue 3, pp. 70-73, May-Jun 2014.
- [3] H. Guo Theory and applications of the shift-invariant, time-varying and undecimated wavelet transforms, *Doctoral Thesis*, *Rice University*, *Houston*, *Texas*, May 1995.
- [4] M. Pradnya, S.D. Ruikar, Image fusion based on stationary wavelet transform, International Journal of Advanced Engineering Research and Studies, pp. 99-101, 2013.
- [5] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital watermarking and steganography, 2nd Edition, 2007.
- [6] D. Kundur, D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, pp. 1167-1180, JULY 1999.

	Results of [1]		Results of Our Algorithm	
Type of Attack	NCC	PSNR	NCC	PSNR
Rotation, Degree=10	0.7508	3.6024	0.9572	10.7707
Rotation, Degree=20	0.7330	3.3475	0.9420	9.4866
Rotation, Degree=30	0.7172	3.1373	0.9726	12.6797
Scaling, Ratio=2	0.9859	15.5166	1	inf
Gaussian Noise, M=0, V=0.01	0.9529	10.3602	0.9976	23.1133
Gaussian Noise, M=0, V=0.02	0.9372	9.1513	0.9963	21.3524
Gaussian Noise, M=0, V=0.03	0.9224	8.2632	0.9936	18.9636
Gaussian Noise, M=0, V=0.04	0.9033	7.3499	0.9922	18.0618
Gaussian Noise, M=0, V=0.05	0.8973	7.1036	0.9926	18.3421
JPEG2000 Compres- sion	0.9989	26.5812	1	inf
Shot Noise	0.8935	6.9538	0.9894	16.7786
Salt & Pepper Noise	0.9516	10.2465	0.9980	24.0824
Crop	0.9000	7.2138	1	inf
Speckle Noise	0.9512	10.2130	0.9969	22.1442

TABLE 2. The simulation results of Baboon image for both methods of [1] and our proposed method.

- [7] C. Pudilchuk, E.J. Delp, Digital watermarking: algorithms and applications, Signal Processing Magazine, IEEE, pp. 33-46, July 2001.
- [8] R. Saini, R. Yadav, A New Data Hiding Method Using Pixel Position and Logical AND Operation, International Journal of Computer and Electronics Research, Volume 1, Issue 1, pp. 12-18, June 2012.
- [9] C. Zhang, J. Wang, X. Wang, Digital image watermarking algorithm with double encryption by Arnold transform and logistic, *Fourth International Conference on Networked Computing and Ad*vanced Information Management, Vol. 1, pp. 329-334, 2008.
- [10] H. Xiang, L. Jianjun, A Digital Watermarking Algorithm for DEM Image Based on Stationary Wavelet Transform, *Fifth International Conference on Information Assurance and Security*, Vol. 1, pp. 221-224, 2009.
- [11] M. Makhloghi, F. Akhlaghian Tab, H. Danyali, A new robust blind DWT-SVD based digital image watermarking, 19th Iranian Conference on Electrical Engineering (ICEE), pp. 1-5, 2011.
- [12] R. K. Arya, S. Singh, R. Saharan, A Secure Non-blind Block Based Digital Image Watermarking Technique Using DWT and DCT, International Conference on Advances in Computing, Communications and Informatics, pp. 2042-2048, 2015.
- [13] N. Lin, J. Shen, X. Guo, J. Zhou, A robust image watermarking based on DWT-QR Decomposition, IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 684-688, 2011.

TABLE 3. The simulation results for Lena image. Extracted watermarks for both methods of [1] and our proposed method.

Extracted waterma	ark for the method in [1]	Extracted waterma	ark for our method
Rotation Attack, 30 Degrees	Scaling Attack	Rotation Attack, 30 Degrees	Scaling Attack
	Ō		Ō
Gaussian Noise	Gaussian Noise	Gaussian Noise	Gaussian Noise
Attack, V=0.01	Attack, V=0.02	Attack, V=0.01	Attack, V=0.02
Ō	Ō	Ō	0
Gaussian Noise	Gaussian Noise	Gaussian Noise	Gaussian Noise
Attack, V=0.03	Attack, V=0.04	Attack, V=0.03	Attack, V=0.04
Ô	Ø	\overline{O}	\bigcirc
Gaussian Noise	Jpeg2000 Com-	Gaussian Noise	Jpeg2000 Com-
Attack, V=0.05	pression	Attack, V=0.05	The second secon
Shot Noise	Salt & Pepper Noise	Shot Noise	Salt & Pepper Noise
\bigcirc	Ô	Ō	Ō
Crop	Speckle Noise	Crop	Speckle Noise
	Õ	Ō	Q

TABLE 4. The simulation results for Baboon image. Extracted watermarks for both methods of [1] and our proposed method.

Extracted watermark for the method in [1]		Extracted watermark for our method	
Rotation Attack, 30 Degrees	Scaling Attack	Rotation Attack, 30 Degrees	Scaling Attack
œ,	(\mathbb{C})		\bigcirc
Gaussian Noise	Gaussian Noise	Gaussian Noise	Gaussian Noise
Attack, V=0.01	Attack, V=0.02	Attack, V=0.01	Attack, V=0.02
	\bigcirc	0	0
Gaussian Noise	Gaussian Noise	Gaussian Noise	Gaussian Noise
Attack, V=0.03	Attack, V=0.04	Attack, V=0.03	Attack, V=0.04
\bigcirc	C	\bigcirc	\bigcirc
Gaussian Noise	Jpeg2000 Com-	Gaussian Noise	Jpeg2000 Com-
Attack, V=0.05	Pression	Attack, V=0.05	pression
Shot Noise	Salt & Pepper Noise	Shot Noise	Salt & Pepper Noise
C	C	\bigcirc	Ō
Crop	Speckle Noise	Crop	Speckle Noise
Ē,	Ō	Ō	Ō

TABLE 5. Comparison between our proposed method and the method in [15] on Baboon image (Note that the min and max values were obtained by variation of free parameters in each attack)

Type of Attack	Our Algorithm	Singh et al. [15]
Salt & Pepper Noise	0.9980	0.9099
Gaussian Noise	0.9926-0.9976	0.9326
Jpeg Compression	1	0.9189

TABLE 6. Comparison between our proposed method and the method in [16] on Lena image (Note that the min and max values were obtained by variation of free parameters in each attack)

Type of Attack	Our Algorithm	Xueyi et al. [16]
Salt & Pepper Noise	0.9966	0.8320-0.9354
Gaussian Noise	0.9941-0.9983	0.5628-0.9354
Jpeg Compression	1	0.7268-1.0000

- [14] K. Thongkor, N. Mettripun, T. Pramoun, T. Amornraksa, Image Watermarking Based on DWT Coefficients Modification for Social Networking Services, 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 1-6, 2013.
- [15] B. Singh, Dr. V.S. Dhaka, R. Saharan, Blind Detection Attack Resistant Image Watermarking, IEEE 3rd Global Conference on Consumer Electronics (GCCE), pp. 289-293, 2014.
- [16] Y. Xueyi, D. Meng, W. Yunlu, Z. Jing, A Robust DWT-SVD blind watermarking algorithm based on Zernike moments, *Communications Security Conference (CSC 2014)*, pp. 1-6, 2014.