An Evaluation of Error Level Analysis in Image Forensics

Nor Bakiah Abd Warif[1], Mohd. Yamani Idna Idris[2], Ainuddin Wahid Abdul Wahab[3], Rosli Salleh[4]
Department of Computer System and Technology,
Faculty of Computer Science & Information Technology
University of Malaya
Kuala Lumpur, Malaysia
[1]nurbaqiyah@siswa.um.edu.my, [2]yamani@um.edu.my, [3]ainuddin@um.edu.my, [4]rosli_salleh@um.edu.my

***Abstract*— The advancement in digital image tampering has encouraged studies in the image forensics fields. The image tampering can be found over various image formats such as Joint Photographic Experts Group (JPEG). JPEG is the most common format that supported by devices and applications. Therefore, researchers have been studying the implementation of JPEG algorithm in the image forensics. In this paper, the Error Level Analysis (ELA) technique was evaluated with different types of image tampering, including JPEG compression, image splicing, copy-move and image retouching. From the experiment, the ELA showed reliability with JPEG compression, image splicing and image retouching forgery.**

***Index Terms*— image forensics, JPEG compression, error level analysis.**

I. Introduction

The rapid growth of digital imaging technologies has enabled the imaging devices with high resolution at low cost. This has led to the extensive use of digital images for various purposes. Unfortunately, the digital image often manipulated to misrepresent the content of the original image. Consequently, the digital image is no longer trusted by the society and resulting in the development of image forensics study. Generally, image forensics is an area of studies that identify the origin and verify the authenticity of an image.

The image forensics studies are categorized into two types which are active authentication and passive authentication. The active authentication requires additional information about the original image. This includes the process of embedding a watermarking into an image or extracting a unique feature as a signature of the image. In opposite, the passive authentication that known as a blind detection technique requires no additional information about the original image. There are two categories in passive authentication, which are identifying the source device and detecting the image tampering. Detecting the image tampering is refers to the use of analysis or statistical techniques to detect the forged regions.

In this paper, we present and discuss an error level analysis (ELA) technique for the passive authentication in image forensics involving JPEG compression, image splicing, copy-move image forgery and image retouching. There are two contributions to this paper. First, we use the compression and resizing technique for the data creation in three main types of image tampering. Second, the ELA technique is applied to the data and the outcomes are shown and explained thoroughly. Therefore, the reliability of the technique for image forensics can be further improved.

The rest of the paper is organized as follows. Section II explains in details the main types of image tampering in image forensics. The explanation of JPEG compression and ELA technique is given in the Section III. Experimental results and discussion are presented in Section IV, continue with section V which discusses the conclusion and recommendation.

II. Image Forensics

The advancement of the editing software made it easy for a person to manipulate the original image without leaving any visible clues. The image tampering can be categorized into three types; image splicing, copy-move image forgery and image retouching [1] as follows:

A. Image splicing

An image splicing is a process of combining two or more images to create a new image. A particular region is copied from one image and pasted into another to form a different image. The dissimilarity in the spliced region can be directed to the de-correlation detection [2].

B. Copy-move forgery

A copy-move forgery is a common type of image tampering. It involves a process of copied and pasted within the same image. The copied region is commonly modified by operations such as scaling, rotation, and adding noise to blend the manipulated region with the surrounding area [3]. As a result, the tampering is therefore difficult to detect by the human eyes.

C. Image retouching

An image retouching is a process of altering copied pixels to match the surrounding pixels [4]. It can be either improving or reducing some features of the original image without altering its true meaning. This type of tampering is commonly performed by the magazine editors to make the image more attractive[5].

978-1-4673-6713-4/15/$31.00 ©2015 IEEE

III. JPEG COMPRESSION

JPEG is a standard compression method developed by the Joint Photographic Experts Group. The JPEG algorithm is a lossy compression technique based on the combination between spatial domain and frequency domain [6].

Fig. 1 shows the process of JPEG compression and decompression in an image. Firstly, the bitmap image is divided into 8 × 8 blocks and transformed into the frequency domain using the Discrete Cosine Transform (DCT). Then, the DCT coefficient d1 is quantized by a quantization table that result in the quantization coefficient Qd1. Next, the lossless entropy encoding will further compress the Qd1 coefficient to form a new JPEG file. Meanwhile, inversion process is occurred for JPEG decompression. The JPEG file is first entropy decoded to retrieve the exact quantized coefficient Qd1 values. Then, the values are multiplied by the table to get the dequantized coefficient d'1. Next, the inverse DCT (IDCT) is performed to get the pixel values in real-valuedrepresentation.

