An Improved Image Steganography Algorithm based on PVD

Sharif Shah Newaj Bhuiyan*, Norun Abdul Malek, Othman Omran Khalifa, Farah Diyana Abdul Rahman
Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University, Malaysia, 53100 Kuala Lumpur, Malaysia.

Article Info

Article history:
Received Nov 12, 2017
Revised Jan 20, 2018
Accepted Feb 11, 2018

Keywords:
Bit-plane slicing
Data hiding
PVD
Steganalysis
Steganography

ABSTRACT

In this paper, a modification of PVD (Pixel Value Differencing) algorithm is used for Image Steganography in spatial domain. It is normalizing secret data value by encoding method to make the new pixel edge difference less among three neighbors (horizontal, vertical and diagonal) and embedding data only to less intensity pixel difference areas or regions. The proposed algorithm shows a good improvement for both color and gray-scale images compared to other algorithms. Color images performances are better than gray images. However, in this work the focus is mainly on gray images. The strength of this scheme is that any random hidden/secret data do not make any shuttle differences to Steg-image compared to original image. The bit plane slicing is used to analyze the maximum payload that has been embedded into the cover image securely. The simulation results show that the proposed algorithm is performing better and showing great consistent results for PSNR, MSE values of any images, also against Steganalysis attack.

1. INTRODUCTION

Internet communication is increasing day by day and the message transmission through it is also increasing. Communication can happen from any places of the world through internet. Therefore the security is also necessary and important for the transmitted messages. Data Encryption is the one of the most effective way to provide security. We transform message to another encrypted format or pattern during communication and the changes we make therefore it become suspicious. So when it gets suspicious, attacker may suspect about the presence of hidden information. To solve this problem, we need to hide the secret or important message behind a cover image, so that it doesn’t draw any attention to HVS (human visioning system). This method is called Steganography [1]. Steganography is the art of secret communication. Many steganography techniques have been introduced. The spatial domain steganography, the secret data are directly embedded into the pixels of cover images. There are several methods of spatial domain steganography available. These are spatial domain methods, such as least significant bit (LSB), pixel value differencing (PVD), Histogram shifting and pixel mapping [2], [3], [17]. The difference of two consecutive pixels is used to determine how many secret bits can be embedded [3]. PVD can be classified into basic PVD, PVD with LSB Substitution [4], [5], [14], Multi-Pixel Differencing (MPD), Modulus Function (MF) [7] and side matching [16]. This paper presents a new improved image steganography PVD method based on various parameter like normalized the hidden data, hiding capacity, PSNR (peak signal to noise ratio), MSE (mean square error) values and RS Steganalysis attack. By applying data normalization like data encoding, it improves the performance and shows great consistency in results.

Copyright © 2018 Institute of Advanced Engineering and Science. All rights reserved.
We are only focusing on spatial domain Steganography. The rest of this paper is organized as follows. Section II presents the basic idea of PVD, Section III presents the PVD related works, Section IV the details of the proposed scheme, the Section V the theoretical analysis and experimental results and the last is conclusion.

2. PIXEL VALUE DIFFERENCE ALGORITHM (PVD)

The PVD method uses grey image as cover image and it embeds dynamic size secret message into the cover image. Embedding message bits rate is different in each regions like fewer bits in smooth region compared with the edged region [3], [4], [9]. Initially it scans the whole cover image in raster scan order and partitioned into the non-overlapping two consecutive pixels blocks. Two consecutive pixels in the i\textsuperscript{th} block are denoted as \( P_i \) and \( P_{i+1} \) respectively [3].

The difference of two consecutive pixels is calculated by
\[
d_i = (P_{i+1} - P_i)
\]  
(1)

The value of \( d_i \) denotes the difference of two consecutive pixels in each block. If \( d_i \) is small value then it means the block is smooth region, where a larger value indicates the block is edge/noise region. In Block-wise PVD method, core idea was to find more edge areas in order to hide more secret data because of Human vision tolerance in edge areas than in smooth areas [10].

The difference value \( (d_i) \) will be in the range from (0 to 255) because greyscale image has max intensity value 256. The difference value \( (d_i) \) can be grouped into the several regions based on the lower and upper bound of each \( R_i \) [3].

