A Coarse-To-Fine Copy-Move image forgery detection method based on discrete cosine transform

Mas Elyna Azol, Nur Hidayah Ramli, Y.S. Lee, Siti Azura Abuzar
1Department of Electronic Engineering Technology, Faculty of Engineering Technology,
Universiti Malaysia Perlis (UniMAP), Malaysia

Article Info

Article history:

Received Sep 28, 2018
Revised Nov 26, 2018
Accepted Dec 10, 2018

Keywords:

Copy move forgery detection techniques
DCT based algorithm
Image forensics
Image tampering
Passive forgery detection

ABSTRACT

Copy-move forgery is a type of image forgery where one part of an image is copied and pasted in other regions of the same image, and it is one of the most common image forgeries to conceal some information in the original image. Discrete Cosine Transform (DCT) is one of the detection techniques which the detection rate relies intensely on the size of block used. Small block size is known for its ability to detect fine cloned objects, but the drawback is it produces too many false positive and requires high execution time. In this research, a method to overcome the weaknesses of using small block size by applying the coarse-to-fine approach with the two-tier process is proposed. The proposed method is evaluated on fifteen forged images on the CoMoFoD dataset. The results demonstrated that the proposed method is able to achieve high precision and recall rate of over 90% as well as improves the computation time by reducing the overall duration of forgery detection up to 73% compared to the traditional DCT method using small block size. Therefore, these findings validate that the proposed method offers a trade-off between accuracy and runtime.

Corresponding Author:

Mas Elyna Azol,
Department of Electronic Engineering Technology,
Faculty of Engineering Technology,
Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia.
Email: maselyna@unimap.edu.my

1. INTRODUCTION

In this current era of science and technology, it can be clearly observed that the digital images are very widely used and distributed, thanks to the emerging usage of smart phones equipped with digital camera and the increasing popularity of the social media which make it possible for an image to distribute worldwide within seconds. This situation however, promotes the questioning integrity of the digital imagery which is undoubtedly vulnerable to the act of forgery. This act of forgery or tempering is also a threat to society as it may be part of the cause to the act of defamation. Therefore, it is essential for the contribution of research in the area of image forgery as well as the promising area of digital forensics.

The fundamental concept of image forgery is the digital manipulation of pictures with the aim of distorting some information in them. There are several types of image forgeries which include copy-move (or cloning), splicing (or cut-and-paste) technique, and image resampling. Generally, the digital image forgery detection techniques can be categorized into two types; namely active and passive (or blind) techniques. In active method, the digital watermark is embedded into the image in order for it to be available for tracing of authentication, if later questioned. However, the glaring flaw of this technique is the watermark needs to be inserted at the time of recording, which limits the approach to specially equipped digital cameras [1]. On the other hand, the passive method does not require any prior information about the source image. These approaches manipulate the statistical changes in the forged digital image assuming that there are some marks left by the camera during creation, and these marks can be used to trace any forgery attack.

2. RELATED WORKS

To conceal a person or an object in the scene, one of the most common image manipulation methods that can be used is by cloning or copy and paste techniques. The image forensics researchers have done a lot of research to overcome this problem. In copy-move forgery detection (CMFD), strong correlation exists between them as the copied parts belong to the same image. Therefore, it can be utilized as evidence to detect copy-move forgery. However, the main challenge for this type of forgery is the computational complexity due to the exhausting searching process to find correlated segments. One of the most frequently used methods to detect such type of forgery is to use block matching algorithm where image is divided into overlapping blocks and the blocks are matched to find the duplicated region. To increase computational efficiency, [2] introduces a block based matching algorithm to detect the blocks with high correlation based on DCT coefficient.

