International Journal of Electrical, Electronics and Data Communication, ISSN(p): 2320-2084, ISSN(e): 2321-2950
Volume-6, Issue-10, Oct.-2018, http://iraj.in

DEVELOPMENT OF THE ERROR LEVEL ANALYSIS FORENSIC TOOL FOR IMAGES SHARED OVER MESSAGING AND SOCIAL NETWORKING APPLICATIONS

[1]ALAA HILAL, [2]SARAH ABOU CHAKRA

Faculty of Technology – Aabey Lebanese University, Lebanon
E-mail: [1]alaa.hilal@ul.edu.lb, [2]sabouchakra@ul.edu.lb

Abstract - Error level analysis is considered as a forensic tool that reveals forged regions in JPEG images. Though being regarded as a simple method; it is considered as an indispensable block in digital image examination routine. Conversely, it has poor performance over images that have been heavily compressed such as images shared over messaging and social networking applications. In this paper, we develop the error level analysis method in order to reveal forgeries in these specific low-quality images. The error-level map is generated and obtained by analyzing the frequency coefficients of the image using the discrete cosine transform. AC coefficients are limited in order to minimize high frequency noise. A specific database of images captured by mobile phones, altered and then shared over well-known messaging and social networking applications is created. The developed method is then implemented and examined over the database. Obtained results show higher readability and better image modifications discrimination than those obtained with the original error analysis method.

Keywords - Error Level Analysis; Digital Image Processing; Discrete Cosine Transform.

I. INTRODUCTION

The last decade has witnessed a huge spread in the use of digital images. Images can be captured using a variety of devices including digital cameras, smart phones and tablets. The recent advances in technology as well as smart-phone market is bringing the professional digital single-lens reflex cameras and the camera-supported smart phones close together. Combining the medium for photography, the digital signal processing power, and the telecommunications connectivity, these devices can take digital photos and transmit the images wirelessly in terms of seconds. The images are in soft copy and can be easily sent to a specific address, transferred and shared using messaging applications. However, from another perspective the availability of graphical editors enabled the user to perform a wide range of editing to the image. Such maneuvers vary from slight modifications like color corrections and image cropping to more serious transformations such as manipulating, removing or duplicating objects in an image. This latter kind of editing is classified as an image forgery.

In view of that,digital image forensics have emerged as a recent science that seeks into verifying the authenticity of digital images. It incorporates specific tools that searches for traces left from various types of forgeries including double, cropping, resampling [1], and copy-paste transformations[2]. Moreover, there has been a lot of attention into adapting forensic tools to detect forgeries in images saved under JPEG (Joint Photographic Experts Group) format[3], [4]. This later is recognized as the most common format used by digital cameras and camera-supported mobile devices. Moreover, it consists 45% of the image requests by format for storing and transmitting photographic images on the World Wide Web[5]. Among the various forensic tools, the error level analysis (ELA) method seeks to expose forgery traces uniquely in JPEG images. It is considered as an essential block in JPEG images investigation routine and it can be found in almost every forensic analysis product[6]. However, no specific development has been made in order to adapt this method for the characteristic features of JPEG images captured by camera-supported mobile phones and shared using messaging and social networkingapplications. Therefore, we develop in what follows, a frequency based method that examines these type of images. First, we explain the ELA method and the related work in section II. In section III, we propose and explain our method. Results are presented and analyzed in section IV before finishing with conclusions in section V.

II. RELATED WORK

ELA method[7],[8], [9], [10]makes use of the lossy characteristic of the JPEG compression algorithm.In fact, JPEG format works following a three main steps process. First, the RGB color image is converted into the YCbCrspace. Y is the luma component that represents the brightness of the color. Cb and Cr are the chrominance components of the blue and the red colors relative to the green color.The human eye is more sensitive to Y component than to Cb and Crcomponents. JPEG format accounts to this characteristic by representing Y components with more accuracy than Cb and Cr components.The image is then transferred into the frequency domain by applying discrete cosine transform over every 8×8 pixels blocks of the down-sampled image.A quantization step, that is responsible of the lossy feature, is later applied in order to discard high-frequency components and save the obtained result,

after entropy encoding, in bit-stream. The values of the quantization coefficients define the quality under which the image is compressed. ELA methodoperates by recompressing the JPEG imageto a certain quality. The recompressed image is then subtracted, pixel by pixel, from the original image. The obtained result, known as error level image (ELI), depicts the various quality levels in the image and can be interpreted under two scenarios:

