# Adaptive Blind Wavelet-Based Watermarking Technique using Tree Mutual Differences over Wireless Sensor Network

Duaa Sh. Momani[1], Razan F. Shatnawi[2]
[1]Electrical Engineering Department, Jordan University of Science and Technology, Irbid-Jordan
[2] Electrical Engineering Department, Jordan University of Science and Technology, Irbid-Jordan

## ABSTRACT

This project presents an adaptive blind wavelet-based watermarking scheme using tree mutual differences (ABW-TMD). This watermarking scheme was innovated for image in wireless sensor network. by using Discrete Wavelet Transform (DWT) to hide watermark in frequency domain. The ABW-TMD scheme proves its robust in wireless sensor network, specially according to packet loss ratio parameter

***Keywords*** *- watermarking, Adaptive Blind Wavelet-Based Watermarking Technique using Tree Mutual Differences (ABW-TMD) wireless sensor networks (WSNs), wireless sensor multimedia networks (WSMNs).*

## I. INTRODUCTION

The with exponential telecommunication progress, the hackers and malicious intruders are a big problem in this field. So, it necessary needs technologies that prevent this problem. One of the most important achievements in the security field is a watermark technique. Watermarking means adding specific data into transmitted information where this data is known for only the wanted receiver and unknown for the others, so guarantee transmission authentication.

Watermark has to be robust enough against intentional or unintentional attacks, including compression, filtering, format conversion. Also watermark must be imperceptible to humans and be able to convey enough information for different purposes embedding watermark into image can be done by two ways: spatial (time) domain or spectral (frequency) domain. Where we can convert the digital data from time domain to frequency by: discrete time wavelet transform (DTWT), the discrete cosine transform (DCT) or the discrete Fourier transform (DFT). It is prefer to use spectral domain since this way is more robust against attacks. Most frequency-domain watermarking schemes are based on the additive spread-spectrum method, which is inspired by the spread-spectrum modulation technique in digital communication systems [1]. This technique provides more security and resistance to channel noise for digital communication. Similarly, the spread-spectrum watermarking scheme can resist more serious content distortion. The watermark is usually represented by a pseudo noise (PN) signal with low amplitude. The PN signal is either added to or subtracted from the host data and then detected later by using a correlation receiver or matched filter[2]. Our project used an adaptive blind wavelet-based watermarking technique using tree mutual differences over wireless sensor network. So we will talk briefly about Wireless Sensor multimedia Network (WSMN) and( WSN).

Wireless Sensor Networks (WSNs) have the capability for sensing, processing and wireless communication all built into a tiny embedded device. This type of network has drawn increasing interest in the research community over the last few years. This is driven by theoretical and practical problems in embedded operating systems, network protocols, wireless communications and distributed signal processing. The primary function of WSNs is to collect and disseminate critical data that characterize the physical phenomena within the target area. Depending on the application scenario[3].

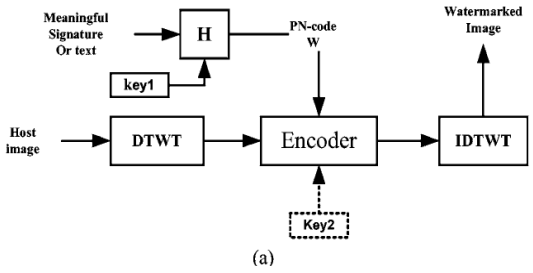
As a Wireless sensor multimedia networks (WSMNs) are an emerging type of sensor networks which contain sensor nodes equipped with microphones, cameras, and other sensors that producing multimedia content. These networks have the potential to enable a large class of applications ranging from military to modern healthcare. Since in WSMNs information is multimedia by nature

and it uses wireless link as mode of communication so this posse's serious security threat to this network. Thereby, the security mechanisms to protect WSMNs communication have found importance lately. However given the fact that WSMN nodes are resources constrained, so the traditionally intensive security algorithm is not well suited for WSMNs[4].

