Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 1, July 2017, pp. 131 ~ 137
DOI: 10.11591/ijeecs.v7.i1.pp131-137

Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation Using Error Level Analysis

Teddy Surya Gunawan*[1], Siti Amalina Mohammad Hanafiah[2], Mira Kartiwi[3], Nanang Ismail[4], Nor Farahidah Za'bah[5], Anis Nurashikin Nordin[6]
[1,2,5,6]Department of Electrical and Computer Engineering, Kulliyyah of Engineering
[3]Department of Information Systems, Kulliyyah of ICT, International Islamic University Malaysia
Jalan Gombak, 53100 Kuala Lumpur, Malaysia, (+603) 6196 4521
[4]Electrical Engineering Department, Faculty of Science and Technology, Universitas Islam Negeri Sunan Gunung Djati, Bandung, Indonesia
*Corresponding author, e-mail: tsgunawan@iium.edu.my, tsgunawan@gmail.com

Abstract

Nowadays, image manipulation is common due to the availability of image processing software, such as Adobe Photoshop or GIMP. The original image captured by digital camera or smartphone normally is saved in the JPEG format due to its popularity. JPEG algorithm works on image grids, compressed independently, having size of 8x8 pixels. For unmodified image, all 8x8 grids should have a similar error level. For resaving operation, each block should degrade at approximately the same rate due to the introduction of similar amount of errors across the entire image. For modified image, the altered blocks should have higher error potential compred to the remaining part of the image. The objective of this paper is to develop a photo forensics algorithm which can detect any photo manipulation. The error level analysis (ELA) was further enhanced using vertical and horizontal histograms of ELA image to pinpoint the exact location of modification. Results showed that our proposed algorithm could identify successfully the modified image as well as showing the exact location of modifications.

Keywords: *JPEG compression; image forgery; image forensic; error level analysis*

1. Introduction

Photo manipulation is the act of altering the photo by removing the information or by adding it without leaving any obvious traces of tampering. Image manipulation or known as images forgeries is not new in the photography world. Photographs were already being manipulated only a few decades after Niepce created the first photograph in 1814. Figure 1 shows the example of image forgery around 1865. In this photo by famed photographer Mathew Brady, General Sherman is seen posing with his Generals. The image were tampered by adding General Francis P. Blair in the original image [1].

Due to widely spread of cheap (sometimes free), easy-to-use and advance image editing software that available on the internet, a digital photo can be easily altered even by novice user. In consequence, the digital manipulated images were increase rapidly in the media and the internet and this phenomenon could create serious vulnerabilities and lower the value digital images. Hence, the importance of creating images manipulation detection algorithm has a great impact to determine the originality and integrity of digital images since peoples are using these images as evidence during the trial, news items, and other purposes.

Received March 25, 2017; Revised June 2, 2017; Accepted June 20, 2017

(a) (b)

Figure 1. Image forgery, circa 1865: (a) General Francis P. Blair (far right) was added to the original photograph, (b) The original photo which General Blair was not present

