An Efficient Blind Watermarking Method based on Significant Difference of Wavelet Tree Quantization using Adaptive Threshold

Thien Huynh The
University of Technical Education Ho Chi Minh City, HCM City, Vietnam
Email: thethien2208@gmail.com

Thuong Le Tien
Ho Chi Minh City University of Technology, HCM City, Vietnam
Email: thuongle@hcmut.edu.vn

Abstract—**In this research, we introduce an efficient blind watermarking method for gray image based on wavelet tree quantization using adaptive threshold in extraction process. Based on difference value between two largest coefficients, each scrambled binary watermark bit is embedded into each block which created by four LH3 coefficients and one LH4 coefficient. In extraction process, we compare difference value in each block to adaptive threshold to recover watermark bit. The quality of extracted watermark depends on the threshold which is determined by the Weighted Within-Class Variance algorithm. Performance of proposed method is represented through experimental results under various attacks such as, Histogram Equalization, Cropping, Low-pass Filtering, Gaussian noise, Salt & Pepper noise and JPEG compression.**

Index Terms—**blind watermarking, 3-level DWT, significant difference, adaptive threshold, within-class variance**

I. Introduction

Due to the advantage of the Internet, people can arbitrarily and access or distribute digital products. Hence, the digital watermarking technique has been used in multimedia products to protect copyright and authenticate image... This technique embeds information into the digital contents so that the viewer cannot see any information. However, there are many problems in the watermarking system: the watermark has to ensure not degrading the quality of the cover image and being perceptually invisible for human eyes; the watermark must be robust to resist different attacks and the watermarking system is blindness.

Several wavelet tree-based watermarking methods are proposed based on the qualified significant wavelet tree (QSWT) [1, 2, 4, 5, and 6]. In [1], the authors embedded watermark in each of two sub-bands of wavelet tree. The authors in [2] improved the method in [1] by using four trees to represent two watermark bits to enhance visual quality. But this method's disadvantage is that it cannot effectively resist low-pass filtering attacks such as median filtering and Gaussian filtering. The authors in [3] proposed the method based on significant difference quantization technique; that is, every seven-wavelet coefficients in 3-level DWT sub-band was grouped as a block and the watermark bit is embedded by quantizing the difference between two largest coefficients. Based on insignificant coefficients of a wavelet tree, the authors proposed the method that improved the quality of the watermarked image, but the quality of recovery watermark was decreased. An intelligent watermarking method based on particle swarm optimization (PSO) in [5] is the improved method in [3]. This method has been resolved the conflict between imperceptibility and robustness of watermarking by selecting randomly coefficients to make up a block to avoid the watermark being detected and the strength of embedding watermark among different blocks is adaptive by PSO method to balance the robustness and perceptual transparency. By scaling the magnitude of the significant difference between the two largest wavelet coefficients in a wavelet tree, the authors [6] improved the robustness of the watermarking. However, extracted watermark cannot ensure the quality under JPEG compression. Embedding the information into the significant wavelet coefficient in those dynamic blocks with strong edges according to a "Binary Algorithm" was proposed in research [7]. Since the change to the blocks with strong edge strengths is less visible to human eyes. The threshold in extraction process was limited by the demanded size of the watermark.

The authors in [8] used wavelet packet decomposition technique for both the original image and the watermark by embedding watermark into low-frequency sub-band and comparing the correlation between recovery and original watermark to decide the existence of watermark. The authors in [9] suggested a method that using statistical characteristics of coefficients to quantize. This method used two quantization algorithm for two phases of watermarking system. Using the same method, the

Manuscript received February 10, 2013; revised May 20, 2013.

doi: 10.12720/ijeee.1.2.98-103

authors in [10] embedded watermark by modifying the center coefficient in each block and the value of this coefficient depend on the watermark bit and the mean of four cross neighbor coefficients. Another way to group was represented in [11]: LH3 and HL3 sub-band are divided into equal four sections. Each block was grouped by one coefficient in each section. Before that, the basic method is proposed in [12] embedding each watermark bit by comparing the difference of two largest significant coefficients in each wavelet tree to the average value. The maximum coefficient was modified based on value of watermark bit. In [13], the authors embedded each pixel of watermark into the wavelet coefficient of middle and low frequency of a block in the cover image. However, the proposed method is non-blind watermarking system; that is, using original image for extraction process. Additions, the authors in [14] used a re-watermarking approach employing blind, quantization-based and robust technique to embed multiple fingerprinting. They investigated two extensions to a wavelet coefficient-tree based embedding technique that turn out to improve detection performance.