The number of embedded secret bits \( (t) \) in two consecutive pixels depends on the user defined range table and it is computed as
\[
\text{bits\_width} (t) = \log_2(Upper_i - Lower_i + 1)
\]  
(2)

Then, obtained the decimal value from the binary sequences \((1011)_2 = (8+0+2+1)_{10} = 11\) Now, the new difference value formula can be obtained by following formula
\[
d' = t_d + \text{lower}_i
\]  
(3)

In our proposed scheme, we have used \((2 \times 2)\) block to find three \((3)\) pixel differences [12].

3. RELATED WORK

PVD method is one of the popular algorithm in special domain used for data hiding. This method has been improved a lot from 2003 till now by researchers. This section represents current literature review of PVD methods based on various characteristics.

In 2003 [3], Wu and Tsai proposed a steganography method which considers pixel value differencing (PVD). This algorithm calculates the difference of two pixels for the gray valued cover image. Non-overlapping blocks of two pixels calculation iterates over all the rows of each image in a zigzag manner. The number of bits to be embedded into two consecutive pixels is calculated by their absolute difference and a user defined range table. If a block difference \( (d_i) \) is close to \( 0 \), then it is considered to be an extremely smooth block, whereas a block difference \( (d_i) \) is close to \(-255\) or \(255\), then it is considered to be a sharply edged block. PVD method embeds more data into complex regions, where pixel pairs with larger difference are often located. Let’s assume that \( P_i \) and \( P_{i+1} \) are two consecutive pixels block in a cover image and their difference is \( d_i \) from the equation (1).

Now, if \( d_i \)'s range is width \( (w) \) then the embedding bits \( (t) \) can be calculated by
\[
t = \log (w)
\]  
(4)

From equation (4), we get the decimal value \( t \) which is the number of bits is taken from secret data and used to update \( d \) to get new value of \( d' \).
\[
d' = \begin{cases} 
  (lk + b) & \text{for } d \geq 0; \\
  -(lk + b) & \text{for } d < 0;
\end{cases}
\]  
(5)

This \( d' \) gives us new values \((P_i')\) and \((P_{i+1}')\) of pixels \((P_i)\) and \((P_{i+1})\).
However, the PVD method causes considerable distortion, leading to degradation in image quality. Below we will explain the details of enhanced PVD method and the combination with different other well known methods.

In [5], Wu et al. proposed a slightly modified PVD method. In this method, user defined range table and pixel value difference calculation steps were used from original PVD method. The user range table was divided into two groups, one is lower division and other one is higher division. Smooth and edged areas were considered as small and large pixel value difference respectively. It used three (3) bits LSB substitution for smooth areas and original PVD for edged areas. This modified PVD method shows better image quality (PSNR value).

In [6], Weiqi Luo et al. proposed a secure steganography based on adaptive PVD scheme. In this approach, the cover image was segmented into small squares, then each one was rotated by a random angle of 0°, 90°, 180° or 270°. Then the processed image was partitioned into non-overlapping squares with 3 consecutive pixels. The center pixel was used for secret data hiding. By calculating the differences, it found the total number of embedded bits. For preserving the local features information, it kept the sorting order of the three pixel values same after data hiding. In addition, this method used sharper regions for adaptive data hiding, while it preserved other smoother regions by value adjustment. The final results analyzed on a large image database and this method improved security issues as compared to the previous PVD-based methods.

Also, Modulus PVD method was proposed by Wang et al. in which modulus function is used for data embedding. The modulus method modifies the value of the difference of the two pixel block. This tackled the boundary falling off problem. But this method shows same result as original PVD.

In previous PVD method, only two consecutive pixel were used as a pixel block for data embedding. The multi-pixel differencing (MPD) is presented by neighboring pixels correlation to estimate the degree of smoothness or contrast of pixels. Below are some of the various MPD methods.

In [8], Weng et al. proposed new scheme based on predictive differencing (PD) to embed in grey image. This approach is where embedding by raster scan order except for the first column and the first row for the cover image. Used several predictors to calculate predictive value (PV) like horizontal, vertical. Predictive error (PE) was calculated as a difference of input pixel and PV. First checked the range table for PE then embedding was done using k-bit substitution into the input pixel. If PE and new prediction error (NPE) are laying in different ranges, then output value has to be re-adjusted. Comparatively this method has provided better capacity and improved output image quality than earlier non MPD works.

