A Survey on Blind Digital Photographs Forensics Based on Image Analysis

Andreja Samčović
University of Belgrade - Faculty of Transport and Traffic Engineering
Belgrade, Serbia
email: andrej@sf.bg.ac.rs

Abstract— **An increasing number of new publications in the field of multimedia forensics requires thinking about definition of terms in this new research area, as well as relationships with existing disciplines. Some image analysis methods used in forensic discipline are presented in this paper. The focus is on Principal Component Analysis, Error Level Analysis, as well as on Wavelet Transformation. Methods of digital photo forensics, picture formats and formatting, as well as some examples of different forensics tools are presented theoretically and practically on real cases.**

Keywords-multimedia, forensics, digital photos, images, JPEG.

I. Introduction

Blind multimedia forensics is a relatively new research direction in multimedia security [1]. It aims at the detection of altered media content, but does not assume any embedded security scheme. Video footage, scanned images, as well as digital and analog photographs can be the target for manipulations [2]. In this paper, we limit ourselves to digital photographs. From a forensics perspective, several changes in a photograph are widely acceptable. For instance, it is well accepted to improve the image quality, e.g., to enhance the contrast, de-noise an image, or highlight important regions. Forensics investigators search for changes in an image that create a different statement of the image. Thus, an "image forgery" is semantically defined, by considering the information communicated by the original image and the tampered image. The creation of forgeries can be motivated politically, economically, commercially, socially, or individualistically [3].

Digital cameras and video software have made it easier than ever to create high quality pictures and movies. Social Networking Sites, such as MySpace, Google Video, and Flickr make it trivial to distribute pictures, and many are picked up by the mass media. However, there is a problem: how can you tell if a video or picture is real? Is it computer generated or modified? In a world where pictures are more influential than words, being able to distinguish fact from fiction in a systematic way is essential.

Images have power. Whether it is the space shuttle exploding during launch, man walking on the moon, or soldiers raising a flag on *Iwo Jima* during World War II, refuges from Syria, powerful images have influence on the society. The advent of sophisticated digital imaging software and photo-realistic graphics allows artists to strengthen images or convey alternate meanings. Unfortunately, many altered pictures are presented as "real".

Photography lost its innocence many years ago. Only a few decades after *Niepce* created the first photograph in 1814, photographs were already being manipulated. With the advent of high-resolution digital cameras, powerful personal computers and sophisticated photo-editing software, the manipulation of photos is becoming more common. Here, we briefly provide examples of photo tampering throughout history, starting in the middle 1800s. In each case, the original photo is shown on the right and the altered photo is shown on the left.

Figure 1 represents the photograph made by famed photographer *Mathew Brady*, General *Sherman* is seen posing with his generals. General *Francis P. Blair*, shown in the far right, was inserted into this photograph.

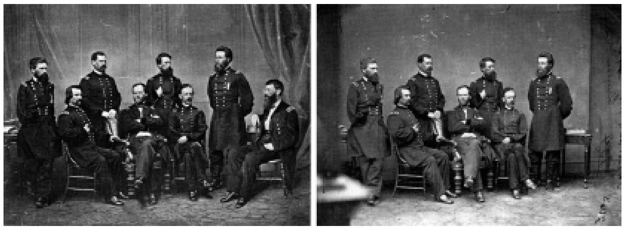

Figure 1. General *Sherman* with his generals (1865) [4]

Figure 2 presents the doctored photograph, where *Mao Tse-tung*, shown on the far right, had *Po Ku* removed from the original photograph, after *Po Ku* fell out of favor with *Mao*.

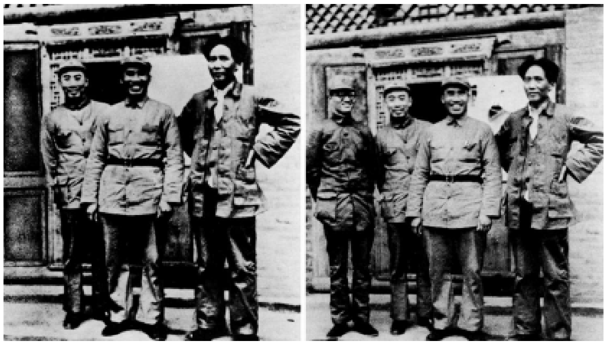

Figure 2. *Mao Tse-tung* (1936) [4]

ISBN: 978-1-61208-638-5

In the doctored photo, shown in Figure 3, of *Queen Elizabeth* and Canadian Prime Minister in Banff, Alberta, English King *George* VI was removed from the original photograph. This photo was used on an election poster for the Prime Minister. It is hypothesized that the Prime Minister had the photo altered because a photo of just him and the *Queen* painted him in a more powerful light [4].