In this research, an efficient blind watermarking method for image based on the significant difference of wavelet coefficients is developed from [3]. Due to the importance of determining threshold value in extraction process, this value could be determined based on the probability density function (pdf) of blocks along difference values instead of proposed algorithm in [3]. By computing the weighed within-class variance [15], we separate *pdf* plot into two parts and the difference value chosen as threshold has minimum variance. Simulation results under different attack cases demonstrate method's performance through PSNR of embedded image and NC of extracted watermark.

II. The Proposed Method

A. The Watermarking Method

Watermarking model is represented in Fig. 1. The watermark after scrambling with security key will be hid into the host image. We decompose this image at 4-level DWT to four sub-bands. Based on the wavelet tree technique, three are three super wavelet trees: HH3-HH3-HH2-HH1 is easily eliminated when using the JPEG lossy compression. HL4-HL3-HL2-HL1 is suitable to embed the watermark in this paper to satisfy extracting watermark under different attacks instead of LH sub-band family. To limit computing capacity, we only choose HL4 and HL3 for embedding process.

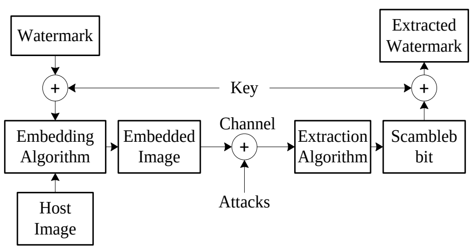


Figure 1. Watermarking model.

We have size of HL3 after decomposing is 64×64 when using 512×512 image. There are 512 watermark bits are embedded into 512 blocks, which are grouped based on wavelet tree as Fig. 2; that is, one coefficient of HL4 and four coefficients of the same orientation in the same location in HL3 are grouped as a block. Each wavelet tree consists of coefficients for a wavelet tree constructed at each node from HL4 to HL3. Each 4-level sub-band, we have 1024 coefficients which is the maximum number of watermark can be embedded.

However, due to watermark with size (16×32), we only need 512 blocks in embedded and extraction algorithm. For embedding process, we modify the maximum coefficient by the fixed quantity, – called quantization value, based on the significant difference of two largest coefficients in each block and value of watermark bit. This value is the mean of all significant difference values of all image used. For one image, we can find this value ε as follows:

$$\varepsilon = \frac{1}{N}\sum_{i=1}^{N}(max_i - sec_i) \qquad (1)$$

where N: number of blocks, max_i and sec_i are two largest coefficients in i^{th} block. For many images, we have:

$$T = \frac{1}{m}\sum_{j=1}^{m}\varepsilon j \text{ ....(2)}$$

where m: number of images. The images are considered in simulation include Lena, Baboon, Pepper, Goldhill and Sailboat. The value of each image and average of them is represented in TABLE I. The quantization value used in this paper is the mean of all above images.

TABLE I. Quantization Value of Each Image

Image	Lena	Baboon	Pepper	Goldhill	Sailboat	*T=Average*
ε	25	41	38	38	58	40

B. The Embedding Process

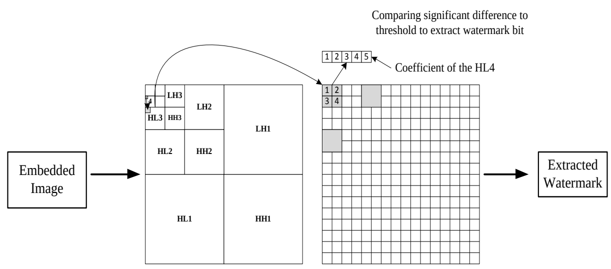


Figure 2. Embedding watermark based on wavelet tree quantization

The watermark image used to embed into the host gray image has size 512 bits with value 0 or 1. After scrambling watermark with security number, each bit will be embedded into each block, respectively. Each block have five coefficients (4 HL3 coefficients + 1 HL4 coefficient) is created after decomposing (512×512)

gray image. In each block, we seek two values: max_i - the largest coefficient and sec_i - the second largest coefficient and significant difference $\delta_i = (max_i - sec_i)$. For i^{th} bit of watermark, we perform the embedding algorithm as the following steps for i^{th} block:

With watermark bit 1:

$$max_i \left\{ \begin{matrix} max_i + \Delta; if\ (\delta_i \le T) \\ max_i \quad ; if\ (\delta_i > T) \end{matrix} \right\} \tag{3}$$

where $\Delta = T - \delta_i$

With watermark bit 0:

$$\begin{aligned} max_i &= max_i - \delta_i / 2 \\ \sec_i &= \sec_i - \delta_i / 2 \end{aligned} \tag{4}$$

The quality of embedded image depend on value T in the case we use same watermark. The detailed of embedding process can be showed in Fig. 3.