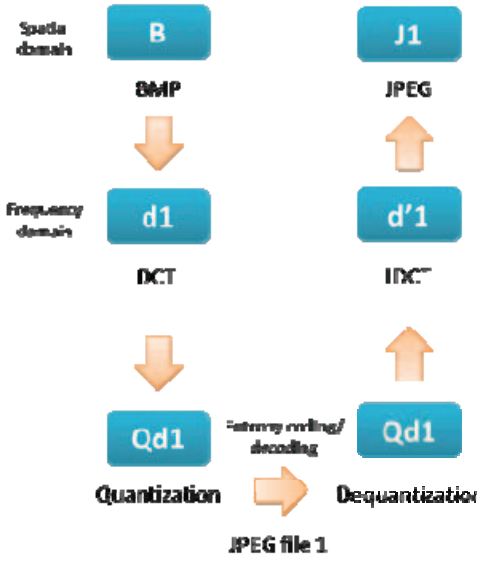

Fig. 1. JPEG compression and decompression process

Moreover, the size of the JPEG compression image is depends on the content and quality of the image. Usually, the homogeneous image requires fewer bits rather than a detailed image while a high quality image provides more details content with a larger size [7]. As the JPEG format is supported by many devices and software applications, analyzing this image format will play an important role in image forensics [8].

A. JPEG Compression in Image Forensics

In many tampering cases, the image usually resaved and recompressed as a new JPEG image. Therefore, the tampering can be detected through the recompression.

Chen and Hsu [9] proposed a new method. The periodic characteristics of JPEG images both in spatial and transform domains are suggested to formulate in order to create a robust detection approach. Alternatively, Bianchi and Piva [10] proposed a statistical model to describe the artifacts that exist in the presence of either A-DJPG or NA-DJPG for any kind of recompression.

B. Error Level Analysis (ELA)

ELA is a JPEG compression algorithm for image forensics detection. As discussed in Section III, the frequency coefficient from the image is quantized by the quantization table and followed by the entropy encoded process. Krawetz with his team (Hacker Factor Solution) adopted the quantization process to develop an algorithm to approximate the JPEG quality. Fig. 2 presents the JPEG quality approximation algorithm as reported in Krawetz study [11]. Through the equations, the JPEG quality calculation can be summarized by computing the difference between the average value from quantization table Y (luminance) and CrCb (chrominance).

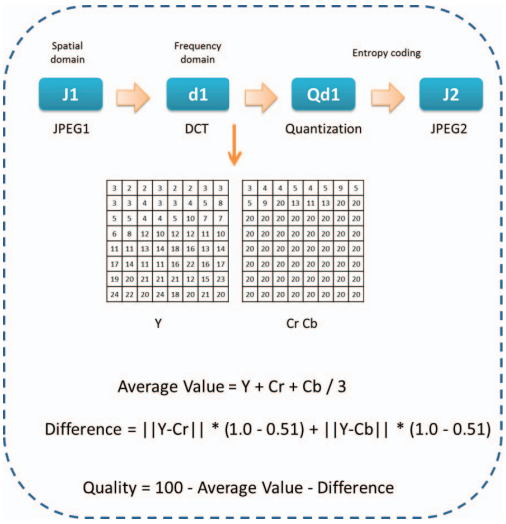

Fig. 2. JPEG quality approximation algorithm

Using ELA, the image is further divided into 8 × 8 blocks and recompressed independently at a known error rate such as 95%. Every square should give an approximately the same quality rate if the image is completely unmodified. The error level is of the loss information during the image is saved in the JPEG format. The illustration of the ELA algorithm quality value is shown in Fig. 3. In the figure, the difference error level in certain blocks could define the modified area.

Additionally, the degree of error will be increased upon the resave operations. Subsequent resave operations could reduce the error level potential and showed through a darker ELA results [12]. After a number of resave operations, the square grid may reach its minimum error level. Therefore,

81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81

Fig. 3. The illustration of the ELA algorithm quality value

frequency and details could be missing by each resaving operation.