Generally, the copy-move forgery detection techniques can be categorized into block-based and keypoint-based methods [3]. [4] proposed the copy-move detection based on the Hu moments. Their technique demonstrated that it was robust to various post-processing techniques including rotation, blurring, lossy JPEG compression, and noise contamination. A study was carried out by [5] to detect copy-move forgery by using the 24 blur-invariant moments as features. Their motivations are the forgery detection must not be affected by the blur degradation and additive noise. In their experiment, the method was able to successfully detect copy-move forgery for images with blurred duplicated region and also the duplicated regions with changed contrast values. Copy-move forgery detection based on Zernike moments of circular blocks has been proposed by [6]. Zernike moments are proven not only to be robust to noise, compression and blurring but also invariant to rotation. This method is also useful to detect copy-move blocks for flat regions. The downside of this technique is it is unable to detect forgery in the scaled copy-move blocks. The drawback of moments based techniques is it requires high computational cost.

3. PROPOSED METHOD

In a coarse-to-fine detection method, the input undergoes a two-tier detection process; the output of *coarse* detection is then feed as input to the second-tier *fine* detection. In this work, large block size is used on the first tier to refine the detection area, followed by detection by small block size on the second tier.

First, for pre-processing, the raw image is converted to grayscale. After that, the descriptor is extracted using large overlapping block size based on the traditional DCT algorithm, followed by feature matching to find the forgery detection result. Next, if the forgery result is found in the detection using large block size, the new detection areas is computed for the next tier process. After that, another process of feature extraction is performed using the small block size only from the new detection areas. Subsequently, the matching process is applied and the result of the detection is marked on the image. Each part involved several steps.

3.1. Pre-processing: Grayscale Conversion

In the pre-processing stage, the RGB image of size M×N which consists of three color components (Red, Green, and Blue) is converted into grayscale form, I using standard grayscale formula:

$$I = 0.299R + 0.587G + 0.114B \tag{1}$$

3.2. Feature Extraction

In this part, the features of the image are extracted into overlapping blocks, assuming similar blocks will produce similar features. The forgery detection decision is made only when similar features are detected within the same distance of features related to the associated blocks [11].

The first step into forgery detection is by dividing the image into a B×B square of overlapping blocks. The block is slide by one pixel in zigzag order, which is from the upper left corner to the bottom right of I. In the first tier of detection, the total number of overlapping blocks of image of size M×N can be computed with the following equation:

$$N_B = (M - B + 1)(N - B + 1) \tag{2}$$

In this research which employ the approach of two tier detection system, the large size block is used on the first tier, and on the second tier, the significantly small block is utilized. When this scanning is performed, the coordinate of the top left pixel is saved in an array to remember its position.

The next step is the extraction of the DCT coefficients of each overlapping blocks scanned from the image. After the DCT coefficient is extracted, it is then quantized with the user-specified parameter Q. This value is represented by a quantization matrix which is to be divided by the DCT coefficients in the previous step.

3.3. Forgery Detection

In this part, the robust match [2] technique for forgery detection is employed. After the DCT transform coefficient is quantized from each overlapping blocks, each blocks is reshaped and stored in one row on matrix A. This matrix has (M– B+1)(N–B+1) rows and B×B columns.

Next, the rows of matrix A are sorted lexicographically. This is to ensure that similar group of block data is placed next to each other and thus reduce the matching time. Subsequently, each two consecutive rows of the sorted matrix are compared to each other. If match is found, the position (upper left pixel) of the matching blocks is stored in another array and the shift vector of the two matching blocks is calculated. The shift vector s between two pair of matching blocks positions (i_1, i_2) and (j_1,j_2) is calculated as:

$$s = (s_1, s_2) = (i_i - j_1, i_2 - j_2) \qquad (3)$$

When a block match is found, there an increment of 1 is applied for the corresponding shift vector counter; C. The next tier decision is made after the previous process is done with the large block size. If there were no matching block detected, then the process is terminated. Else, it would take into account the shift vector values captured.

3.4. Reduction of Detection Area

To reduce the computing time, the new detection area is determined, so that it will reduce the number of blocks required for feature extraction and block matching. In this approach, a new threshold criterion is required which is the copy-move quantity value, G. This value served as a filter to truncate the shift vector array after descending row sort. The value reflects how many copy and pasted objects that are expected from the detection.