Scenario A: we consider that an authentic JPEG image will have a quality level $Q1$depending on the compression algorithm. When recompressing the image again, values in the 8×8 pixels block will be re-quantized. The amount of error introduced due to the lossy compression after each re-save is not linear. For instance, an initialimage with quality $Q1$=90%that has been recompressed and saved at aquality$Q2$=90% is similar to having the raw image one-time saved at quality Q=81%[7]. It has been stated that after 64 re-saves, there won't be any virtual change in the pixels since they have reached their local minima for error. Therefore, when applying the ELA method to a JPEG image, an important examination is to evaluate the intensity of the ELI. A low intensity result signifies that either (i) the image has been re-saved numerous times since, the more an image has been compressed, the less the error level will be between re-compressions, or (ii)the JPEG image is already in a very low quality, which is generally the case of images shared over messaging applications.

Scenario B: Let us consider the fact that in a forged image, the forged regions tend to be re-compressed fewer or more times than the remainder of the image. This reflects an error level margin for the forged regions that is different than the untouched regions of the image. In more details, considering that a region in the JPEG image has been replaced by that of another one, or has been modified,it will probably reflect a quality level that is different than the rest of the image. Therefore, by applying ELA to the modified image, regions with different qualities will be re-quantized with non-linear ratio. The obtained ELI will possess distinct values that reflects the different qualities embedded in the initial image. Few works have been reported over the ELA method.Patel and Patel [11] used ELA method to examine video frames for possible forgeries. Warif et al. [12]evaluated the performance of the ELA method with respect to various types ofimage tampering, without presenting any development to the method. The obtained results showed high reliability with JPEG compression, image splicing andimage retouching forgery. The method was unable to reveal traces of copy-move transformations. The images used for evaluation were collected from Ipad Mini 2, however the number of the images under consideration was not presented. Gunawan et al. [13]andJeronymo et al. [14]introduced post-modifications to the ELI obtained after applying the ELA method. Gunawan et al. [13]proposed to use vertical and horizontal histograms of error level image to pinpoint the exact location of modification. Experimentsover 20 images captured from two separate camera devices showed positive outcome.Jeronymo et al. [14] proposed to reduce noisy components form the ELIusing automatic wavelet soft-thresholding acting as a low-pass filter. Positive results are obtained in noise filtering while preserving necessary error levels.

III. DEVELOPMENT OF ELA

When a scene is captured by a mobile phone camera, each of the RGB channels is obtained through an image processing engine that implements the main processes: white balance,saturation enhancement, color interpolation and space conversion, color and gamma correction. The digital output is finally compressed under an image of JPEG format[15]. In order to share the images, messaging and social networkingapplications are frequently used. However, these applications do not send the original stored image. They assume that a lower-quality description of the scene can represent the purpose of the image. The shared image is generally obtained by re-compressing the original image into a lower quality copy following the JPEG compression algorithm. This enables a size reduction up to 80 %between the original and the shared image which results in a lower consumption of mobile data and a faster transmission of the file.Therefore, when assessing forgery traces in an image obtained from messaging or social networkingapplications, one must account to the fact that the quality of the questioned image has been sharply reduced. Consequently, applying the standard ELA algorithm to such type of images would fail since all regions of the image will share the same low level of error as explained in Scenario A, in the previous section. To account for such cases, we propose to calculate the error levels over the frequency domain of the image. For this purpose, let $I\ x$, represent the initial image. The image is recompressed into $I'\ x$, using the JPEG algorithm [4]under a quality Q. Then, two-dimensional discrete cosine transform (2-D DCT) is applied over every $N\times N$ pixels block, $\mathcal{B}\ x,y$, considered as data unit,of the initial and the re-compressed images.The 2-D DCT, $f\mathcal{B}\ x',y'$, is a linear, separable transform which represents thesample values as the weighting factors of sampled cosinefunctions at various frequencies as follows: $f\mathcal{B}\ x',y' = \alpha x'\alpha y'\ \mathcal{B}\ x,y \cos\ \pi\ 2x+1\ x'2N \cos\ \pi\ 2y+1\ y'2N\ a-1n=0a-1m=0$ (1)

where $0\leq x'\leq N-1$, $0\leq y'\leq N-1$, and $\alpha x'\ ,\alpha y'= 1\ N,x'=0\ ory'=0\ 2N,otherwise$ (2)