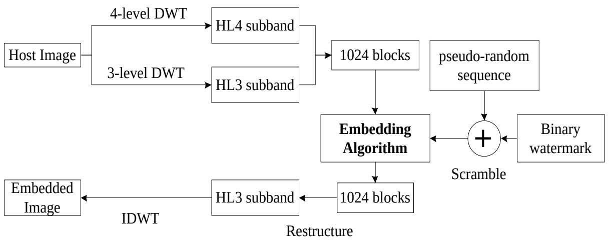


Figure 3. The flowchart of embedding process.

C. The Extraction Process

Watermark bit embedded into each block can be recovered based on comparing significant difference to threshold - denoted as ρ. After embedding, difference in each block of cover image will be 0 or larger than T as (3) and (4). In with non-attack case, watermark is extracted exactly when the threshold in the range $(1 \le y \le \varepsilon)$. However, this value can be changed in different attack cases; that is, extracted bit is 1 instead of 0. When find out the threshold ρ, we can extracted as below equation:

$$bit_i = \left\{ \begin{matrix} 0 \quad ; if\ (d_i < \rho) \\ 1 \quad ; if\ (d_i \ge \rho) \end{matrix} \right\} \tag{5}$$

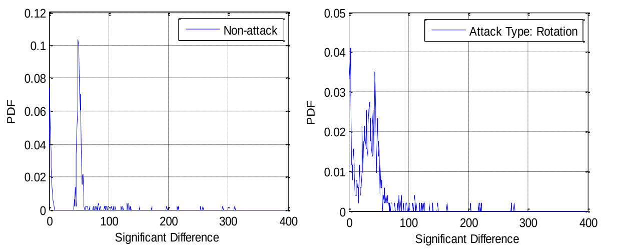


Figure 4. Probability density function $x(n)$ of significant difference of cover image

We can consider the probability density function $x(n)$ of significant difference in Fig. 4. The function $x(n)$ represents the number of block having the same difference value. Without attacks, we can determine the threshold value to extract watermark exactly. However, the change of pdf is very light under some attacks, such as, histogram equalization, Gaussian filter; otherwise, some attacks affect pdf extreme seriously, such as average filter. In these cases, we cannot extract correctly encoded watermark; it can be explained that the watermark bit 0 are embedded, significant differences will be 0; however under various attacks, they are larger than value ε.

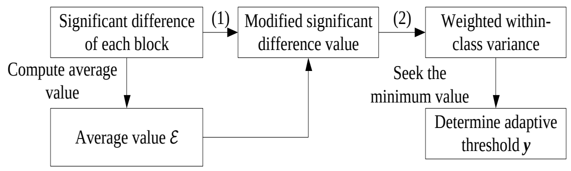


Figure 5. The flowchart for determining threshold

In this paper, we proposed an algorithm to determine adaptive threshold based on computing the weighed within-class variance. In more detail, we find the threshold that gets minimized the weighted within-class variance, or this turn out to be the same as maximizing the between-class variance. However, we need to modify significant difference of the blocks which have $d_i > \varepsilon$. This preprocess does not affect the quality of recovery watermark because these blocks will extract exactly since threshold value is always less than ε. The proposed algorithm for determining threshold is showed in Fig. 5. The process (1) in Fig. 5 can be performed as follows:

$$d_i = \left\{ \begin{matrix} d_i \quad ; if\ (d_i \le \varepsilon) \\ \varepsilon \quad ; if\ (d_i > \varepsilon) \end{matrix} \right. \tag{6}$$