After truncation is done, the new detection area is computed which corresponds to pixel clusters of the remaining shift vectors. This is done by getting the top right and bottom left coordinate from both objects of the matching pair. Next, another parameter, which is the offset value to be added to the detection area, is required with the intention that it will enhance the robustness of the detection when the small block size is applied. New detection areas are based on the top left and bottom right coordinate with added offset value shows in Figure 1.

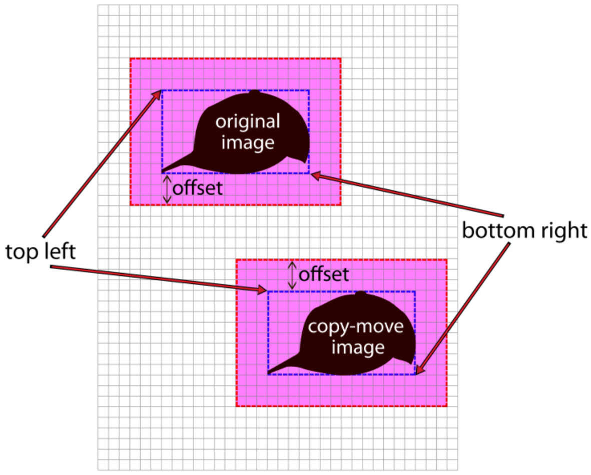

Figure 1. New detection areas are based on the top left and bottom right coordinate with added offset value

For each remaining shift vector, the top left and bottom right coordinate of the detected block matches from an image M×N is computed by the following algorithm. Algorithm for determination of second tier detection area as shows in Table 1.

Table 1. Algorithm for Determination of Second Tier Detection Area

```
Input: Detected clones matric, [rowC, colC]
Initializations: Sort shift vector v, truncate to G

for each selected shift vector v[rowV, colV] do
   for x=1 to rowV do
        Set topmost = M, leftmost = N,
                    bottommost = 1, rightmost = 1
        for y=1 to rowC do
             if clones(y,match1) equals v(x,1)
                  and clones(y,match2) equals v(x,2)
                  i1 = clones(y,1);
                  j1 = clones(y,2);
                  i2 = clones(y,3);
                  j2 = clones(y,4);
                  Set the topleft and bottomright of the first match
                       if  i1 < topmost
                           topmost = i1
                       end if
                       if  i1 > bottommost
                           bottommost = i1
                       end if
                       if  i2 < leftmost
                           leftmost = i2
                       end if
                       if  i2 > rightmost
                           rightmost = i2
                       end if
                  Repeat for the second match
             end if
        end for
   end for
end for
```

Algorithm to get the top left and bottom right coordinate of the matching object cluster. This algorithm is applied on both objects of the matching pair.

Next, the offset value is added to the top left and bottom right coordinates and it is stored in a new array. The block size is changed to the small block size value and another batch of detection (feature extraction, block matching) is done on the new calculated detection area for each remaining shift vectors of the previous detection by the large block size.

Following the second tier of detection, the match blocks found is finally filtered by the threshold value, T so that only the pixel clusters which frequencies are higher than the threshold value is accepted as the detection result. Finally, the detection result is marked on the image pixels.

4. EXPERIMENTAL RESULTS

4.1. Dataset and Evaluation

The evaluation of this proposed method is done by utilizing fifteen images provided in CoMoFoD, which is a standard dataset of copy-move forged images [12]. The performance of this algorithm is based on the accuracy measure and execution time. The accuracy measurement is based on the performance of the detection on pixel level, to evaluate the accuracy of the identified tempered region [13]. To measure the correctness of detection performed, some parameter results are captured by comparing the detection result with the provided ground truth images:

TP - Correctly detected forged pixels
FP - Erroneously detected pixels as forged
FN - Forged pixels missed detected

From this values, the Precision,p, and Recall,r is computed. Precision is the probability that the detection result is truly a forgery, and Recall (true positive rate) show the probability that a forged pixel is detected.