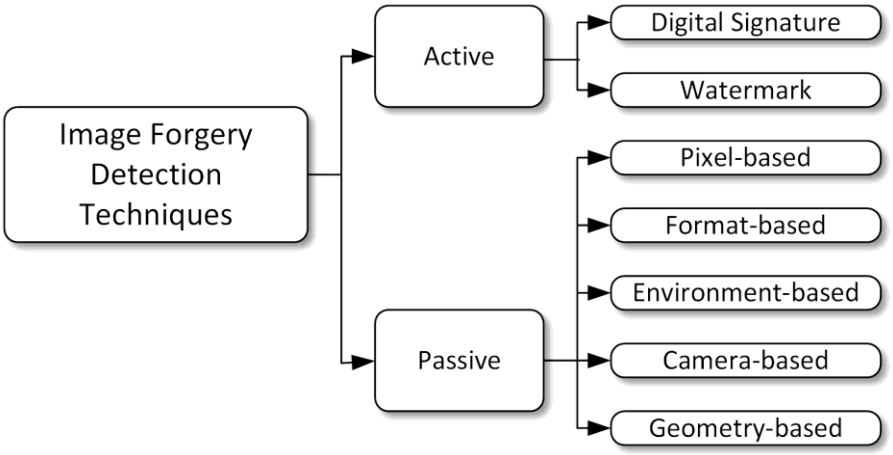


Figure 2. Image Forgery Detection Techniques

JPEG image [2] is one of the most extensively used image formats in many websites as tracked by [3]. There are many researches have been conducted for image forgery detection. Figure 2 shows the classification of image forgery detection techniques as reviewed by [4, 5]. Many techniques have been developed to detect image manipulation, such as JPEG error analysis [6], median filter [7], improved discrete cosine transform (DCT) [8], contrast-enhancement [9], DCT based detection on multiple chain manipulations [10], maximal entropy random walk [11], and recently quantization step estimation [12]. There also active researches in the field of anti-forensics [13, 14], recovery of fragmented JPEG files [15], and a new performance metric for image forensic [16].

Of the various techniques available for image forgery detection, we selected pixel-based technique which is the most common technique [4]. The two most common technique in pixel-based are cloning, also known as copy-move or copy-paste, and slicing. Image splicing is done by copying one portion of the image and paste it to other image. Error level analysis is one of the most successful technique to detect image manipulation [17, 18]. We further evaluate the effectiveness of error level analysis for different image captured by digital camera and smartphone. Therefore, the objective of this paper is to develop a photo forensics algorithm using error level analysis and evaluate its effectiveness on the image captured by digital camera and smartphone camera and manipulated by Adobe Photoshop.

2. Overview of JPEG Image Compression

JPEG is a lossy compression technique based on the combination between spatial domain and frequency domain [2]. Figure 3 shows the process of JPEG compression and decompression. The raw data image is divided into 8x8 blocks and conduct color transformation and down-sampling to reduce the data for processing. It is then transformed into the frequency domain using DCT. The DCT coefficient is ordered in zigzag manner and quantized using quantization table. The lossless entropy coding compress the quantization coefficients to form a new JPEG file. The inverse process is occurred for JPEG decompression. The size of the JPEG compression image is depends on the content and quality of the image. The homogeneous image with few objects requires fewer bits compared to a complex scene image with many objects. Many image manipulations using Adobe Photoshop or GIMP, for example, will usually resave and recompress it as a new JPEG image.

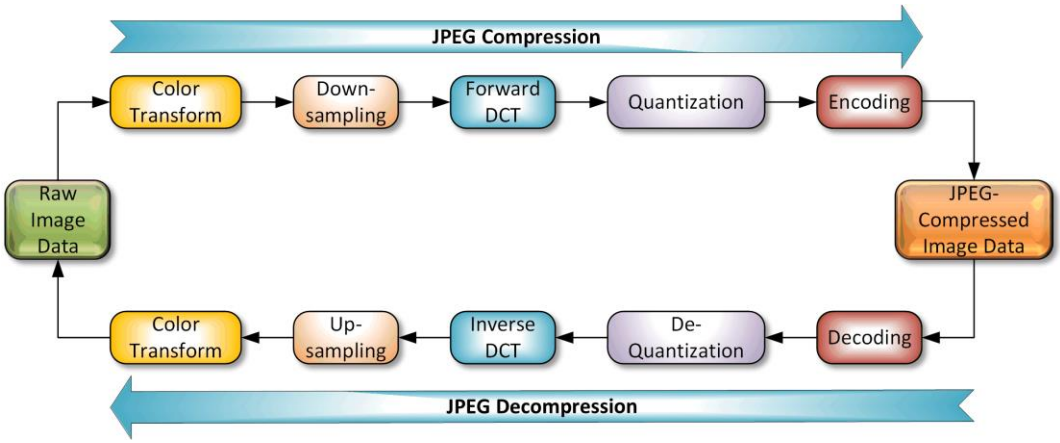


Figure 3. JPEG Compression and Decompression

3. Image Forensic Detection using Error Level Analysis

Error level analysis (ELA) is one of the technique to detect image manipulation by resaving the image at a specific quality level and then computing the difference between the compression levels. If the images are not altered, 8x8 squares should have similar error potentials [17]. However, if the image is altered, the portion of the image that have manipulated should have higher error potential than other part of the image. ELA works by intentionally resaving the image at a known error rate, such as 95%, and then computing the difference between the images.