## II. Theoretical procedures

### 1. ABW-TMD concept:

The blind embedding procedure is illustrated in Fig1(a), where the input image is applied to a DTWT transformer; then the resulting wavelet coefficients are used to construct the wavelet trees in the encoder. Since the watermark Wn is a binary PN sequence of ±1, it can be generated by mapping the binary image into a sequence of binary data through a one-way deterministic function (scrambler). In the encoder, a decision rule is used to force the mutual tree difference to hold the incoming bits of the watermark sequence Wn. At the end, an inverse DTWT (IDTWT) transformer is used to restore the watermarked image. At the decoder side Fig1(b), assuming that the image has exposured to attacks (filtering, compression, etc.), the extracted watermark Wn' will be compared with the owner watermark Wn, and the decision is made based on the normalized correlation coefficient between Wn and Wn'. If the correlation coefficient is above the predetermined threshold, the watermark exists, else does not exists. The choice of the threshold depends on the desired false-positive alarm probability. As is clear from Fig1, there are two keys for the system: key1, which is used for scrambling the input watermark bits; and key2, which is generated for embedding the sequence as will be seen later. Here, key2 is generated based on some features of the wavelet trees, and its length defines the total number of bits that can be allowed for the watermark embedding.



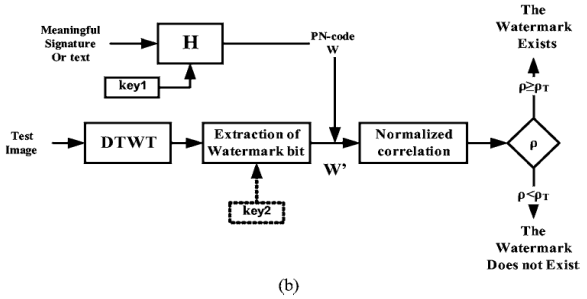




**Fig. 1 proposed watermarking (a) encoder and (b) decoder.**

### 2. Tree Construction:

In this scheme, a 4L-DTWT decomposition is implemented, as shown in Fig 2. A grayscale 512×512 image is used as a host image with 13 frequency bands. If L denotes the number of DTWT decomposition levels, there will be (L−1)×3+4=13 frequency bands with L=4. In each tree, there are 21 coefficients sorted, as pointed in Fig 3. The first coefficient will be from one of (LH4,HL4,HH4), the next four coefficients will be from (LH3,HL3,HH3), and the remaining 16 coefficients are obtained from (LH2,HL2,HH2). The total number of trees will be equal to the number of coefficients in LH4, HL4, and HH4. For example, if the host image is of size 512×512 pixels, we get 3072 trees. This enables us to embed up to 1536 watermark bits. Note that the number of embedded watermark bits is 1/2 of the constructed trees.

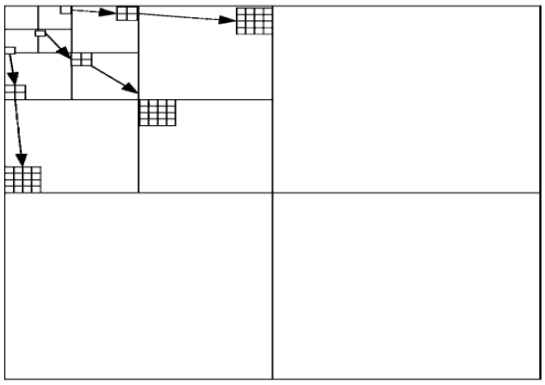


**Fig. 2 4L-DTWT decomposition of the host image illustrating of grouping wavelet coefficients .**

After the 3072 trees are being composed[ T(i , j) , i=1,2, . . .3072, j=1,2, . . . 21]. These trees are exploited into the embedding procedure in such a way to minimize the total embedding error by employing the mutual difference between tree pairs. As a first step, the difference between adjacent trees is computed using the following as seen in Fig3:

$$D_H^{old}(i) = \sum_{j=1}^{21} [T(i,j) - T(i+1,j)]$$

If the current $D_H^{old}$ (i) <Tdef, its position is accepted for

watermark embedding and the position is saved as a sequential value in key2. Consequently, the number and positions of the tree pairs that can accept watermark embedding are already determined. The length(size) of key2 defines the size of the watermark