Noisy components obtained due to compression algorithms used when sharing the images are of high frequency as reported by Jeronymo et al. [14]. Therefore, neglecting high frequency components

would result in a better representation of the various error-levels in the image. As a matter of fact, when calculating the 2-D DCT over every image block, $\mathcal{B}$, the obtained result, $fB\ x','$, will have the largest value, known as DC coefficient, concentrated in its upper left corner. With increasing distance from the DC coefficient, the rest of the coefficients, known as AC coefficients, willhave smaller values. It is known that higher details of the image are represented in the AC coefficients. Since the compression noisy components are of high frequency, we discard the last, M, AC coefficients from consideration. We denote by fI and fI' the result of applying the 2D DCT over the initial and the recompressed images I and I' respectively while considering the correspondent DC and AC coefficients.The error level image is finally constituted by calculating the 2-D inverse discrete cosine transform (IDCT) of the differences in DC and AC coefficients between fI and fI':

$ELI=IDCT\ fI-fI'$ (3)

The proposed algorithm is applied to each of the three channels whenever investigating a true color RGB image.

IV. RESULTS

In order to evaluate the proposed methods, a database of convenient images has been created. For this purpose, 2500 images have been collected evenly from camera-supported mobile phones. They include the following brands: HTC, Huawei, iPhone, Lenovo, LG, Nokia, Samsung, and Sony. Several models have been considered from each brand. The images were taken from the front and the rear cameras. The images are in JPEG format with variable dimensions. The images were then exported to computers in order to apply various types of forgeries. Since it has been reported that the ELA is reliable in the detection of splicing and retouching forgeries [12], only these two types of transformations were considered. More precisely, forged images were created under any of the following scenarios:

- A forged image is created by combining two different images, or slices of two or more different images.
- A forged image is created by inserting shapes to an image like, lines, and different objects.
- A forged image is created by inserting text graphics into an image or replacing existing text in the original image..

All transformations were done using Adobe Photoshop image editing software[16]. Once the images are tampered, they were saved in JPEG format under the highest quality. The forged images were later shared over messaging and social networkingapplications that were limited to WhatsApp[17], Facebook [18], and Twitter[19]. Finally, the images were downloaded and collected from the three applications. This will ensure that the distinct image processing and compression algorithm embedded in each of the applications has been applied over the images. The total number of forged images and shared over the three applications is 10000 images. The proposed method and the original ELA method, considered as reference method, have been implemented and evaluated over the database. In order to implement our method, two parameters need to be fixed, the block size, N, and the number, M, of last AC coefficients. Since the JPEG format applies the compression algorithm by considering image blocks of dimensions 8×8 pixels, the block size parameter was chosen to be identical, N=8. As for AC coefficients, it was found empirically that discarding the last, M=9, AC coefficients was successful in minimizing high frequency components enough to have better error level images. As for the quality factor, Q, meant for recompressing the initial image, its value wasn't fixed to a unique number. Instead, it was found in the experimentations that different forgery traces were detectable under different quality factor values. For this purpose, while investigating an image, under any of the three methods, several values of quality factor, Q, were evaluated in order to examine the error level image.

Figure 1 shows samples of the obtained results. Sub-images (a), (d) and (g) of the first column have been tampered and collected after sharing over Facebook, Twitter, and WhatsApp respectively. Rectangular blackcolored shapes have been added to the images (a). Image (d) has been tampered by inserting a line at the edge of the book on the top left of the image and two lines below the table in the right bottom of the image. Image (d) has been forged by inserting a text graphic"Welcome home" and duplicated slice from the same image.Results obtained from applying the proposed method and the reference method to each tampered image are shown in the second and the third column respectively. A first observation of the results shows that the proposed method keeps the unaltered regions of the image unchanged while highlighting the tampered regions only ((b), (e), and (h)) which is not the case of the reference method. Indeed, the error level image obtained by the reference method needs serious