When a JPEG photograph is first saved, it compresses the photo for the first time. Most image editing software such as Adobe Photoshop or GIMP supports the operation of JPEG compression. Therefore, if the image is then opened into Photoshop, edited and saved again as a JPEG, it will be compressed again. From this process, it shows that the “original” parts of the photographic image have been compressed twice which are once by the camera that took the photo and again by Photoshop. Whereas, the “edited” part of the photographic image, was only compressed once, by Photoshop. To the human eye, we cannot notice the difference by looking at the image. However, we can compare the two images together and look at the differences.

Figure 4(a) shows the JPEG quality approximation algorithm [17]. It can be summarized by computing the difference between the average value from quantization table Y (luminance) and CrCb (chrominance), as shown in Equation (1). The illustration of the ELA algorithm quality value is shown in Figure 4(b), in which the difference error level in certain blocks could define the modified area.

$$\begin{aligned} \mu &= \frac{Y + Cr + Cb}{3} \\ \Delta &= |Y - Cr| \times (1.0 - 0.51) + |Y - Cb| \times (1.0 - 0.51) \\ Q &= 100 - \mu - \Delta \end{aligned} \tag{1}$$

The error degree is increased in resave operations. Subsequent resave operations could reduce the error level potential and shows through a darker ELA results. After a number of resave operations, the square grid may reach its minimum level. Therefore, frequency and details could be missing by each resaving operation. The error produced by ELA algorithm could help detecting the manipulations of JPEG images.

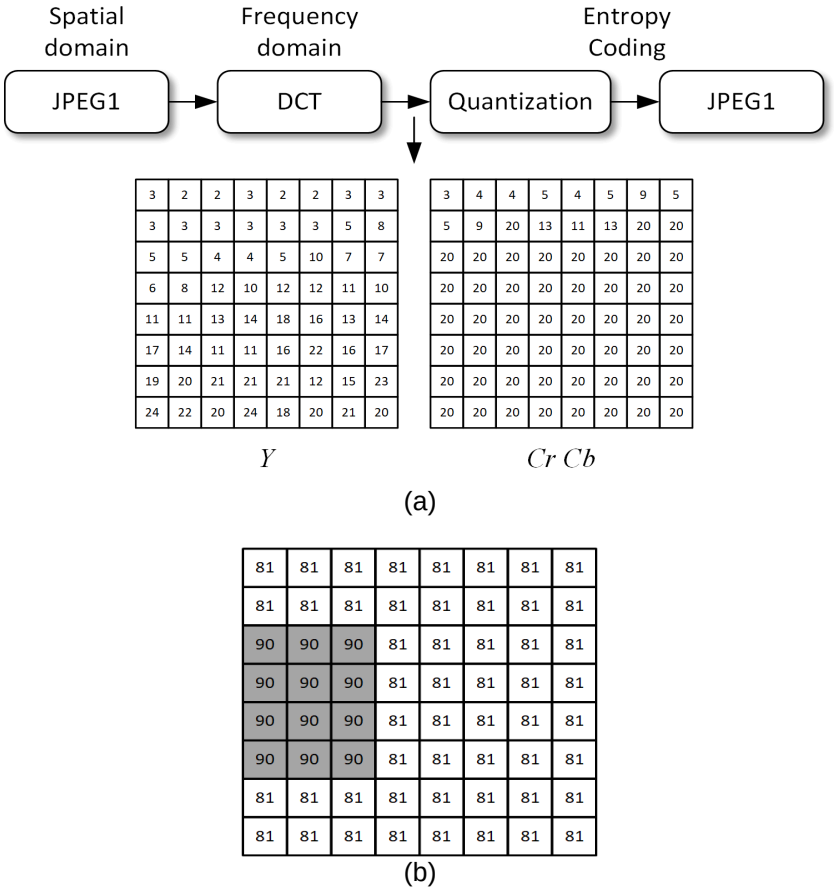


Figure 4. JPEQ Quality and Error Level Analysis, (a) JPEG Image Quality Approximation, (b) ELA algorithm quality value