4.2. Testing Parameters

For this experiment, the copy-move forgery detection is done using the variable block size approach with two tier detection process based on DCT algorithm. For the first tier process, the DCT features are extracted from source images using large overlapping blocks of 16×16. In the next tier process, the small block is used, which is with block size 2×2. Another parameter, the pixel occurrence threshold value, T is set with 50, copy-move quantity value, G set to 4, and offset value set to 30.

The control images for performance comparison are run using traditional DCT CMFD method with block size 2×2 and threshold value = 50. Control result is also obtained using block size 16×16 with the same threshold value for the purpose of visual comparison.

4.3. Results and Discussion

Visually, the proposed method revealed good performance on forgery detection compared to recognition with traditional DCT method of block 2×2 which apparently giving more false positive results. Forgery detection result on the CoMoFoD image dataset shows in Figure 2.

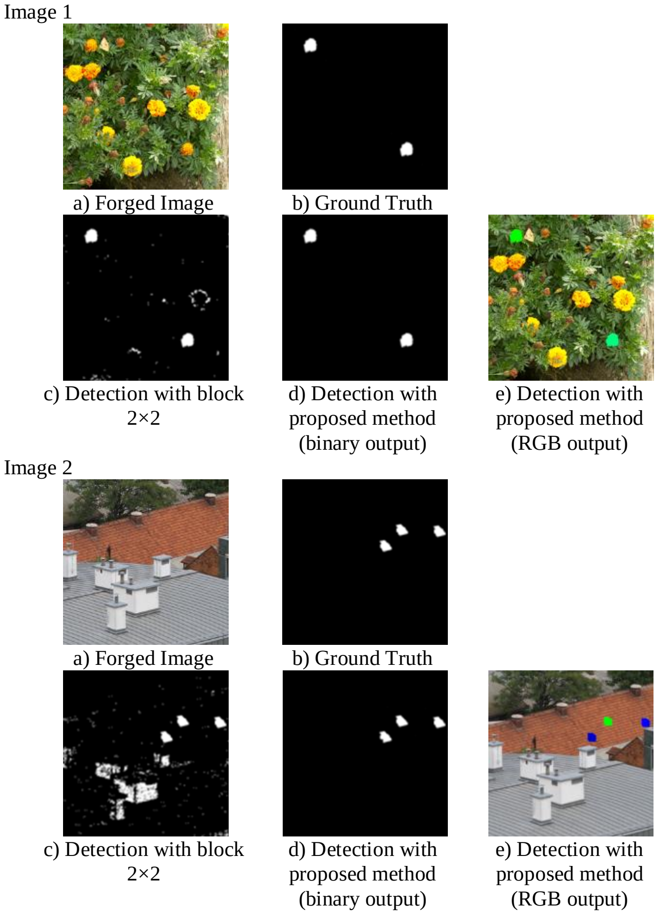

Image 1

a) Forged Image

b) Ground Truth

c) Detection with block 2×2

d) Detection with proposed method (binary output)

e) Detection with proposed method (RGB output)

Image 2

a) Forged Image

b) Ground Truth

c) Detection with block 2×2

d) Detection with proposed method (binary output)

e) Detection with proposed method (RGB output)

Figure 2. Forgery detection result on the CoMoFoD image dataset

The information about the actual predicted classifications of each image are in the form of TP (True Positive), FP (False Positive), and FN (False Negative). An ideal detection result should consist of high TP, low FP, as well as low FN.

The proposed method significantly produced high true positive result and low false positive and false negative results. Incidentally, the number of true positive result strongly relies to the size of the copy-move objects on each image. Positive and negative prediction values result shows in Figure 3.