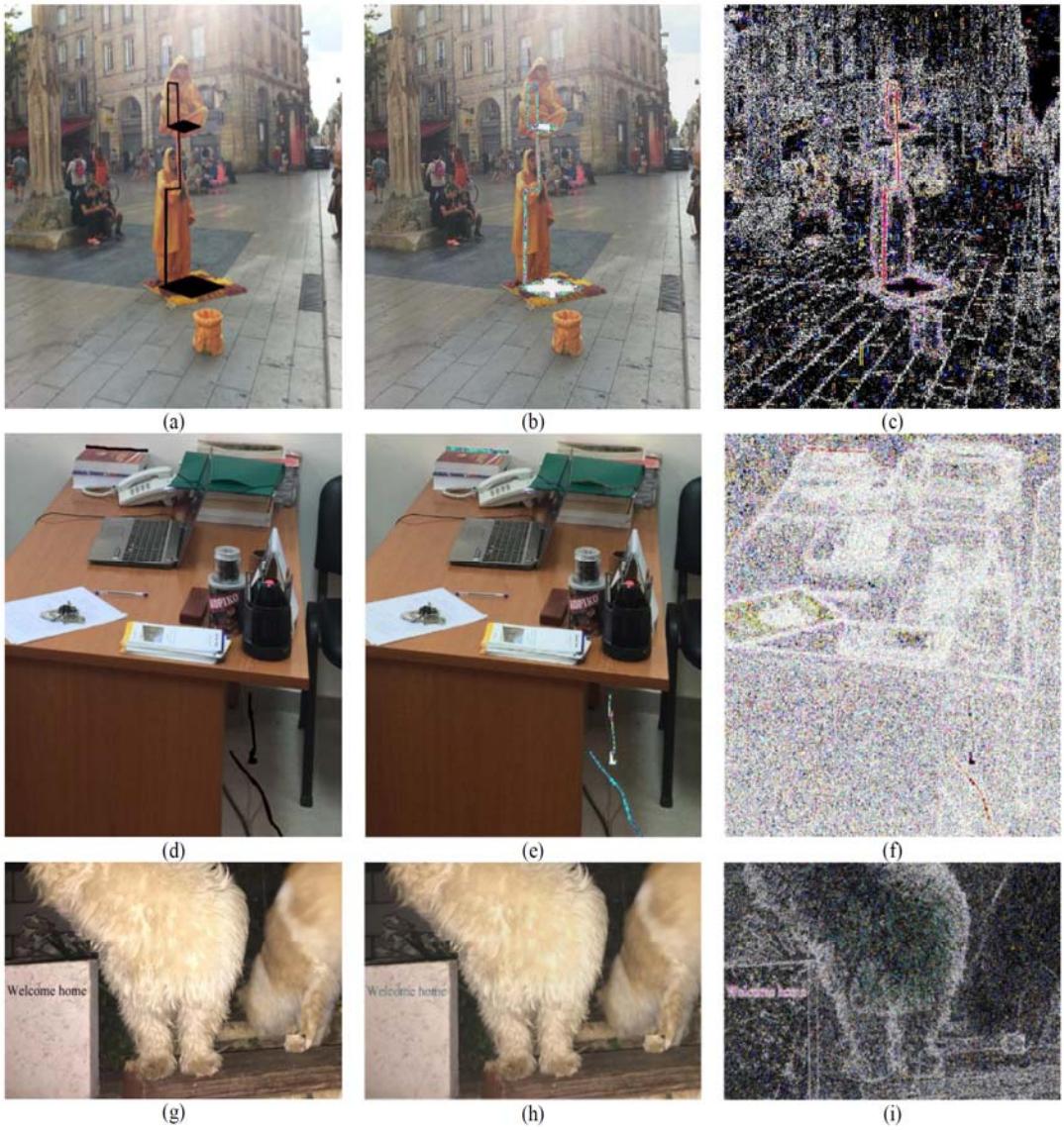

Fig. 1. Images (a), (d), and (g) shown on the first column have been tampered and shared over Facebook, Twitter, and WhatsApp respectively. Shapes in black color have been added to the images (a) and (d). Text graphics and slicing haven added to image (g). Results from applying the proposed method and the reference method to each tampered image are shown in the second and the third column respectively. Tampered regions can be easily noticed following the proposed method. They are displayed as regions with artificial colors as in (b) and (e). Results from the reference method are harder to notice especially as in sub-image (f).The images are manually cropped and contrast enhanced for display purposes.(a)(b)analysis in order to classify any region whether it has been altered or not ((c), (f), and (i)).