In [12], Ko-Chin Chang et al. (2008) proposed Tri Pixel Value Differencing (TPVD), it increases the capacity and also provides better imperceptible stego-image for HVS (human vision system). It is also a new approach that uses tri-pixel value differencing. The horizontal, vertical and diagonal edges are used to embed more secret data than the Wu and Tsai (PVD) method [3]. Furthermore, it reduces the quality distortion of the stego-image through an optimal selection and adaptive rules. The output results demonstrate that the embedding in the stego image is imperceptible for human vision while compared to the cover image. This method can provide better embedding capacity than the original PVD method. It also shows the robustness and good results in the dual statistical analysis. The extraction method can work correctly without the original cover images.

In [13], the proposed method which used TPVD with adaptive LSB matching revisited algorithm to maximize the data embedding rate. This method initializes some parameters during data embedding phase which are used for data preprocessing and region selection. After the initial phase, the capacity of those selected region is estimated. If the region is large enough then it performs only at the selected regions the data hiding. Then it also performs post-processing to obtain the stego-image. At the end for data extraction, the side match information is used and based on this information some preprocessing can be performed. After this processing, it can identify the region where data is hidden.

4. PROPOSED SCHEME

In this section, we shall present the proposed scheme in two parts: new embedding method and extraction method, the concept of this new scheme is based on Multi-pixel differencing. During our investigation, we have observed that if we can normalize/encode the value of our secret data then we can simplify the multi-pixel differencing algorithm in a few steps. For our new proposed scheme, we don’t have to vary the quantization range table. In this method, we are using fixed length table range. This way our proposed scheme is very much consistent with any images compared to other algorithms which are not consistent in terms of PSNR (pixel value noise ratio) or MSE (mean square error).

First step of our embedding procedure is the secret data encoding, then save into a file or variable to process with the cover image. In our scheme, we have used base64 encoding which has given very good...
performance for new pixel value differencing. Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. There are 3 other character +, /, =.

Example: (Secret Text)

“The quick brown fox jumps over the lazy dog”

Encoded Text:

VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBxYXp5IGRvZw==

Secret text size is 43 but encoded size will be little larger 60. So, encoded size equation will be

\[ 4 \times \text{ceil} \left( \frac{\text{length of original text}}{3} \right) \]

The reason to use the encoding mechanism, to minimize the error of new pixels value difference.

Our focus is to increase the security, capacity of secret data and simplify the implementation for further development.

Figure 1 shows the proposed scheme’s block diagram for PVD image steganography.

---

**Figure 1. Block Diagram for PVD Image Steganography**
As defined above in Tri-way pixel method, for each component of a block, we can obtain three pixel value differences, $d_1$, $d_2$ and $d_3$.

\[
\begin{array}{c}
p(1,1) \\
p(2,1) \\
p(1,2) \\
p(2,2)
\end{array}
\]

\[
d_1 = p(1, 2) - p(1, 1) \\
d_2 = p(2, 1) - p(1, 1) \\
d_3 = p(2, 2) - p(1, 1)
\]

Then according to $d_1$, $d_2$ and $d_3$ to find the hiding capacity from range table $R_j$, the width

\[
w = \text{upper}(j) - \text{lower}(j) + 1
\]

(7)

The hiding capacity of bits is fixed for our method. It is either 4 or 3 depends on the security and capacity level parameters.

**Range Table (1)**

- Lower = [0 16 32 48 64 80 96 112 128 144 160 176 192 208 224 240]
- Upper = [15 31 47 63 79 95 111 127 143 159 175 191 207 223 239 255]

**Range Table (2)**

- Lower = [0 8 16 24 32 40 48 56 64 72 80 88 96 104 112 120 128 136 144 152 160 168 176 184 192 200 208 216 224 232 240 248]
- Upper = [7 15 23 31 39 47 55 63 71 79 87 95 103 111 119 127 135 143 151 159 167 175 183 191 199 207 215 223 231 239 247 255]

- \(\text{bits\_width}(t) = \log_2(\text{upper}_t - \text{lower}_t + 1)\) (8)

After embedding secret bits with lower value of range table, we get new difference value. Now we need to construct new pixel value for our proposed scheme. We have observed several methods and did our own investigation. Then we came up the following new value construction method which is much simpler than any other methods currently exist.