4. Results and Discussion

4.1 Experimental Setup

For this research, a total of 20 images were captured by two imaging devices, 10 by Nikon D3000 and the other 10 by Nokia 301 by our own. This is to ensure that the analysis is not depending on the camera resolution and quality setting. It will ensure that the image is original without any tampered. The ELA algorithm was implemented using Matlab R2017a on Microsoft Windows 10 64bits. The hardware used was a computer with i7 Core, 16 GB RAM, and 1 TB hard disk. Moreover, the performance measures used are SNR, MSE, and PSNR.

4.2 JPEG Compression with Various Quality Levels

The first experiment is on the variation of quality levels in JPEG compression. To evaluate what is the quality level appropriate for our ELA experiment, we observed the SNR, MSE, and PSNR value. For this purpose, we set the quality level to 75%, 85%, and 95%, as shown in Table 1. From the table, it is shown that using quality level of 95% is better for JPEG compression algorithm. Therefore, we decided to use quality level of 95% for the next experiments.

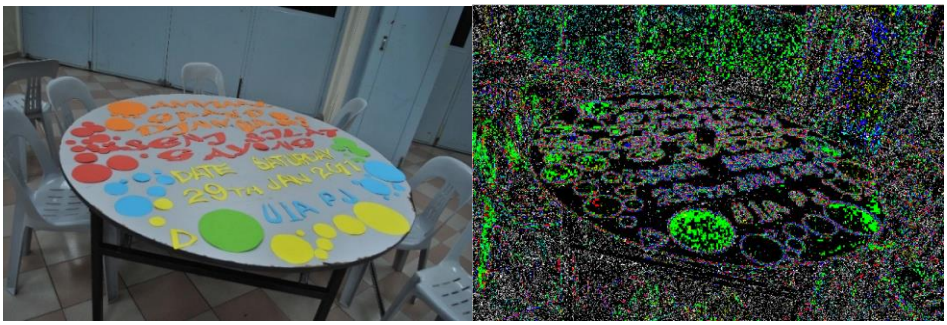
Table 1. Performance of JPEG Compression at Various Quality Levels

Quality level	95%	85%	75%
SNR	30.15	29.37	30.05
MSE	4.96	5.93	5.072
PSNR	41.18	40.40	41.08

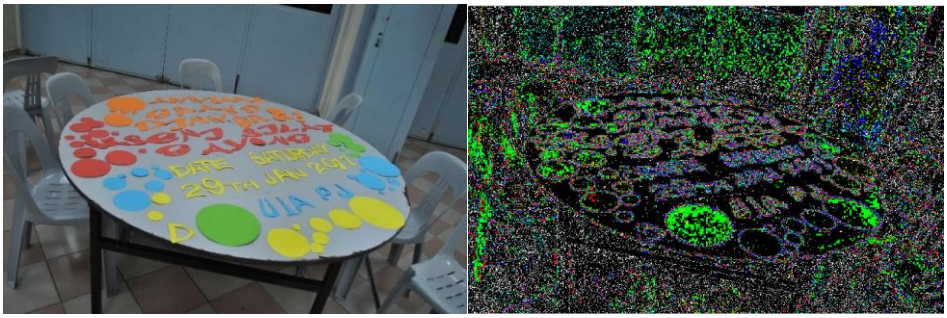
4.3 Experiment on JPEG Quality Level Modification

In this experiment, the original photo from digital camera was resaved at 75% quality level, and then resaved again at 75% quality level using Adobe Photoshop. Each picture is associated with the 95% ELA for the image. Error state is calculated as the difference between original image and resaved image.

(a) Original photo from a digital camera.



(b) First resaved at 75% from original photo



(c) Second resaved image from first resaved image

Figure 5. Experiments on Image Resaving with Varying Quality Levels

From Figure 5, we can conclude that the original image from the digital camera have a high ELA value meanwhile if the images are resaved multiple times it will lower the ELA value (getting darker). Because of the image is only perform resaving without any modification, therefore we can not detect any noticeable modification.

