Multiple Watermarking with Biometric Data Using Discrete Curvelets and Contourlets

Hoan Nguyen-Thanh, Thuong Le-Tien, and Thang Nguyen-Duy
Dept. of Electronics Engineering, University of Technology, Ho Chi Minh City, Vietnam
Email: {hoannguyen1609, nguyenduy.thang10}@gmail.com, thuongle@hcmut.edu.vn

***Abstract*—The use of biometric data to increase the robustness and security of private data has been mentioned and studied extensively. The multiple watermarking approach has proposed in this paper aims to improve the security of biometric data features; we consider using multiple watermarking techniques with fingerprint, face, iris and signature features. Before embedding, the fingerprint feature extracted by Minutiae with Gabor filter enhancement. Iris feature is extracted by Daugman Gabor filter. Face and signature features are extracted through a Gabor filter that combines PCA. Then the features of Iris and Fingerprint are mixed together, called iris-finger. And facial and signature features are also mixed together in terms of coefficients, called face-sig. The iris-finger feature set is embedded in the *curvelet* coefficients at level 1. The face-sig feature set is embedded in curvelet coefficients at level 2. All features of the fingerprint, iris, face and signature are used for authentication and copyright protection if there are attacks. the results have been also compared to others approaches.**

***Index Terms*—biometric features, multilevel discrete curvelet transform, contourlet transform, multiple watermarking, daugman gabor filter, gabor wavelet, minutiae, PCA**

I. Introduction

The development of modern science and technology; as well as the rapid increase of communication technologies, poses problems of copyright and security authentication. In particular, Digital watermarking allows embedding of hidden information into digital data. The Biometrics features contain individual characteristics. It is used for an individual verification and authentication [1] to improve security and sustainability, in watermarking [2], to embed digital images via DWT 4 level, or other techniques [3], [4]

The current watermaking methods largely use original images, as well as text information, digital images, video and audio [3], [5], [6]. The review aims to change watermark information in different combinations such as Othman & Ros's IrisPrint [7]. And multiple watermaking methods like Rohit Thanki [8] use a variety of biometric features with embedded methods of embedding different features on different discrete curvelet transform frequencies. However, we are concerned that separating features at different frequencies can lead to unsustainability when attacks eliminate those frequencies. In another work by Thien Huynh-The [2] on improving the optimization of watermarking techniques, he mentions embedding coding information into 4-DWT blocks, to improve the complexity and sustainability of watermarking information. before the attack. It has also been compared to SVD and DWT in ref [9].

Multiple watermarking technique uses a variety of features to protect one or more of the original information, such as using fingerprint, iris, face or signature simultaneously embedded on the original image [3, 5, 8, 10, 11, 12]. This helps ensure the robust, reliable, and robust requirements of confidential information. Multiple watermarking techniques can be divided into the following categories: Composite Watermarking, Segmented Watermarking, Successive Watermarking; it's described as the refer [8].

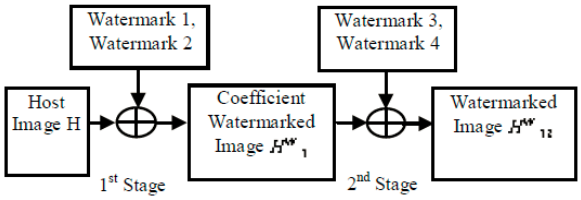


Figure 1. Propose combine composite and successive multiple watermarking.

In this paper, we combine both methods: Composite Watermarking and Successive Watermarking, as shown in Fig. 1. Firstly, we integrate the feature of iris-fingerprint and face-signature pairs, then use Multilevel Discrete Curvelet Transforms (references [13, 14, 15]) and Contourlet (references [16, 17]) to decompose the original image with 2 levels. Iris-fingerprint embedded at level 1, then use decomposition coefficient and embedded face-signature at level 2.