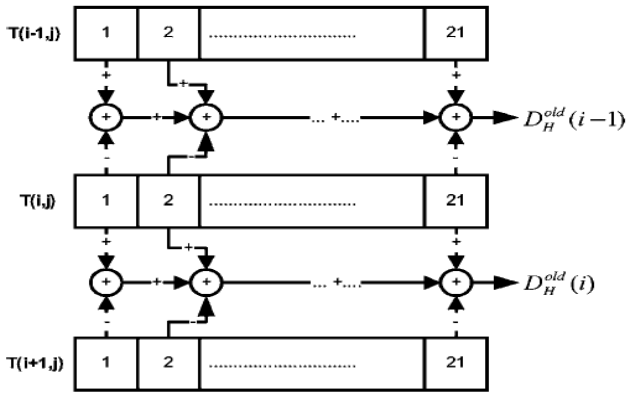



**Fig. 3 Bit host difference construction of 21 grouped coefficients**

### 3.Threshold Selection:

We adaptively update the current host difference DH(old)[key2(n)] to a new value DH(new)[key2(n)] depending on its ability to host a watermarking bit. It was found that THR can be defined as the minimum absolute host difference used to represent a bit in the corresponding tree pair host.

$$THR = \left| \sum_{i=1}^{3071} D_H^{old}(i) \right| / 3071 \qquad (1)$$

### 4. Watermark Embedding:

The watermark bit length {W(n):n=1,2,….Nw},

if the watermark bit W(n)=+1 then:

$D_H^{new}$ [key2(n)]={THR if $D_H^{old}$ [key2(n)] <THR

$D_H^{old}$ [key2(n)] if $D_H^{old}$ [key2(n)] > THR} (2)

If the first condition of above equation holds, then coefficients corresponding to the host tree pair are updated:

$T_H^{new}$ [key 2(n), j] $T_H^{new}$ [key 2(n) + 1,j] }=

{ $T_H^{old}$ [key 2(n), j] + {THR- $D_H^{old}$ [key2(n)] }/42

$T_H^{old}$ [key 2(n)+1, j] -{THR - $D_H^{old}$ [key2(n)] }/42 } (3)

Otherwise, the host tree pair is said to be self-embedded and does not need to be modified.

if the watermark bit W(n)=-1then:

$D_H^{new}$ [key2(n)]={-THR if $D_H^{old}$ [key2(n)] > -THR $D_H^{old}$ [key2(n)]

if $D_H^{old}$ [key2(n)] <-THR}

{ $T_H^{new}$ [key 2(n), j] $T_H^{new}$ [key 2(n) + 1,j] }=

{ $T_H^{new}$ [key 2(n), j]- {THR+ $D_H^{old}$ [key2(n)] }/42

$T_H^{new}$ [key2(n)+1,j]+{THR+$D_H^{old}$ [key2(n)]}/42} (4)

### 5. Getting the watermarked image:

After the host tree pairs have been modified, the achieved updates $T_H^{new}$ (i , j) , i∈ {1,2, . . .3072}, j∈ {1,2, . . . 21} can be used to regenerate the new modified wavelet coefficients by taking the IDTWT to obtain the watermarked image.

### 6. Blind Watermark Extraction Using the ABW-TMD:

After we have got the watermarked image and transmitted it, The ability to restore the watermark and

extract it will indicate how the system is robust and secure. As we mentioned in the embedding process, we have to find the host tree pairs (T'):

$$D'(n) = \{T'[key2(n),j]-T'[key2(n)+1, j]\} \quad (5)$$

$n \in \{1,2,\ldots Nw\}$

Since D'(n) was forced to carry the sign of the embedded watermark bit W(n), then the received watermark can be extracted using:

$$W'(n)=sign[D'(n)], \quad (6)$$

$n \in \{1,2,\ldots.Nw\}$

To quantify the relation between the original watermark and the extracted one, it is useful to use the normalized correlation coefficient:

$$P=( W(n)W'(n) ) / Nw \quad (7)$$

## III. EXPERIMENTAL EXECUTION

First we simulated grayscale Lena test image of the size 512*512 pixels and 8 bits/ pixel resolution by adaptive blind wavelet-based watermarking scheme using tree mutual differences (ABW-TMD). Then, we applied the image to packet loss ratio during wireless sensor network. The figure below appears watermarked Lena image before applying WSN parameter such as Packet Loss Ratio (PLR).

**Fig.4 Lena image (a) original image (b) watermarked image**

According to different values of threshold so different watermark bit size (Nw), we had several values of peak signal to noise ratio (PSNR). Figure 5 explains the resulting relation using ABW-TMD technique .