However, the amount of error in ELA is limited to the 8×8 blocks. The block error has reached its local minima if no changes in the quality level. The pixels are not at their local minima if there is a large amount of change later could identify the changes [11]. For instance, saving a 90% image and then resaving it at 90% again will generate virtually the same image for a one-time save of 81%. Moreover, blue or red areas designed by the ELA represent the changes done by the commercial software such as Photoshop and GIMP.

The error produced by the ELA technique could help identifying the manipulations in the JPEG images. After all, the ELA technique can be summarized as a process of quality level evaluation of grids squared within the images.

Based on the characteristics of the ELA, the technique is believed could be useful to image forensics area. Henceforth, the following section explains the experiments results and discussions.

IV. Experiments

A. Experimental Setup

In the experiment, we used the ELA technique introduced by Krawetz [11] which available online from the website (http://fotoforensics.com/). The experimental environment as follows, the operating system is based on the Windows 7 64 bit with Google Chrome browser version 43.0.2357.65. Due to no standard dataset on the JPEG compression and resizing technique, we create our own image combines with the technique for each type of image tampering. The test images are taken by the camera from Ipad Mini 2 and edited using Adobe Photoshop CS5 software. The experiments are done with different types of image tampering including:

1) *Original image with different compression*
2) *Resizing the original image*
3) *Image splicing with 60% JPEG compression*
4) *Spliced image in image resize*
5) *Copy-move image forgery with 60% JPEG compression*
6) *Copy-move image forgery in image resize*
7) *Image retouching*

B. Experiments Result and Discussion

In this section, the results obtained from the experiments are discussed. The ELA was tested with different types of image tampering as presented in the following.

1) Original image with different compression

From the experiment, the ELA is able to detect the manipulation even with unchanged region. A high quality of JPEG image will yield obvious white ELA results while the lower quality will generate darker results. Fig. 4 shows the results for different quality of JPEG compression in the original image.

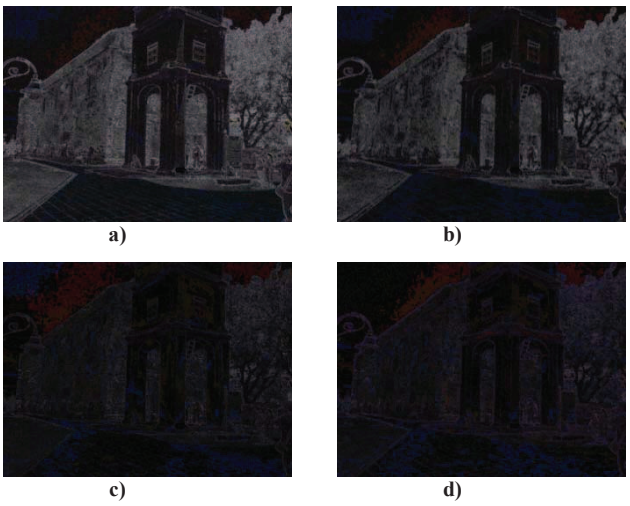

Fig. 4. ELA results for: a) Original image b) Image with JPEG quality 90% c) Image with JPEG quality 70% d) Image with JPEG quality 50%

2) Resizing the original image

Fig. 5 presents more noise results when the image has been resized instead of compressed. Furthermore, the bluish edge represents that the image has been edited by Adobe Photoshop software.

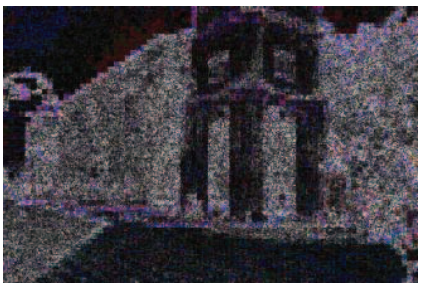

Fig. 5. ELA results when the image is resized to 600×400

3) Image splicing with 60% JPEG compression

In this case, ELA were evaluated through the edge and smooth variations. The level of whiteness and brightness between the edges should be identical for the original image. Likewise, similar smooth regions should have a similar error level for each variation. For instance, image splicing as discussed in the Section II.A should produce a result that displayed the difference at the edges or smooth variations. Fig. 6 presents the contrast of the white area at the sleeves of a person in the image. Thus, the sleeves are the possible manipulated regions of the image.

a)

b)

Fig. 6. a) Sample of image splicing b) ELA results for the sample with 60% JPEG compression