II. Referenced Watermarking Technique

According to a study by Rohit Thanki and his colleagues, the multiple watermarking technique uses biometric features extracted from original information such as iris, fingerprint, face and signature, using ISEF Shen-Castan edge detection and Principal Component Analysis (PCA). Features are given the same size and are embedded in the original image based on Fast Discrete Curvelet Transform (FDCT) [8]. The schema is as follows in Fig. 2:

Manuscript received March 14, 2018; revised August 2, 2018.

doi: 10.18178/joig.6.2.122-126

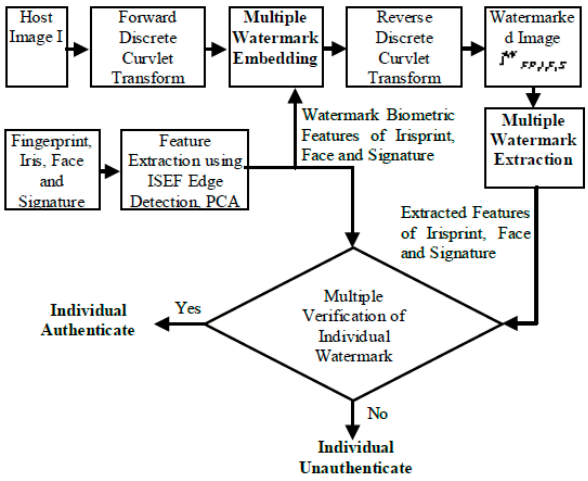


Figure 2. Block diagram of reference watermarking technique.

Watermark information are extracted as a PCA feature then each feature is embedded in the FDCT wrapping at different frequencies. The method enables rapid watermarking through an FDCT transform. However, the method of limiting the extraction of the features of each biometric data are different, requiring appropriate extraction techniques and the ability to recognize this information as needed. In addition, embedding different frequencies can lead to vulnerabilities that damage the watermark at certain frequencies.

III. Proposed Watermarking Technique

In this paper, we embed multiple biometric features into an original image. Forms of attack include compression, histogram, watermarked image editing. Implementing a combination of attributes into a different domain and embedding one at a time will have limitations. Therefore, we consider this technical proposal watermarking.

The watermark embedding technique is shown in Fig. 3. We set out the problem of combining Composite Watermarking and Successive Watermarking. In this technique, the fingerprint feature is extracted through Gabor and Minutiae filters; Iris feature extracted through Daugman Gabor filter (ref [18]); Face feature filtered through PCA and Gabor algorithms; Signature filtered through Gabor. The results are extracted in the form of Gabor matrix, these Gabor coefficients are combined in pairs (Fingerprint + Iris, Face + Signature), the composite feature set will be embedded in the original image at different levels.

In that, original image will be decomposed to 2 levels using Multilvel Discrete Curvlet or Multilevel Contourlet Transform. At level 1, the transform coefficients are embedded with the feature set iris-finger; Then, get the result, continue decomposing at level 2. At level 2, the coefficients are embedded with the feature set face-sig. Finally, to do the reverse level 2 transform, we obtain the watermarked image.

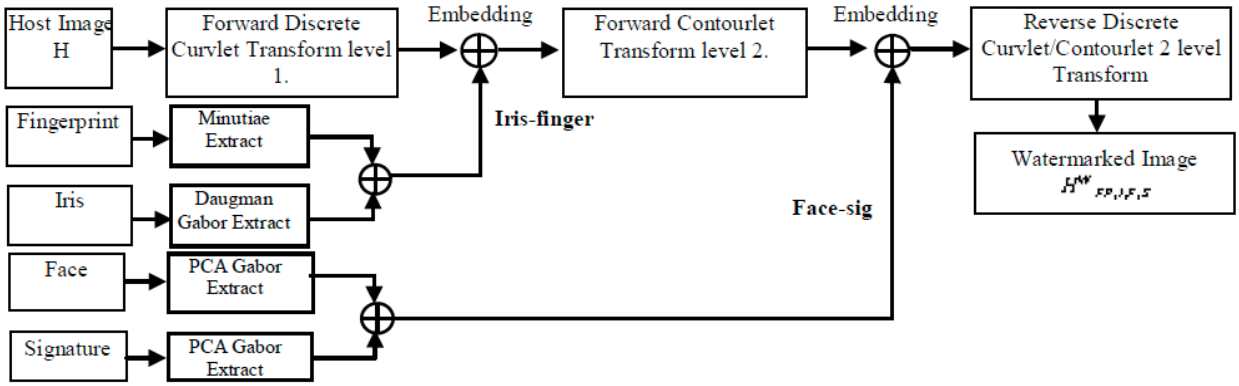


Figure 3. Block diagram of proposed embedding multiple watermarking technique.