The detailed process (2) in Fig. 5 can be calculated as:

$$\sigma_w^2(d) = W_0(d)\sigma_0^2(d) + W_1(d)\sigma_1^2(d) \ldots\ldots (7)$$

where class probabilities $W_0(d)$ and $W_1(d)$ are estimated:

$$\begin{aligned} W_0(d) &= \sum_{i=1}^{d} p(i) \\ W_1(d) &= \sum_{i=d+1}^{max(d_i)} p(i) \end{aligned} \tag{8}$$

And the class means are given by:

$$\begin{aligned} \mu_0(d) &= \sum_{i=1}^{d} \frac{i \times p(i)}{W_0(d)} \\ \mu_1(d) &= \sum_{i=d+1}^{max(d_i)} \frac{i \times p(i)}{W_1(d)} \end{aligned} \tag{9}$$

Finally, the individual class variances are:

$$\sigma_0^2(d) = \sum_{i=1}^{d} \left((i - \mu_0(d))^2 \frac{p(i)}{W_0(d)} \right) \tag{10}$$

$$\sigma_1^2(d) = \sum_{i=d+1}^{max(d_i)} \left((i-\mu_1(d))^2 \frac{p(i)}{W_1(d)} \right)$$

These calculation steps were done through the range of value $d_i \in [0, max(d_i)]$ and pick out the value that minimized $\sigma \frac{2}{W}(d)$. The adaptive threshold is the significant difference value which has $(\sigma \frac{2}{W} = min)$. If there are many values, the threshold will be the mean of them:

$$\rho = mean(d / \sigma_W^2(d) = min) \tag{11}$$

After determining adaptive threshold, we use (5) to extract watermark.

III. Experimental Result

We use the peak signal-to-noise ratio PSNR to evaluate the quality between embedded image and original image. This formula is defined as follows:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE}) \tag{12}$$

where MSE is computed as below equation:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M}\sum_{j=1}^{N} \left(I(i,j) - I'(i,j) \right)^2 \tag{13}$$

where M and N are height and width of the image, respectively. $I(i,j)$ and $I'(i,j)$ are the grey value located at coordinate (i,j) of the original image and embedded image. After extracting, estimation for quality of extracted watermark is compared to the original watermark is express according the normalized correlation NC value:

$$NC = \frac{1}{m \times n} \sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j) \times w'(i,j) \tag{14}$$

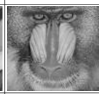
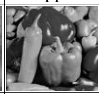
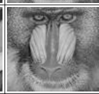
where $m \times n$ is the watermark of size. $w(i,j)$ and $w'(i,j)$ are the values located at coordinate (i,j) of original watermark and extracted watermark. Value of $w(i,j)$ is set 1 if it is a watermark bit 1, otherwise, it is set -1 and similar to $w'(i,j)$. So the value of $w(i,j) \times w'(i,j)$ is either 1 or -1. If number of bit extracted correctly is larger than 50%, the NC value is positive; otherwise, it is negative.

A. *With Non-Attack*

In below the simulation, the gray-images used as cover images have size (512×512) and watermark is the binary image with size (16×32). Additions, we apply the Haar wavelets to decompose and reconstruct to cover image. Simulation result of embedding process showed in TABLE.II, all cover images in this simulation get good invisibility (PSNR larger than *41dB*).

In the non-attack case, the watermark image is extracted from the cover image according using proposed determining threshold algorithm. Table. II shows the quality of recovered watermark with *NC=1* for all images.

TABLE II. Result of Embedded Image and Recovery Watermark

Image	Lena	Baboon	Pepper	Goldhill	Sailboat
Original Image					
Embedded Image					
PSNR	45.86	46.88	44.00	44.53	41.64
Watermark	2013	2013	2013	2013	2013
MSE	1.0000	1.0000	1.0000	1.0000	1.0000

B. *With Geometric Attacks*

Under various attacks, we only use image **Lena** for simulation. There are some geometric attack types are considered in this simulation, such as, cropping, scaling, rotation and Gaussian noise. For the cropping attack, $1/4$ pixel of image is dropped at the center of embedded image and they are replaced by gray value 0 pixels. In the scaling case, the host image is scaled to (256×256) and then scale one more time to original size. For two last attack types, the cover image is rotated by small degree and added Gaussian noise with many different variances. The result of watermarking under geometric attacks is showed in Table. III. With the larger value T, the robustness of watermark will be increased but the invisibility of host image will be reduced. There is a tradeoff between the robustness of watermark and the transparency of host image.