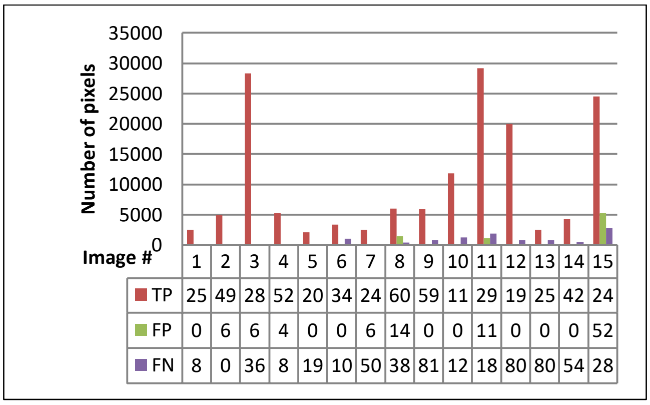

Image #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
🟥 TP	25	49	28	52	20	34	24	60	59	11	29	19	25	42	24
🟩 FP	0	6	6	4	0	0	6	14	0	0	11	0	0	0	52
🟪 FN	8	0	36	8	19	10	50	38	81	12	18	80	80	54	28

Figure 3. Positive and negative prediction values result

Table 2 gives a comparison of the performance of the proposed method against the implementation by [13]. The proposed method averagely surpassed the Precision rate of the benchmark method by 18.69%. However, it slightly underperformed in terms of the Recall value with 7.86% difference. Despite that, the proposed method exhibits superior accuracy in combined accuracy measures, F1 with a marked difference of 6.34% higher than the benchmark method.

Table 2. Benchmarking Result Comparison

Method	Precision	Recall	F_1
Christlein et al. (2012)	78.69	100	88.07
Proposed Method	97.38	92.14	94.41

The first four test images illustrated very impressive results which all Precision, Recall, and F1 values achieved almost 100% score. In terms of Precision, 87% of the images are giving a 100% rate. The Recall factor however, is fluctuated among the test images. It can be seen that although 4 of the images have a perfect Recall value, only 8 images achieve higher than 90% rate while the other 2 images have between 70% and 80% score. One of the images having low Recall value is image #6, which as previously mentioned, having less accuracy by the cause of some undetected copy move objects due to the reduced detection area based on the result of *coarse* detection in the first tier process. The accuracy result of the proposed method for each tested images shows in Figure 4.

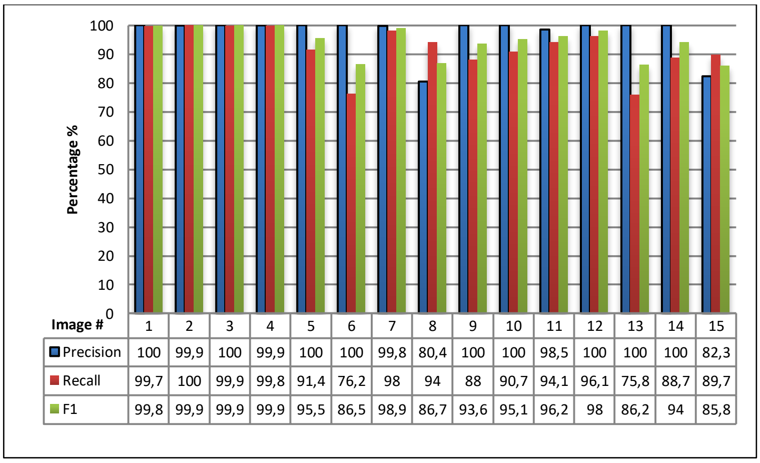

Image #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
🟦 Precision	100	99,9	100	99,9	100	100	99,8	80,4	100	100	98,5	100	100	100	82,3
🟥 Recall	99,7	100	99,9	99,8	91,4	76,2	98	94	88	90,7	94,1	96,1	75,8	88,7	89,7
🟩 F1	99,8	99,9	99,9	99,9	95,5	86,5	98,9	86,7	93,6	95,1	96,2	98	86,2	94	85,8