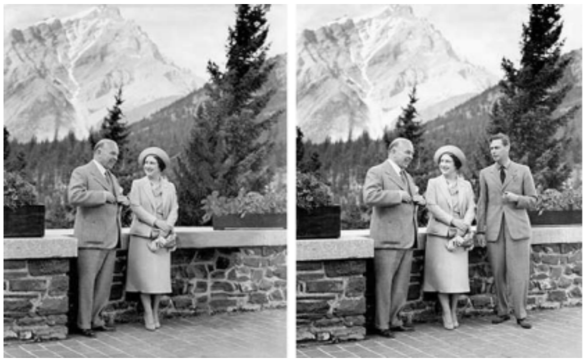

Figure 3. *Queen Elizabeth*, Canadian Prime Minister and King *George* VI (1939) [4]

The remainder of this paper is organized as follows. Section II presents the image analysis used in digital forensic discipline, such as Principal Component Analysis. Section III describes Error Level Analysis, another method for digital photographs analysis. Some examples carried out by online forensic tool are presented by using this analysis. The wavelet transformation is pointed out in the next section. Finally, we outline some directions for research in the field of digital image forensics

II. IMAGE ANALYSIS TOOLS

The following terms are used throughout this paper:

- **Computer Generated (CG)**. An image created entirely with computer software. For example, every scene from the movie *Toy Story* is computer generated image.
- **Digital photo**. A photograph from a digital camera or scanned image that has not been manipulated.
- **Digitally enhanced photo**. A digital photo that has been manipulated. This includes minor manipulations, such as cropping and red eye reduction, to major re-coloring or digitally combining with other images.
- **Photo-shopping**. Adobe Photoshop is a popular tool that can digitally enhance images. Images that have been modified using Photoshop or similar drawing tools (e.g., Gimp, Corel Draw, MS Paint) are described as being “photo-shopped” or “shopped”. The quality of the shopped image depends on both the tool and the artist. Many shopped images are obvious, while others can be very subtle.
- **Principal Component Analysis (PCA)**. An analysis approach based on data clustering.
- **Wavelet Transformations**. An analysis method based on signal decomposition.

Image format analysis can confirm metadata in accuracies and detect the last tool that modified an image [5]. However, format analysis does not evaluate the image itself. Methods, such as principal component analysis, error level analysis, and wavelet transformations permit the identification of specific image manipulations.

A. Principal Component Analysis

The *Joint Photographic Expert Group* (JPEG) image compression standard is currently the most commonly used image format for digital photographs. Most consumer cameras store the picture already in the JPEG format. The main advantages are the simplicity of the format, spatially local compression operations, and the fact that it is an open standard. JPEG compression is lossy, thus every time an image is stored in this format, content is slightly changed. This property has been the starting point for developing forensic algorithms. The information loss enables analysts to distinguish whether an image has been compressed once or multiple times with the JPEG algorithm [6]. Depending on the scenario, an answer to this question can be very useful in practice. For instance, assume that a photographer claims that an image is directly copied from his camera. Thus, the image should be single-compressed. Evidence that the image, or a part of it, is double-compressed can deliver an initial suspicion to a forensic investigator [7].

The image rendered from a JPEG file is not a perfect copy of the original image. Each time a JPEG image is resaved by a graphics editor, the image loses quality – even if the editing tool made no picture changes. This leads to a problem with quantization table analysis: if an image is saved at 75%, loaded into a drawing program, and resaved at 90%, then the quantization tables will reflect 90% while the image quality is 67.5% (90% of 75%).

Errors within a JPEG appear as blocky artifacts and color distortions. The blocky artifacts appear on the 8x8 pixel boundaries used by the JPEG algorithm. In many cases, the JPEG artifacts are too subtle for the human eye to detect. However, PCA tool can identify these JPEG artifacts.

For image analysis, PCA is used to identify the color spectrum within the image. Consider an entire image that is plotted based on the pixel colors (R, G, B) is mapped to (*x, y, z*), as presented in Figure 4. Most images have a narrow range of colors that appear as a large cluster when plotted. PC1 identifies the widest range across the color set. When two images are spliced to get her from different color sets, they usually end up forming two distinct clusters. With PCA, areas within the picture that come from different clusters will have noticeably different values [8].

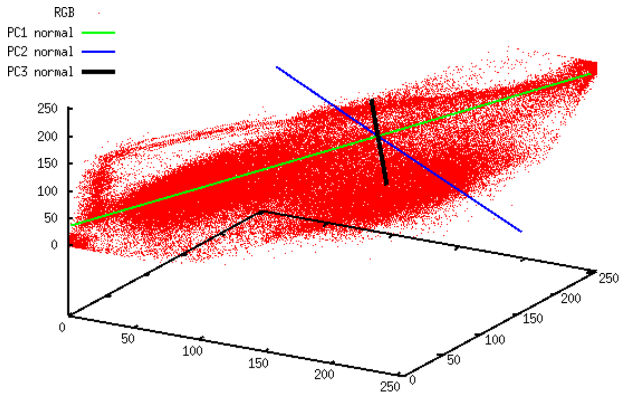

Figure 4. Sample scatter plot of an image and principal components [8]

In 2006, *Andrea Bertaccini* was awarded the "CG Choice Award" from the CG Society for the rendering of *Buzz Aldrin's* famous moon-walk, that is presented in Figure 5. According to the artist, the picture was based the original NASA photo. However, details within the picture suggest additional resources.