We consider the first pixel (1, 1) from sub-pixel block as reference point (RF) for positive and negatives differences.

Now, if difference is positive then the general form will be:

\[ NPV = \text{RF} + \text{ND} + 1 \] (9)

If negative then

\[ NPV = \text{RF} - \text{ND} - 1 \] (10)

**Data Extraction Process**

The extraction architecture of the proposed system for text file/image file is same.

1. Partition the stego-image into the (2 x 2) sub-pixel blocks.
2. Calculate the difference values as we did in embedded phase.
3. Find the embedding bits based on the quantization range table of pixel difference value.
4. Continue the process until we find all the hidden bits according to encoded file length.

5. **RESULTS ANALYSIS AND DISCUSSION**

We have chosen cover images from the SIPI Image Database. Here, we have used peak signal-to-noise ratio (PSNR) and MSE methods to analyze our result to show our method is well defined and then the experiment results show the proposed method has better imperceptibility.

The output image quality is calculated by the PSNR. The PSNR formula is defined as

\[
\text{PSNR} = 10 \times \log_2 \frac{255^2}{\text{MSE}} \text{(dB)}
\]

(11)
Where MSE is the mean square error between the cover and stego images. For a cover image, whose width and height are \( w \) and \( h \), then MSE is defined as

\[
\text{MSE} = \frac{1}{w \times h} \sum_{i=1}^{w} \sum_{j=1}^{h} (s(i, j) - c(i, j))^2
\]

(12)

Where \( s(i, j) \) denotes pixel value from stego images and \( c(i, j) \) denotes pixel values from cover images respectively.

PSNR and MSE values of the 70,827 bytes (70KB) image capacities for embedding data by using the cover Images. All images are 512x512 and two set of width ranges are used for gray values (Table 1 and Figure 2).

### Table 1: EXPRES 1

| Cover Image (512 x 512) | PSNR(db) for Range Table 1 (width 4) | MSE | PSNR(db) for Range Table 2 (width 3) | MSE |
|-------------------------|--------------------------------------|-----|--------------------------------------|-----|
| Lena                    | 37.765                               | 10.879 | 39.119                               | 7.9652 |
| Baboon                  | 35.898                               | 16.722 | 39.503                               | 7.2909 |
| Peppers                 | 37.555                               | 11.417 | 39.359                               | 7.5368 |
| Jet                     | 37.508                               | 11.541 | 38.906                               | 8.3656 |
| Tiffany                 | 37.493                               | 11.581 | 39.411                               | 7.4462 |

Figure 2. Comparison of PSNR for 3 bit vs 4 bit width.

Comparison of original PVD, TPVD and our proposed scheme of stego-images (512 x 512) for PSNR, MSE values (Table 2 and Figure 3).

### Table 2. EXPRES 2

| Cover Image (512 x 512) | Wu and Tsai Original PVD Cap. (bytes) | PSNR | Ko-Chin Chang Tri-way PVD Cap. (bytes) | PSNR | Our Proposed Method Cap. (bytes) | PSNR |
|-------------------------|-------------------------------------|------|--------------------------------------|------|---------------------------------|------|
| Lena                    | 50960                               | 41.79 | 75836                                | 38.89 | 74047                           | 38.907 |
| Baboon                  | 56291                               | 37.90 | 82407                                | 33.93 | 74047                           | 39.305 |
| Peppers                 | 50685                               | 40.97 | 75579                                | 38.50 | 74047                           | 39.150 |
| Jet                     | 51243                               | 40.97 | 76352                                | 38.70 | 74047                           | 38.696 |
5.1 Security Verification using RS Method

After embedded the secret data into the cover images using our proposed method, the primary target is to generate our final stego images perceptually as much as close to the original cover images. The method which is called stego-analysis is generally used to check and detect whether an image is a stego-image or not. The dual statistical stego-analytic technique proposed by Fridrich et al. [15] can detect whether the final stego-image is suspicious or not, using LSB substitution. Therefore, we have applied RS method against our generated final stego-image to test our proposed new method performance for security measurement; data is shown in Table 3.