Figure 4. The accuracy result of the proposed method for each tested images

Figure 5 presents the comparison of F1 or combined factor results on each image of using overlapping large block, as well as the small block size, and the proposed method with detection by large block followed by the small block utilization. In this experiment, the proposed method which utilized variable block size is denote with B=16-2 that represents its two-tier detection by B=16 followed by B=2. The result indicates that each image used gave varied results when different block size is applied. On average, the result of F1 for B=16, B=2, and B=16-2 are 87.5%, 70.5%, and 94.4% respectively. This exposed that by combined factor judgment, the proposed method exhibits better accuracy compared to using only a single block size as in traditional method.

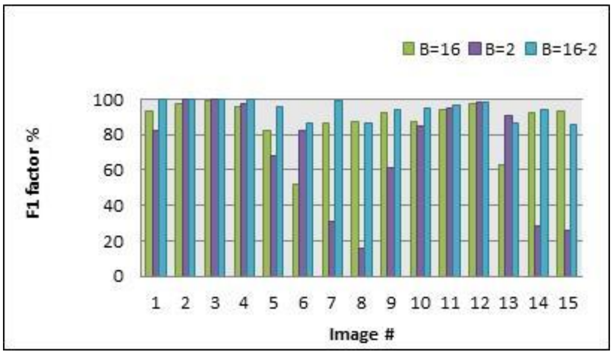

Figure 5. Comparison of F1 factor between traditional DCT CMFD method using block size 16 and 2 against coarse-to-fine approach with block 16 on first tier and block 2 on the second tier

Based on each image result, the proposed method is observed to have a clear advantage against B=16 seeing that the F1 percentage on all images with proposed method surpassed the result of the large block size. In spite of this, there is only 1 image that generated higher F1 value compared to the proposed method which is image #13. In this image, the accuracy using proposed method is less than B=2 for the reason that the detection on the first tier using large block size outputted an area of less than ideal to cover all forged areas. Therefore in this case, it implies that an optimal offset value should be applied so that it is able to include the entire possible forged regions.

Performance is measured by the value of execution time to complete the method algorithm. The assessment of required execution time is crucial in this experiment in view of the fact that the problem with small block usage is computationally expensive.

Although the proposed method requires roughly double execution time for DCT extraction, it significantly decreased the time required for the matching process by 83%, hence lessen the overall duration of forgery detection by 73% (refer to Figure 6). This implies that the proposed method is able to effectively lessen the execution time needed to process CMFD besides facilitate almost the same accuracy as using the small block size. It also suggests that the proposed method offers a worthy trade-off between accuracy and performance

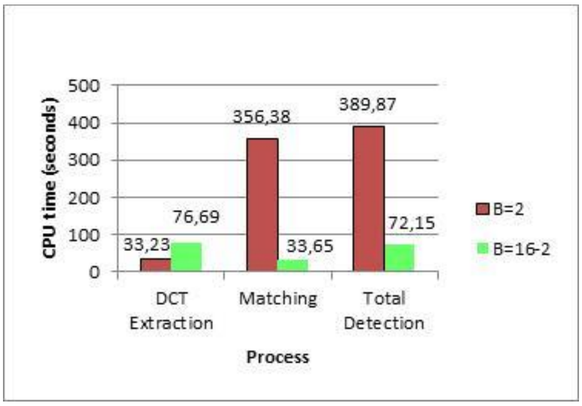

Figure 6. The accuracy result of the proposed method for each tested images

5. CONCLUSIONS

In this paper, it is proven that by applying the proposed approach, a better result in terms of accuracy and execution time is achievable as it is able to overcome the weaknesses of using the traditional DCT CMFD method using small block size. The proposed method is also capable of achieving a fine detection with less false positive results and execution time.

ACKNOWLEDGEMENTS

This research was funded by the short-term grant (No. 9001-00516) under Universiti Malaysia Perlis, Malaysia.

REFERENCES

[1] Farid, H., Image forgery detection. Signal Processing Magazine, IEEE, 2009. 26(2): p. 16-25.