4.4 Experiment on Image Manipulation

Figure 6(b) shows the ELA result of manipulated image shown in Figure 6(a). The ELA results showed that the person in the image have been manipulated. This is because the modified part shown higher ELA while the background showed lower ELA value (darker). If the images are not altered, 8x8 squares should have similar error potentials (dark). However, if the image is altered, the modified part will have higher error potential.

To make it easier to identify which part of the image have been manipulated, we analysed the vertical and horizontal histogram as shown in Figure 6(c) by converting the ELA image into grayscale value and counting number of pixels have certain intensity in each horizontal and vertical direction. Based on the histogram, we could derive the top left and bottom right coordinates, in which we can draw a red box indicator as shown in Figure 6(d).

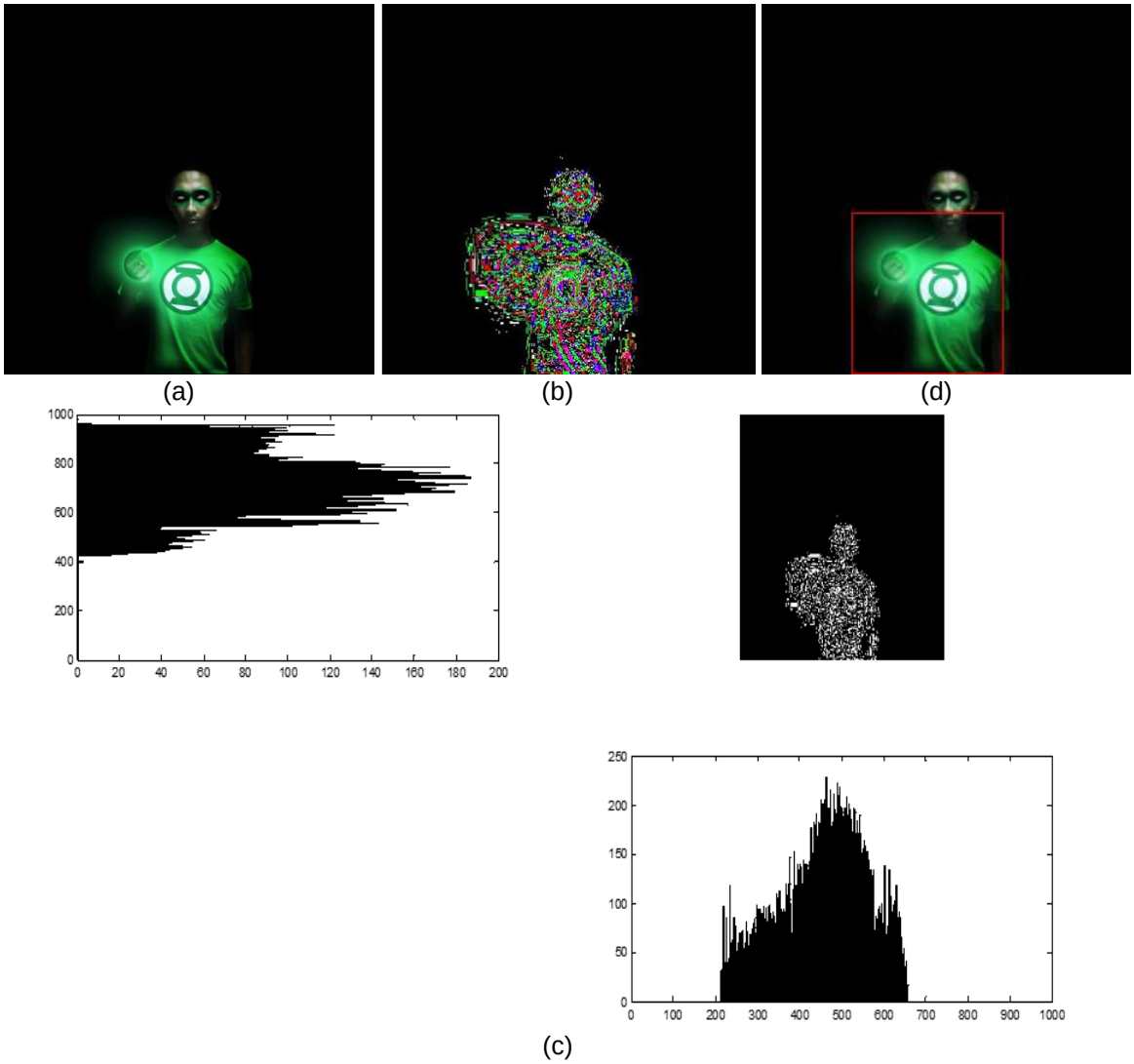


Figure 6. Experiment on Image Manipulation, (a) Manipulated Image, (b) ELA image, (c) Horizontal and Vertical Histograms of ELA image, (d) Detected area in which the image have been modified.

5. Conclusions and Future Works

This paper has presented the design and development of image forensic application on JPEG images. Error level analysis was used to detect any modification on the JPEG images. Around 20 images have been captured using digital camera and smartphone. The first

experiment observed the relationship between JPEG quality levels, i.e. 75%, 85% and 95%, and its image quality in terms of SNR, MSE, and PSNR. The second experiment is resaving the original JPEG images for several times with the same quality levels. No noticeable difference was observed from this experiments. The last experiment is the ELA on the modified image, in which noticeable difference was observed. We further enhance the ELA algorithm by identifying the part of the image which have been modified using vertical and horizontal histograms of ELA image. Further research could be conducted on the use of deep neural network to detect the image forgery.

Acknowledgement

This research has been supported by International Islamic University Malaysia Research Grant, RIGS16-336-0500.

References

[1] M. Fineman, *Faking it: Manipulated photography before Photoshop*, Metropolitan Museum of Art, 2012.
[2] G. K. Wallace, "The JPEG still picture compression standard," *IEEE transactions on consumer electronics*, vol. 38, pp. xviii-xxxiv, 1992.