The ‘mask’ in RS Steganalysis [15] determines how the pixels are grouped and which pixels of each group are LSB-flipped. The masks [0 1 1 0] and [0, 1; 1, 0] were used by Fridrich et al., ACM workshop. RS result value is 0~100%, if $RS \leq 0$, then it means no embedded message exists in the image.

| Final Stego-Image | Mask         | RS result   | Comment   |
|-------------------|--------------|-------------|-----------|
| Lena              | [1 0 1 0 1]  | 0.010232    | Less Suspicious |
| Baboon            | [1 0 1 0 1]  | -0.021465   | No Msg    |
| Peppers           | [1 0 1 0 1]  | -0.071083   | No Msg    |
| Jet               | [1 0 1 0 1]  | -0.019284   | No Msg    |
| Tiffany           | [1 0 1 0 1]  | -0.087895   | No Msg    |

From our above results (Table 4), we can see that Mask matrix is very important for the RS Steganalysis method. In future we can improve our algorithm more against the RS matrix value. So that attacker can’t use any smaller matrix to suspect our final generated steg-image. We have to improve such a way, RS method has to be used the bigger multi-dimensional matrix to detect, which won’t be feasible in real-time or even few weeks situation. This way we can provide 100% real time security.

| Final Stego-Image | Mask (Used by Fridrich et al.) | RS result  | Comment   |
|-------------------|--------------------------------|------------|-----------|
| Lena              | [0 1 1 0]                       | 0.0068959  | Less Suspicious |
| Baboon            | [0 1 1 0]                       | -0.10637   | No Msg    |
| Peppers           | [0 1 1 0]                       | 0.0066805  | Less Suspicious |
| Jet               | [0 1 1 0]                       | -0.003463  | No Msg    |
| Tiffany           | [0 1 1 0]                       | -0.12353   | No Msg    |
In future, we can apply more similarity measures parameters like RMSE, SSIM, Shannon’s Entropy, NAE, Average difference and so on. It can also be tested against BPNN, SVM and K-NN classifier based Steganalysis algorithm [18].

6. CONCLUSION
This work designs a new novel efficient image steganography PVD based method to embed secret information into images without producing any perceptible image distortions. In particular, we proposed an intuitive idea of secret data encoding to apply in image steganography. It helps to reduce the edge distortion because of new value construction. There is no need of referencing the original image when extracting the embedded data from a stego-image. If we choose a proper range table width then we can also improve the PSNR and increase the data embedding capacity, as well as, better image quality. The theoretical analysis shows the proposed scheme is well defined and has larger capacity and higher PSNR than those of Wu and Tsai (original PD), Ko-Chin Chang (Tri-way PVD) and other PVD based methods.

ACKNOWLEDGEMENTS
The author wishes to thank International Islamic University Malaysia (IIUM) for supporting the dissemination of this research. This research was supported by Ministry of Education Malaysia through Research Initiative Grant Scheme (RIGS) 2016.