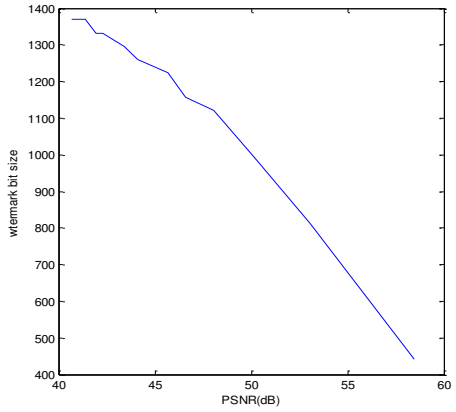



**Fig.5 watermark size Vs PSNR in Lena watermarked image**

Now the ABW-TMD is examined by WSN channel with various values such as the PLR. To find the amount of PLR, we divided the image into 4-by-4 sub-block, so we have 16384 sub-block. And assumed every sub-block is representing by one packet. Then, we found the watermark correlation depends on increasing PLR (i.e. make more packets equal zero) gradually. The resulting relation was as seen in figure 6. correlation depends on increasing PLR (i.e. make more packets
equal zero) gradually. The resulting relation was as seen in figure 6.

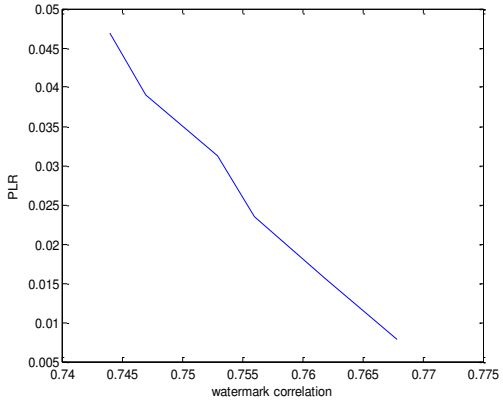



**Fig.6 watermark correlation with different values of packet loss ratio(PLR)**

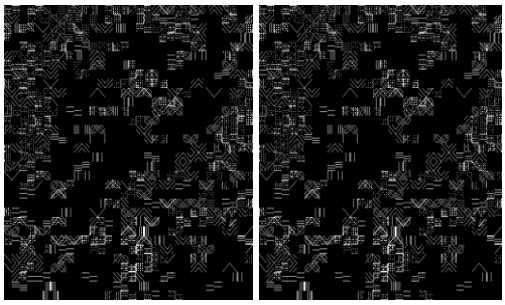


**Fig.7 Embedding error in frequency domain: (a) without PLR (b) with PLR**

From figure 6, we can note that the PLR did not affect the robustness of watermark since the values of watermark correlation are still high. So ABW-TMD may achieve excellent performance in WSNs. And from embedding error as in figure 7 seems that the different is unnoticeable before and after PLR.

Figure 8 shows the difference between original watermarked image and the image which has PLR in time domain, after increased the contrast to the image to be noticeable.

**Fig.8 the difference between original image and the image after PLR.**

## IV. CONCLUSION

An adaptive blind wavelet-based watermarking scheme using tree mutual differences (ABW-TMD) is proposed by exploiting mutual differences between the grouped coefficients of tree pairs, each watermark bit is embedded by introducing a predetermined difference between each tree pair, and that new host difference carries the same sign of the embedded bit. The ABW-TMD encoder adaptively searches for the bit host difference in such a manner to minimize bit embedding error. At the encoder same procedure was done, using the sign of the difference of the host to extract the watermark. .After that the image was divided into sub block and transmitted over WSN then the PLR was calculated. Good result of correlation at different PLR was achieved. This scheme may improve the algorithm of watermark by rearranged the coefficient in descending order and hope to study the effect of algorithm on energy .

## REFERENCES

[1] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "*DCT-Based watermark recovering without resorting to the uncorrupted original im- age*", Proc. IEEE Intl. Conf. Image Process. (ICIP) 1, 520–523(1997).

[2] I. J. Cox, F. T. Leighton, and T. Shamoon, "*Secure spread spectrum watermarking for images, audio and video*", Proc. IEEE Intl. Conf.I mage Process. (ICIP), pp. 243–246 (1996).

[3] B Harjito , SHan, V Potdar, EChang, M Xie "*Secure Communication in Wireless Multimedia Sensor Networks using Watermarking*". IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010).

[4] S. Wang and Y. P. Lin, "*Wavelet tree quantizing for copyright protection watermarking*," IEEE Trans. Image Process. 2(3), 154–165(2004).

[5] H. Otum, N. Samara, " *Adaptive blind wavelet-based watermarking technique",* 2006