[3] W3Techs, "Usage of image file formats for websites," [http://w3techs.com/technologies/overview/image_format/all], Retrieved on: 1 June 2017.
[4] M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review," *IETE journal of education*, vol. 55, pp. 40-46, 2014.
[5] H. Jin, "Research of Blind Forensics Algorithm on Digital Image Tampering," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, pp. 5399-5407, 2014.
[6] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 480-491, 2010.
[7] H.-D. Yuan, "Blind forensics of median filtering in digital images," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1335-1345, 2011.
[8] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic science international*, vol. 214, pp. 33-43, 2012.
[9] G. Cao, Y. Zhao, R. Ni, and X. Li, "Contrast enhancement-based forensics in digital images," *IEEE transactions on information forensics and security*, vol. 9, pp. 515-525, 2014.
[10] V. Conotter, P. Comesana, and F. Pérez-González, "Forensic detection of processing operator chains: Recovering the history of filtered JPEG images," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2257-2269, 2015.
[11] P. Korus and J. Huang, "Improved Tampering Localization in Digital Image Forensics Based on Maximal Entropy Random Walk," *IEEE Signal Processing Letters*, vol. 23, pp. 169-173, 2016.
[12] T. H. Thai, R. Cogranne, and F. Retraint, "JPEG Quantization Step Estimation and Its Applications to Digital Image Forensics," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 123-133, 2017.
[13] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 1211-1226, 2014.
[14] Y. Li and J. Zhou, "Anti-Forensics of Lossy Predictive Image Compression," *IEEE Signal Processing Letters*, vol. 22, pp. 2219-2223, 2015.
[15] J. De Bock and P. De Smet, "JPGcarve: An advanced tool for automated recovery of fragmented JPEG files," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 19-34, 2016.
[16] M. Al-Ani and F. Khelifi, "On the SPN Estimation in Image Forensics: A Systematic Empirical Evaluation," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 1067-1081, 2017.
[17] N. Krawetz, "A pictures worth digital image analysis and forensics," *Black Hat Briefings*, pp. 1-31, 2007.
[18] N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab, and R. Salleh, "An evaluation of Error Level Analysis in image forensics," in 2015 5th IEEE International Conference on System Engineering and Technology (ICSET), pp. 23-28, 2015.