More specifically, results from the proposed method shown in images (b) and (e) show that the altered regions are highlighted with artificial colors. This result is less observable in image (h) that has been shared over WhatsApp and needs careful observation. In addition, the slicing transformation hasn't been detected.

On the other hand, these observations are not applicable to the results from the reference method. The error level images shown in (c), (f), and (i) are very hard to interpret. The understanding and the analysis of the images is subjective. Altered and untouched regions tend to possess similar texture, color and brightness. In addition, it would be very difficult to detect regions of image tampering.The same results are consistent over all the images of the database. The proposed method was able to easily detect modifications made by adding text graphics, shapes, and slicing from two separate images on the opposite of the reference method.

CONCLUSION

In this paper, an error level analysis method has been proposed in order to reveal transformations made to images of low quality such as those shared over messaging and social networking applications. The developed method follows a frequency-based approach,that calculates differences in DC and AC coefficients of discrete cosine transform. Obtained

results show high readability of the error level image in contrast to the reference method. Unaltered regions remain unchanged while attributing artificial colors to tampered regions in contrast to the reference method. The method is robust to low quality images and can easily detect modifications that include text graphics, shapes, and slicing from two separate images. The obtained results validate the suitability of the proposed method.

ACKNOWLEDGMENT

This work was supported by a Grant from the Lebanese University.

REFERENCES

[1] Hilal, "Image Re-Sampling Detection through a Novel Interpolation Kernel," Forensic Science International, vol. 287, pp. 25-35, 2018.
[2] Hilal and S. Chantaf, "Uncovering Copy-Move Traces using Principal Component Analysis, Discrete Cosine Transform and Gabor Filter," Analog Integrated Circuits and Signal Processing, 2018.
[3] G. K. Wallace, "The JPEG still picture compression standard," IEEE Transactions on Consumer Electronics, vol. 38, no. 1, p. 18–34, 1992.
[4] J. Miano, Compressed image file formats : JPEG, PNG, GIF, XBM, BMP, United States of America: ACM Press, 1999.
[5] "http archive," 2017-2018. [Online]. Available: http://httparchive.org/interesting.php#imageformats. [Accessed 1 4 2018].
[6] "ELA Photo Forensics," eForensics Magazine, [Online]. Available: https://eforensicsmag.com/ela-photo-forensics/. [Accessed 1 4 2018].
[7] N. Krawetz, "A picture's worth: digital image analysis and forensics," Hacker Factor Solutions, 2008.
[8] N. Krawetz, "Hacker Factor," [Online]. Available: https://www.hackerfactor.com. [Accessed 1 4 2018].
[9] N. Krawetz, "Image Error Level Analyser," [Online]. Available: http://www.errorlevelanalysis.com/. [Accessed 1 4 2018].
[10] N. Krawetz, "Foto Forensics," Hacker Factor, [Online]. Available: https://fotoforensics.com/. [Accessed 1 4 2018].
[11] H. C. Patel and M. M. Patel, "An Improvement of Forgery Video Detection Technique using Error Level Analysis," International Journal of Computer Applications, vol. 111, no. 15, pp. 26-28, 2015.
[12] 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 IEEE International Conference on System Engineering and Technology, Shah Alam, 2015.
[13] T. S. Gunawan, S. A. M. Hanafiah, M. Kartiwi, N. Ismail, N. F. Zabah and A. N. Nordin, "Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation Using Error Level Analysis," Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 1, pp. 131-137, 2017.
[14] D. C. Jeronymo, Y. C. C. Borges and L. d. S. Coelho, "Image forgery detection by semi-automatic wavelet soft-Thresholding with error level analysis," Expert Systems with Applications, vol. 85, pp. 348-356, 2017.
[15] B.-C. Huang and C.-S. Fuh, "Image Pipeline Algorithms for Standard Mobile," in Computer Vision, Graphics and Image Processing, Taipei, 2005.
[16] "Adobe photoshop," Adobe, [Online]. Available: https://www.adobe.com/products/photoshop.html. [Accessed 1 4 2018].
[17] "WhatsApp," [Online]. Available: https://www.whatsapp.com/. [Accessed 1 4 2018].
[18] "Facebook," [Online]. Available: https://www.facebook.com/. [Accessed 1 4 2018].
[19] "Twitter," [Online]. Available: https://twitter.com/. [Acces
[20] sed 1 4 2018].

★★★