TABLE III. NC of Extracted Watermark Under Geometric Attacks

Attack Type	Cropping	Scaling	Rotation 0.25^0	Gaussian Noise
PSNR	11.67	33.88	29.44	28.1692
Watermark	2013	2013	2013	2013
NC	0.64	0.99	0.86	0.86

C. *With Non-Geometric Attacks*

TABLE IV. NC of Extracted Watermark Under Non-Geometric Attacks

Attack Type	Histogram Equalization	Gaussian Filter	Median Filter (3×3)	Average Filter (3×3)	Sharpening
PSNR	19.12	39.86	35.14	33.58	25.27
Watermark	2013	2013	2013	2013	2013
NC	0.88	0.98	0.97	0.95	0.88

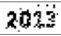
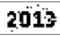
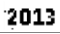
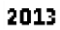
There are some non-geometric attacks: Histogram Equalization, Gaussian filter, Median filter, Average filter, sharpening. Based on the experiment result represented in Table. IV, the proposed method has a good resistance to many non-geometric attacks.

D. With JPEG Compression

TABLE.V showed the simulation result in JPEG lossy compression with quality factor from 10 to 60 . When we compress the image with quality factor 10%, although the size on disk of image is very small, NC value of watermark is always greater than 0.57 and NC=1 for 60%.

E. Comparing to The Other Methods

TABLE V. NC OF EXTRACTED WATERMARK UNDER JPEG COMPRESSION

Quality Factor	10%	20%	30%	40%	50%	60%
PSNR	30.23	32.77	33.97	34.76	35.40	35.98
Watermark						
NC	0.57	0.87	0.94	0.99	0.99	1.00

We compare our proposed method with some recently published papers: Lin et al [3], Wang et al [5], Run et al [6]. In our method, the experimental result is far better than the listed method, especially for JPEG lossy compression, scaling, rotation, low-pass filter, histogram equalization. Only cropping and sharpening, the proposed method is not good. Comparison is represented in TABLE.VI.

TABLE VI. COMPARING PROPOSED METHOD TO THE OTHER METHODS

Attack Type	Lin et al [3] (PSNR=44.25dB)	Wang et al [5] (PSNR=45.9dB)	Run et al [6] (PSNR=42.98dB)	Proposed 2 (PSNR=43.20dB)
Cropping ¼	0.70	0.76	0.68	0.64
Scaling	0.86	0.91	0.86	0.99
Rotation 0.25^0	0.67	0.75	0.65	0.86
Rotation 0.30^0	0.57	0.68	0.58	0.79
Gaussian filter	0.86	0.96	0.95	0.99
Histogram Equalization	0.77	0.82	0.86	0.88
Sharpening	0.99	1.00	0.99	0.88
Median filter (3×3)	0.88	0.95	0.93	0.97
Median filter (5×5)	0.74	0.86	0.84	0.87
Average filter (3×3)	0.91	0.97	0.95	0.95
Average filter (5×5)	0.72	0.86	0.80	0.75
JPEG (QF=10)	0.41	0.41	0.32	0.57
JPEG (QF=20)	0.68	0.74	0.68	0.87
JPEG (QF=30)	0.87	0.90	0.85	0.94
JPEG (QF=40)	0.95	0.97	0.93	0.99
JPEG (QF=50)	0.98	0.99	0.96	0.99

IV. CONCLUSION

In this research, we propose an efficient blind watermarking for digital image when using the adaptive threshold algorithm in extraction process. This threshold is given based on computing weighted -within class variance through considering probability density function of significant difference. The proposed method is considered in simulation under different attack types. The proposed method in this paper has good imperceptibility through PSNR – peek signal-to-noise ratio parameter (PSNR>41dB) and effectively resist many attacks, such as, Gaussian filter, Median filter, Average filter (NC - Normalized Correlation of extracted watermark larger than 0.95) and JPEG compression (NC=0.87 for QF=30%). However, this method is weakly at some geometric attacks: cropping, Gaussian noise.

REFERENCES

[1] M. Hsiel, D. Tseng, and Y. Huang, “Hiding digital watermarks using multiresolution wavelet transform,” *IEEE Trans. Ind. Electron*, vol. 48, pp. 875–882, Oct. 2001.

[2] B. K. Lien and W. Lin, “A watermarking method based on maximum distance wavelet tree quantization,” in *Proc. 19th Conf. Computer Vision, Graphics and Image Processing*, pp. 269-276, 2006.