REFERENCES
[1] Lee YP, Lee J-C, ChenW-K, Chang K-C, Su I-J, Chang C-P, "High Payload Image Hiding With Quality Recovery Using Tri-Way Pixel Value Differencing," Information Sciences, vol. 191, pp. 214-225, 2012.
[2] Hsien-Wen Tseng and Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Journal of Applied Mathematics, 2013.
[3] Wu D-C and Tsai W-H., "A Steganographic Method For Images By Pixel Value Differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.
[4] El Sayed M. El Alfy and Azzat A. Al-Sadi, "Improved Pixel Value Differencing Steganography Using Logistic Chaotic Map," Innovations in Information Technology, 2012.
[5] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic Scheme Based On Pixel-Value Differencing and LSB Replacement Methods," IEEE Proceedings-Vision, Image and Signal Processing, vol. 152, No. 5, pp. 611-615, 2005.
[6] Weiqi Luo, Fangjun Huang, Jiwu Huang, "A More Secure Steganography Based On Adaptive Pixel-Value Differencing Scheme," Multimedia Tools and Applications, vol. 52, pp. 407-430, 2011.
[7] C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, "A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function," Journal of Systems and Software, vol. 81, pp. 150-158, 2008.
[8] C.Y. Weng, H.K. Tso and S.J. Wang, "Steganographic Data Hiding in Image Processing using Predictive Differencing," Opto-Electronics Review, vol. 20, pp. 126-133, 2012.
[9] J. K. Mandal and Debasis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain," International Journal of Information Sciences and Techniques, vol. 2, 2012.
[10] Yuan-Yu Tsai, Jian-Ting Chen, and Chi-Shiang Chan, "Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding," International Journal of Network Security, vol. 16, pp. 363-368, 2014.
[11] Cheng-Hsing Yang, Chi-Yao Weng, Shih-Jeng Wang and Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488-497, 2008.
[12] Ko Chin Changa, Chien-Ping Changa, Ping S. Huangb, and Te-Ming Tu, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, vol. 3, no. 2, 2008.
[13] P. Mohan Kumar and K. L. Shanmuganathan, "Developing a Secure Image Steganographic System using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate," Information Security Journal: A Global Perspective, vol. 21, pp. 65-70, 2011.
[14] Mojtaba Bahmanzadegan Jahromi and Karim Faez, "An Adaptive Steganography Scheme Based on Visual Quality and Embedding Capacity Improvement," International Journal of Electrical and Computer Engineering, vol. 4, pp. 573-584, 2014.
[15] J. Fridrich, M. Goljan and R. Du, "Detecting LSB Steganography in Color, and Gray-Scale Images," IEEE Multimedia, vol. 8, pp. 22-28, 2001.
[16] Chin-Chen Chang and Hsien-Wen Tseng, "A Steganographic Method for Digital Images using Side Match," Pattern Recognition Letters, vol. 25, pp. 1431-1437, 2004.
[17] Eskandari, Ahmad Reza, "A Robust Steganography method Using Adjustable Parameters," International Journal of Electrical and Computer Engineering, vol. 3, pp. 207-214, 2013.
[18] Souvik Bhattacharyya and Gautam Sanyal, "Moments and Similarity Measure Feature Based Image Steganalysis Technique (MSM)," International Journal of Information and Network Security, vol. 2, pp. 138-153, 2013.
BIOGRAPHIES OF AUTHORS

Sharif Shah Newaj Bhuiyan obtained his BSc degree in Computer Science and Engineering from Ahsanullah University of Science and Technology (AUST), Bangladesh in 2008. Currently he is completing his MSc in Computer and Information Engineering from IIUM, Malaysia. He has 10 years of experience in Software Engineering. His area of interests includes to Image Processing, Artificial Intelligence, Distributed Computing, Parallel Computing and Data Mining.

Othman Omran Khalifa received his Bachelor’s degree in Electronic Engineering from the Garyounis University, Libya in 1986. He obtained his Master degree in Electronics Science Engineering and PhD in Digital Image Processing from Newcastle University, UK in 1996 and 2000 respectively. He worked in industrial for eight years and he is currently a Professor at Electrical and Computer Engineering Department, International Islamic University Malaysia. His area of research interest is Communication Systems, Information theory and Coding, Digital image/ video processing, coding and Compression, Wavelets, Fractal and Pattern Recognition. He published more than 450 papers in international journals and Conferences. He is SIEEE member, IEEE computer, Image processing and Communication Society member.

Norun Abdul Malek obtained her PhD degree from School of Electronic, Electrical and Systems Engineering, Loughborough University, UK in 2013. She has been appointed as an Assistant Professor in Electrical and Computer Engineering Department, Faculty of Engineering, International Islamic University Malaysia (IIUM). Her research interest includes to antenna and propagation, signal processing particularly of antenna arrays, algorithms and wireless communication systems. She is an active member of the IEEE, a registered member of the Board of Engineers Malaysia (BEM) and Institute of Engineers Malaysia (IEM).

Farah Diyana Abdul Rahman obtained her PhD degree from Department of Electrical and Electronic Engineering, University of Bristol, UK in 2015. She has been appointed as an Assistant Professor in Electrical and Computer Engineering Department, Faculty of Engineering, International Islamic University Malaysia (IIUM). Her research interest includes image and video processing, video quality evaluation, multimedia transmission and wireless communication systems. She is an active member of the IEEE, a registered member of the Board of Engineers Malaysia (BEM) and Institute of Engineers Malaysia (IEM).