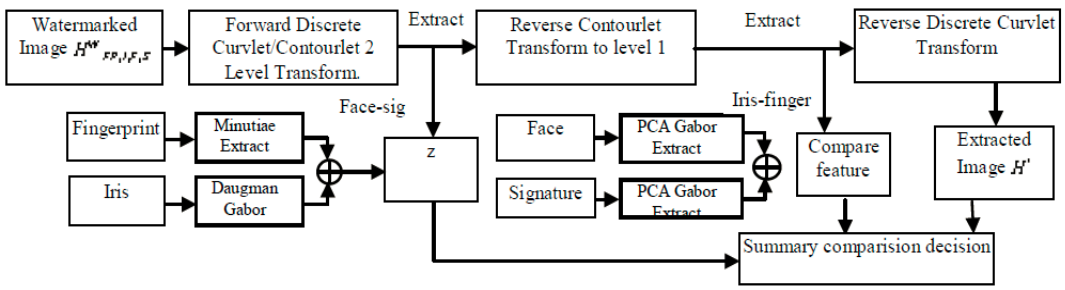


Figure 4. Block diagram of proposed extraction multiple watermarking technique.

The biometric data feature will be saved and used in extracting and comparing properties separated from the watermarked image, as shown in Fig. 4. The watermarked image is decomposed at level 2 to separate the attribute set. Face-sig first, then reverse at level 1 to separate the Iris-Finger attribute, the opposite process of embedding.

Both sets of attributes are parsed back to their original attributes: Face, Signature, Iris and Finger Feature. We

compared the extracted attribute sets with the original attribute set to evaluate criteria such as PSNR, SSIM for attack detection, sustainability, and security of the method.

A. Feature Extraction of Biometric Watermarks

With various extraction methods as mentioned in [3, 10, 13, 14, 15, 16, 12, 19, 20], in which we consider the extraction ability of the Gabor filter bank, they are performed based on frequencies, orientations and Gaussian factor. In this paper, we propose a new approach to the Gabor filter bank, the filter that creates a compact Gabor filter bank, and reduces the computational complexity of attribute extraction. The form of the Gabor function that given as

$$G(x,y) = \exp\left\{-\frac{1}{2}\left[\frac{x^2}{\delta^2 x} + \frac{y^2}{\delta^2 y}\right]\right\} \cos(2\pi f x) \quad (1)$$

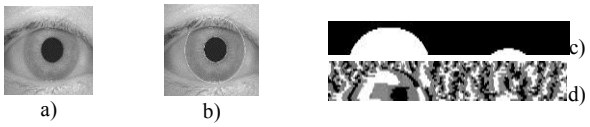
where, f represents the local ridge frequency of the fingerprint where an iris minutia will be appended, and δx and δy are the space constants of the filter envelope along x and y axes, respectively.

In extracting iris features, we rely on log-Gabor filters modified similarly to the method proposed by Daugman to extract the iris phase information instead of the complex Gabor filters used. Daugman algorithm (2)

$$max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \quad (2)$$

where I(x, y) is the eye image, r is the radius to searches over the image (x,y), G(r) is a Gaussian smoothing function. A log-Gabor filter is used for capturing the local structure of the normalized annular iris. Refer to Fig. 5 below.

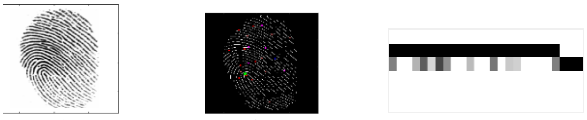
$$G(f) = \exp \frac{-(\log(f/f_0))^2}{(\log(\sigma/f_0))^2} \quad (3)$$



a) b) c) d)

Figure 5. Examples of (a) input images, (b) circle iris images, (c) normalized Daughman mask images and (d) Gabor Feature.

The extraction of fingerprint feature, we use the Minutiae extraction algorithm after the enhancement by Gabor Filter. (Fig. 6)



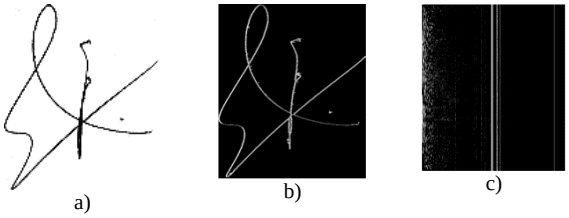
a) b) c)

Figure 6. Examples of (a) input fingerprint images, (b) Minutiae Gabor images, (c) Minutiae Gabor feature extracted.