4) Spliced image in image resize

When the original image has been resized, the ELA shows more noise that could make the manipulated regions even harder to detect. As we can see in the Fig. 7, the possible manipulated regions could be the text of "Rumah Sarawak" inside the signboard;

Fig. 7. ELA results for image splicing with image resized

5) Copy-move image forgery with 60% JPEG compression

Differs from image splicing, copy-move image forgery is difficult to detect due to the possible copied regions have the same quality level. Nevertheless, ELA can help to identify the manipulated regions if the original image has another quality level with the copied regions. Fig. 8 shows that the top lamp is much brighter in white compared to the bottom lamp. Therefore, the possible copy-move regions could be the top lamp.

a)

b)

Fig. 8. a) Sample of copy-move image forgery b) ELA results for the sample with 60% JPEG compression

6) Copy-move image forgery in image resize

Unlike image splicing, ELA gives poor results in copy-move image forgery with image resize. The copied regions are seen to be impossible to detect (see Fig. 9).

Fig. 9. ELA results for copy-move image forgery with image resized

7) Image retouching

On the contrary, Fig. 10 presents the different ELA results like the original image (see Fig. 10a) with the retouching image (see Fig. 10b). It is shown that the face of the person has some noise with a few white areas compared to the original image. In that case, the face might be tampered with image retouching forgery.

Image Retouching

a) b)

Fig. 10. ELA results for: a) Original image b) Image retouching

Based on the results, we can see that the tool provided by Krawetz is displayed in image representation. The analysis therefore is too much depending on human interpretation and might give the incorrect result. We intended to improve the tool as a system specifically to provide quantitative results for the performance of the ELA technique.

V. Conclusion

Based on the different conditions of image tampering tested with the ELA technique, we can see that the technique can be further improved in image forensics. ELA shows significant results on the JPEG compression, image splicing and image retouching. Besides, ELA can be useful to any size of image, as long as no resize operation has been performed. For future direction, the planning is to study on how to expand the results for copy-move image forgery and image resize.

Acknowledgment

This work is fully funded by Bright Sparks Unit, University of Malaya, Malaysia, and partially funded by the Ministry of Education, Malaysia under the University of Malaya High Impact Research Grant UM.C/625/1/HIR/MoE/FCSIT/17.

References

[1] W. Lin, S. U. Khan, K. C. Yow, T. Qazi, S. a. Madani, C.-Z. Xu, J. Kołodziej, I. a. Khan, H. Li, and K. Hayat, "Survey on Blind Image Forgery Detection," *IET Image Process.*, vol. 7, no. 7, pp. 660–670, Oct. 2013.

[2] X. Zhao, J. Li, S. Li, and S. Wang, "Detecting digital image splicing in chroma spaces," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6526 LNCS, pp. 12–22, 2011.

[3] M. Hussain, S. Q. Saleh, H. Aboalsamh, G. Muhammad, and G. Bebis, "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection," in *IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings*, 2014, pp. 197–204.

[4] D. R. Cok, "Cloning Technique For Digital Image Retouching," 1996.

[5] S. Sadeghi, H. a Jalab, and S. Dadkhah, "Efficient Copy-Move Forgery Detection for Digital Images," *World Acad. Sci. Eng. Technol.*, vol. 71, no. 11, pp. 542–546, 2012.

[6] M. Shneier, "Exploiting the JPEG compression scheme for image retrieval," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 18, no. 8, pp. 849–853, 1996.

[7] B. Arcangelo and M. Massimo, "JPEG compression factor control: a new algorithm," *Int. Conf. Consum. Electron. 2001. ICCE.*, pp. 206–207, 2001.

[8] L. Weiqi, H. Jiwu, and Q. Guoping, "JPEG Error Analysis and Its Applications to Digital Image Forensics," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 480–491, 2010.

[9] Y.-L. Chen and C.-T. Hsu, "Detecting Recompression of JPEG Images via Periodicity Analysis of Compression Artifacts for Tampering Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 396–406, Jun. 2011.

[10] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, pp. 1003–1017, 2012.

[11] N. Krawetz, "A Picture ' s Worth□: Digital Image Analysis and Forensics," 2008.

[12] P. Paganini, "Photo Forensics: Detect Photoshop Manipulation with Error Level Analysis," 2013. [Online]. Available: http://resources.infosecinstitute.com/error-level-analysis-detect-image-manipulation/. [Accessed: 21-May-2015].