[3] W. H. Lin, S. J. Horng, T. W. Kao, P. Fan, C. L. Lee, and Y. Pan, “An efficient watermarking method based on significant difference of wavelet coefficient quantization,” *IEEE Transactions on multimedia*, pp. 746–757, Aug. 2008.

[4] W. H. Lin, Y. Rau, and S. J. Horng, “A wavelet-tree-based watermarking method using distance vector of binary cluster,” *Expert Systems with Applications*, pp. 9869–9878, 2009.

[5] Y. R. Wang, W. H. Lin, and L. Yang, “An intelligent watermarking method based on particle swarm optimization,” *Expert Systems with Applications 38*, pp. 8024–8029, 2011.

[6] R. S. Run, S. J. Horng, W. H. Lin, T. W. Kao, P. Fan, and M. K. Khan, “An efficient wavelet-tree-based watermarking method,” *Expert Systems with Applications*, pp. 14 357–14 366, 2011.

[7] M. Keyvanpour and F. M. Bayat, “Bind image watermarking method based on chaotic key and dynamic coefficient quantization in the dwt domain,” *Mathematical and Computer Modelling (2012)*, doi:10.1016/j.mcm.2012.07.008.

[8] A. Ding and S. Dong, “Algorithm of Digital Image Watermark Based on Decomposition of Wavelet Packet,” *2012 Sixth International Confer-ence on Internet Computing for Science and Engineering*, pp. 135–137, 2012.

[9] K. Byun, S. Lee, and H. Kim, “A watermarking method using quanti-zation and statistical characteristics of wavelet transform,” *PDCAT 2005. Sixth International Conference on Parallel and Distributed Com-puting, Applications and Technologies*, pp. 689–693, Dec. 2005.

[10] L. Fan and T. Gao, “A Novel Blind Robust Watermarking SchemeBased on Statistic Characteristic of Wavelet Domain Coefficients,” in *Proc. International Conference on Signal Processing Systems*, pp. 121–125, May 2009.

[11] M. Hajizadeh, M. S. Helfroush, and M. J. Dehghani, “A Novel Blind Watermarking Method Based on Distance Vector of Significant Wavelet Coefficients,” *6th Iranian Machine Vision and Image Process-ing (MVIP)*, pp. 1–6, Oct. 2010.

[12] P. Liu and Z. Ding, “A Blind Image Watermarking Scheme Based on Wavelet Tree Quantization,” *Second International Symposium on Electronic Commerce and Security*, vol. 1, pp. 218–222, May 2009.

[13] J. Huang and C. Yang, “Image Digital Watermarking Algorithm Using multiresolution Wavelet Transform,” *2004 IEEE International Conference on Systems, Man and Cybernetics*, vol. 3, pp. 2977–2982, Oct. 2004.

[14] J. H. Uhl, C. Koidl, and A. Uhl, “Multiple Blind Re-watermarking with Quantization-Based Embedding,” in *Proc. 18th IEEE International Conference on Image Processing*, pp. 265–268, 2011.

[15] Y. Qiao, Q. Hu, G. Qian, S. Luo, and W. L.Nowinski, “Thresholding based on variance and intensity contrast,” *The journal of the pattern recognition society*, vol. Pattern Recognition 40, pp. 596–608, 2007.

Thuong Le Tien was born and grew up in Saigon, now is Ho Chi Minh City – Vietnam. He got Bachelor Degree in Engineering from the University of Technology, Vietnam in 12-1980, since then he has been with the Electronics & Telecommunications Department, Ho Chi Minh City University of Technology. He spent 3 years in the Federal Republic of Germany as a visiting scholar at the Ruhr University of Bochum from 1989 until 1992. He received the Ph.D. in Telecommunications from the University of Tasmania, Australia in 1998. He served as Deputy Department Head for many years and has been the Telecommunications Department Head since 1998. He has also appointed for the second position as the Director of Center for Overseas Studies since 1998.

His areas of specialization includes: Communication Systems, Signal Processing and Electronic Circuits.

Thien Huynh The was born in Bentre province, Vietnam in 1988. He received the B.E degrees from the University of Technical Education Ho Chi Minh City (HCMUTE), HCM City, Vietnam in 2011. He is currently pursuing the M.E degree at Faculty of Electrical & Electronics Engineering, HMCUTE.
His research interests are signal processing, digital watermarking, and hiding information.