We extract Face and signature features using the Gabor filter bank to reduce the size of the Principal Component Analysis (PCA). This combination enhances responsiveness as well as extracts the best features from biometric data. (Fig. 7 and Fig. 8)

a) b) c)

Figure 7. Examples of (a) input face images, (b) Gabor extracted, (c) PCA+Gabor extracted.



a) b) c)

Figure 8. Examples of (a) input signature images, (b) Gabor extracted, (c) PCA+Gabor extracted.

In the feature extraction process, we propose to use the advantage of the Gabor filter that has been appreciated in this regard.

B. Mixing Pair of Feature Iris-Fingerprint, Face-Signature

For the purpose of enhancing complexity and mutual authentication, we consider mixing the watermark feature in kit, including: iris watermark feature with fingerprint watermark feature, face watermark feature with signature watermark feature. In order to do this, the combined features will be rescaled to the same size and then combined under the equation (4), (5).

$$F_{IF} = F_{Iris} * (1 + k1 \times F_{FingerPrint}) \quad (4)$$

$$F_{FS} = F_{Face} * (1 + k2 \times F_{Signature}) \quad (5)$$

where k1, k2 are gain factor, F_{Iris} is the Iris feature, $F_{FingerPrint}$ is the Fingerprint feature, F_{Face} is the Face feature, $F_{Signature}$ is the signature, F_{IF} is the iris-fingerprint combination, and F_{FS} is the face-signature combination.

IV. Multiple Biometric Watermark Processing

In this proposed method, the original image will be embedded with multiple biometric features information at 2 transform levels. Multiple watermark data will be embedded in the Multilevel Discrete Curvelet Transform and Contourlet Transform (CCT) coefficients, to perform and evaluate the watermarking capabilities of the two algorithms.

A. Multiple Biometric Watermark Embedding

1) Take a fingerprint, iris, face and signature of the individual as a watermark information.

2) Then Iris feature is extracted by Daugman Gabor filter. Face and signature features are extracted through a Gabor filter that combines PCA. These biometric

watermark features are denoted as F_{IF} (iris - fingerprint) and F_{FS} (face-signature).

3) Implement Fast Discrete Curvelet Transform and Contourlet Transform (CCT) to calculate the coefficients of the host image at 2 levels, and *embed* the information at each level as follows

$$C_{Watermarked\_level1} = C_{Curvelet_{level1}}(1 + k3 \times F_{IF}) \quad (6)$$

$$C_{Watermarked\_level2} = C_{Curvelet_{level2}}(1 + k4 \times F_{FS}) \quad (7)$$

4) Applied reverse frequency UFFT based Multilevel Fast Discrete Curvelet Transform and Contourlet Transform (CCT) on modified coefficients with another unmodified coefficient to get watermarked biometric image.

B. Multiple Biometric Watermark Extraction

1) Take a watermarked image and apply Multilevel Fast Discrete Curvelet Transform and Contourlet Transform (CCT) to calculate the coefficients of the host image at 2 levels on it to convert into various coefficients.

2) Extracted sparse measurements of a watermark biometric image using the reverse procedure of embedding.

$$RF_{PS} = \frac{\left(\frac{C_{Watermarked\_level2}}{C_{Curvelet\_level2}} - 1\right)}{k} \quad (8)$$

$$RF_{IF} = \frac{\left(\frac{C_{Watermarked\_level1}}{C_{Curvelet\_level1}} - 1\right)}{k} \quad (9)$$

where k = gain factor, RF_{IF} = recovered features of iris-fingerprint watermark, RF_{PS} = recovered features of face-signatue watermark.

3) Using biometric watermark features are denoted as F_{IF} (iris - fingerprint) and F_{FS} (face-signature) to compare with RF_{IF} and RF_{PS}.

C. Comparison of Features Extracted with Original Features

For the evaluation of quality, authentication and robustness of the proposed method, we used the Structural Similarity Index Measure (SSIM) to compute similarity between two features.

$$S_1 = SSIM(F_{IF}, RF_{IF})$$

$$S_2 = SSIM(F_I, RF_I) \quad (10)$$

$$S = \frac{S_1 + S_2}{2}$$

where S_1 = similarity between iris-fingerprint watermark features, S_2 = similarity between face-signature watermark features, S = average similarity between multiple watermark features. Similar to the evaluation method in [8], we consider the SSIM results in two cases:

- Confirm not attack if S> μ
- Confirm attack if S <μ

where S = average value of SSIM, μ = threshold decision.