[2] Fridrich, A.J., B.D. Soukal, and A.J. Lukáš. Detection of copy-move forgery in digital images. in in Proceedings of Digital Forensic Research Workshop. 2003. Citeseer.

[3] Thajeel, S.A. and G.B. Sulong, State Of The Art Of Copy-Move Forgery Detection Techniques: A Review. International Journal Of Computer Science Issues (IJCSI), 2013. 10(6).

[4] Wang, J.-W., et al., Fast and robust forensics for image region-duplication forgery. Zidonghua Xuebao/ Acta Automatica Sinica, 2009. 35(12): p. 1488-1495.

[5] Mahdian, B. and S. Saic, Detection of copy-move forgery using a method based on blur moment invariants. Forensic Science International (Online), 2007. 171(2): p. 180-189.

[6] Ryu, S.J., M.J. Lee, and H.K. Lee, Detection of Copy-Rotate-Move Forgery Using Zernike Moments. Information Hiding, 2010. 6387: p. 51-65.

[7] Popescu, A.C. and H. Farid, Exposing digital forgeries by detecting duplicated image regions. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[8] Kang, X., et al. Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. 2008. IEEE.

[9] Huang, H.L., W.Q. Guo, and Y. Zhang, Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. Paciia: 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vols 1-3, Proceedings, 2008: p. 1241-1245.

[10] Bo, X., et al. Image copy-move forgery detection based on SURF. in 2010 International Conference on Multimedia Information Networking and Security. 2010. IEEE.

[11] Bayram, S., H.T. Sencar, and N. Memon. A survey of copy-move forgery detection techniques. in IEEE Western New York Image Processing Workshop. 2008. Citeseer.

[12] Tralic, D., et al. CoMoFoD—New database for copy-move forgery detection. in ELMAR, 2013 55th International Symposium. 2013. IEEE.

[13] Christlein, V., et al., An Evaluation of Popular Copy-Move Forgery Detection Approaches. Ieee Transactions on Information Forensics and Security, 2012. 7(6): p. 1841-1854.

BIOGRAPHIES OF AUTHORS

	Mas Elyna Azol is a Lecturer at the Department of Electronic Engineering Technology, Faculty of Engineering Technology, Universiti Malaysia Perlis (UniMAP), Malaysia. She holds a Masters Degree in Science, specializing in Computer Science from the Faculty of Computer Science and Information Technology at Universiti Teknologi Malaysia (UTM). She is also a certified Professional Technologist (PTech) endorsed from the Malaysian Board of Technologist (MBOT). Her research interests include Image Processing, Information Security, Computer Science, and Software Engineering.
	Dr Nur Hidayah Ramli is a Senior Lecturer at the Department of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), Malaysia. She received her Ph.D in Electrical Engineering from Universiti Teknologi Malaysia. She is also a member of BEM and MBOT. Her research interests include antenna design and configuration, wireless sensor network, smart agriculture system and signal processing.

	Dr. Lee Yeng Seng is a Senior Lecturer at the Department of Electronic Engineering Technology, Faculty of Engineering Technology, Universiti Malaysia Perlis (UniMAP), Malaysia. He received his Ph.D. in communication engineering from the School of Computer and Communication Engineering at Universiti Malaysia Perlis (UniMAP), Malaysia. He also a member of IET, BEM, MBOT, IEEE and IEEE Microwave Theory and Techniques Society. His research interests include dielectric material characterization, microwave absorber, Frequency Selective Surface (FSS), and antenna.
	Siti Azura Abuzar is a Senior Lecturer at the Department of Electronic Engineering Technology, Faculty of Engineering Technology, Universiti Malaysia Perlis (UniMAP), Malaysia. He received her MSc in computer science from the School of Computer and Information Technology at Universiti Putra Malaysia (UPM). Her research interests include Cyber Security, Distributed Computing, Computer Network, Cloud Computing, and Network Security.