V. Experimental Results

In this proposed watermarking, multiple biometric features are embedded in an original lena image, and the image afterwards are used to check the image quality. Biometric data models are available from CASIA, faculty chicagobooth, YCCE College; about 100 sets of diometric data are used for testing. Quantitative assessment methods are used, such as the Structural Similarity Index Measure (SSIM), PSNR, to evaluate the quality, individual authentication and sustainability of biometric features. Fig. 9 shows the biometric feature and the original image used for the watermark. The size of host image is 512x512 pixels and a size of watermark image is 128x128.

a) b) c) d) e)

Figure 9. Original Lena image and multiple biometric data as feature watermark.

TABLE I. The Technical Evaluation Criteria Proposed

Attacks	PSNR (dB)	S1	S2	Mean SSIM (S)	Decision about Attacked
No Attack	44.21	1.00	1.00	1.00	No
JPEG Compression (Q = 80)	39.24	0.41	0.46	0.43	Yes
JPEG Compression (Q = 70)	36.57	0.21	0.27	0.24	Yes
Gaussian Noise (μ =0, σ =0.001)	31.43	0.17	0.22	0.19	Yes
Salt & Pepper Noise (Noise Density = 0.005)	28.03	0.14	0.19	0.16	Yes
Speckle Noise (Variance = 0.004)	36.24	0.21	0.17	0.19	Yes
Median Filter (size = 3 × 3)	39.02	0.19	0.15	0.17	Yes
Mean Filter (size = 3 × 3)	35.73	0.07	0.06	0.06	Yes
Gaussian Low Pass Filter (size = 3 ×3)	41.34	0.38	0.59	0.48	Yes
Histogram Equalization	20.05	0.50	0.57	0.54	Yes
Cropping	35.73	0.62	0.67	0.64	Yes

The biometric data are used embedded in the original image. The size of the iris and fingerprint features is 48x128; size of face and signature features is 128x128. The watermark feature is a 48x128-sized iris-fingerprint, and the face-signature is 128×128.

In this article, the watermarked image is tested by different attacks such as JPEG compression, Gaussian noise and others noise, some type of filter and cropping attacks. We use the threshold of μ as 0.85 to determine the attack. For a general evaluation, we consider the PSNR, SSIM and the mean SSIM values as shown in Table I.

TABLE II. COMPARE MULTIPLE PROPOSED WATERMARKING AND REFERENCE TECHNIQUES

Features	Inamdar Technique (2014) [9]	Thanki Technique (2016) [8]	Proposed Technique
Type of Multiple Watermarking	Successive	Composite	Composite + Successive
Used Watermark Information	Biometric Trait	Biometric Features	Biometric Features
Used Image Transform for Watermark Embedding	Discrete Wavelet Transform (DWT)	Fast Discrete Curvelet Transform (FDCT)	Multilevel Discrete Curvelet, Contourlet Transform (CCT)
PSNR value	35.18 dB	42.44 dB	44.21dB

The proposed multiple watermarking was compared to the same criteria in the references as in Table II. The results suggest that the proposed technique is superior to the techniques described.

VI. CONCLUSIONS

In this paper, we propose a new method for performing multiple watermarking. We have implemented embedded biometric features using the Daugman Gabor filter, Minutiae, PCA; and use the or Multilevel Fast Discrete Curvelet Transform and Contourlet Transform (CCT) for attack detection, individual recognition and copyright authentication. We have presented various approaches performing watermaking on the whole frequency domain of multiscale wavelets: transform coefficients of curvelet and contourlet, and at various levels. As well, combining features in sets will increase the complexity and authenticity of the biometric feature. The experimental results show that our approach is performed better than existing watermarking referenced.

In the future, we consider developing models with color photos and realtime video.

REFERENCES

[1] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems," *IEEE Signal Processing Magazine*, vol. 32, pp. 66-76, Sept. 2015.

[2] T. Huynh-The, O. Banos, S. Y. Lee, Y. Yoon, and T. Le-Tien, "Improving digital image watermarking by means of optimal channel selection," *Expert Systems with Applications*, vol. 62, pp. 177–189, November 2016.

[3] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data – A state of the art overview," *IEEE Signal Processing Magazine*, vol. 17, 2000.

[4] M. H. Lim, A. B. J. Teoh, and J. Kim, "Biometric feature type transformation," *IEEE Signal Processing Magazine*, vol. 32, pp. 77-87, August 2015.

[5] S. Edward, S. Sumathi, and R. Ranihemamalini, "Person authentication using multimodal biometrics with watermarking," in *Proc. International Conference on Signal Processing, Communication, Computing and Networking Technologies IEEE*, July 2011, pp. 100-104.

[6] V. Inamdar and P. Rege, "Dual watermarking technique with multiple biometric watermarks," *Indian Academy of Sciences, Sadhana*, vol. 39, pp. 3-26, February 2014.

[7] A. Othman and A. Ross, "Fingerprint + Iris = IrisPrint," in *Proc. 12th SPIE Biometric and Surveillance Technology for Human and Activity Identification*, April 2015, vol. 9457.

[8] R. M. Thanki, V. V. Dwivedi, and K. R. Borisagar, "A watermarking technique using discrete curvelet transform for security of multiple biometric features," *International Journal of Information Processing*, vol. 10, no. 1, pp. 103-114, Jan. 2017.

[9] M. Douglas, "Fingerprint watermarking using SVD and DWT based steganography to enhance security," in *CUAL Repository*, master thesis, Sept. 2015.

[10] B. A. H. Bindu and V. Saraswati, "Watermarking of digital images with iris based biometric data using wavelet and SVD," *International Journal of Engineering Development and Research*, vol. 4, no. 1, pp. 726-731, March 2016.

[11] P. Bedi, R. Bansal, and P. Sehgal, "Multimodal biometric authentication using PSO based watermarking," *Procedia Technology*, vol. 4, pp. 612-618, 2012.

[12] M. Vatsa, R. Singh, A. Noore, M. Houck, and K. Morris, "Robust biometric image watermarking for fingerprint and face," *IEICE Electronics Express*, vol. 3, no. 2, pp. 23-28, 2006.

[13] L. H. Yin, "Study of digital image watermarking in curvelet domain," degree of master of philosophy, City University of Hong Kong, July 2009.

[14] J. D. Xu, H. M. Pang, and J. P. Zhao, "Digital image watermarking algorithm based on fast curvelet transform," *Journal of Software Engineering and Applications*, vol. 3, no. 10, pp. 939-943, 2010.

[15] N. S. Kumar and B. M. Kumar, "Improved image watermarking with curvelet wavelet," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 4, pp. 363–368, April 2013.

[16] S. M. E. Sahraeian, M. A. Akhaee, S. A. Hejazi, and F. Marvasti, "Contourlet based image watermarking using optimum detector in the noisy environment," in *Proc. IEEE 15th International Conference on Image Processing*, 2008.

[17] H. H. Song, S. Y. Yu, X. K. Yang, S. Li, and C. Wang, "Contourlet-based image adaptive watermarking," *Image Communication*, vol. 23, pp. 162–178, Jan. 2008.

[18] N. Deshpande, "Robust invisible video watermarking using log Gabor mask," *International Science Press IJCTA*, vol. 10, no. 9, pp. 315-326, 2017.

[19] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "Biometric template security based on watermarking," *Procedia Computer Science*, vol. 2, pp. 227–235, 2010.

[20] M. Barbier, J. M. L. Bars, and C. Rosenberger, "Image watermarking with biometric data for copyright protection," in *Proc. 10th ARES International Conference*, Aug. 2015, pp. 24-27.

Hoan Nguyen-Thanh is a master of Department of Electrical Electronics Engineering, Hochiminh City University of Technology, Vietnam. Hornor bachelor in electrical & electronic engineering of Ho Chi Minh University of Technology. He specializes in signal processing, image processing, automation and big data. Head of research SCADA automation base on cloud bigdata, image processing and intelligent data processing base on big data.

Thuong Le-Tien is with Department of Electrical Electronics Engineering, Hochiminh City University of Technology, Vietnam. Thuong Le-Tien (IEEEM'96) is a full Professor at the Ho Chi Minh City University of Technology (HCMUT). He received the Bachelor's and Master's Degrees in Electronics Engineering from the HCMUT, and the Ph.D. Degree in Electronics-Telecommunications from the University of Tasmania, UTAS, Australia.
He has authored over 160 research articles and many teaching textbooks for university students related to Electronics 1 & 2, Antenna and Wave Propagation, Digital Signal Processing and Wavelets, and Communication Systems.