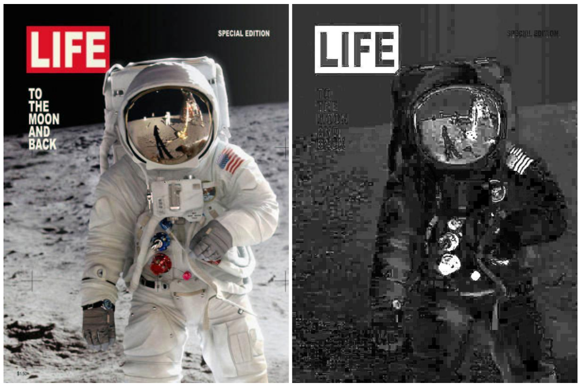

Figure 5. Image by *Andrea Bertaccini* and PC1 analysis [8]

The artist stated that the image was created using 3DSMAX and post-processed using Combustion and Photoshop tool. The quantization matrix matches Photoshop's "high (8)" quality, equivalent to a JPEG saved at 89%. However, using the PC1 line shows a significant number of artifacts that resemble a quality around 40%. This suggests that the image was saved multiple times.

III. Error Level Analysis

JPEG is a lossy format, but the amount of error introduced by each resave is not linear. A 90% image resaved at 90% is equivalent to a one-time save of 81%. Similarly, saving an image at 75% and then resaving it at 90% (75% to 90%) will generate virtually the same image as 90% to 75%, or saved once at 67.5%. The amount of error is limited to the 8x8 cells used by the JPEG algorithm; after roughly 64 resaves, there is virtually no change. However, when an image is modified, the 8x8 cells containing the modifications are no longer at the same error level as the rest of the unmodified image [8].

Error Level Analysis (ELA) works by intentionally resaving the image at known error rate, such as 95%, and then computing the difference between the images. If there is virtually no change, then the cell has reached its local minima for error at that quality level. However, if there is a large amount of change, then the pixels are not at their local minima and are effectively "original". Figure 6 presents an example of picture manipulation that is used in advertising for "*Old Spice*" company.

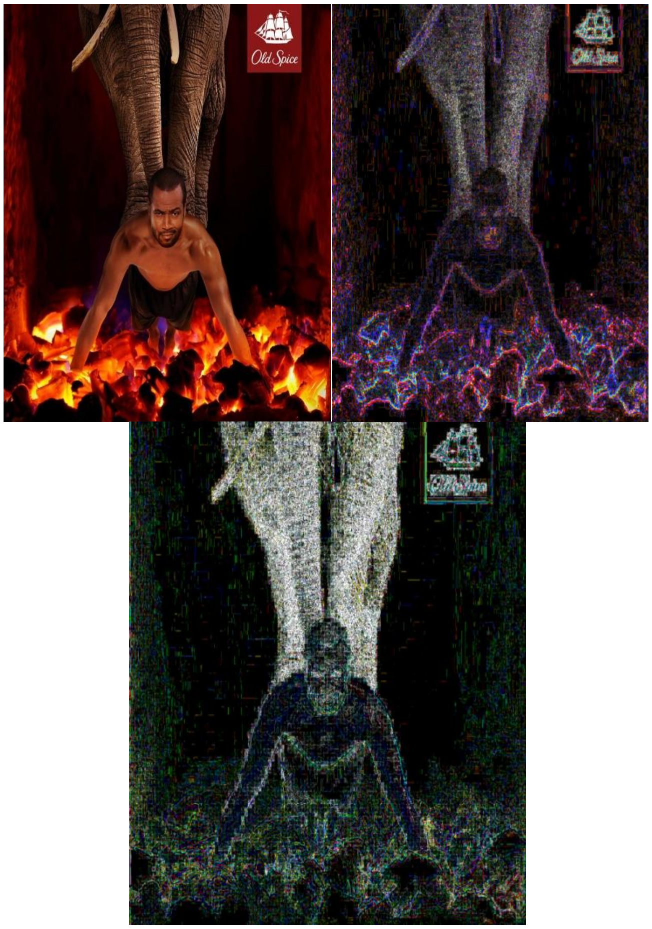

Figure 6. "*Old Spice*" commercial (upper left), 88% of JPEG quality (upper right) and Noise Analysis (lower, online tool "Forensically")

We used Error Level Analysis by online forensic tool "Forensically" and our analysis confirmed that the picture is computer generated and presents a composition of four parts: logo of "*Old Spice*", actor *Isaiah Mustafa*, an elephant and ingle.

IV. WAVELET TRANSFORMATION

While ELA is useful for identifying recent changes relative to the number of resaves, resaving a picture many times or using a very low quality JPEG can obscure ELA results. However, changes to pictures can still be identified through the use of wavelet transformations.

Wavelets are used for signal decomposition. A single wavelet is a known and well-defined signal. This signal can be scaled and added in order to create more complex signals. Any real signal can be decomposed into a set of wavelets that, when combined, approximate the signal.

Although wavelets can approximate any signal, some signal types are more difficult to approximate. Square waves, or areas with sharp color changes, are difficult to approximate. Although the flat area of the square wave can be approximated quickly, the sharp corners may require many wavelets to properly fit the signal. Similarly, linear transitions are approximated by a series of stepped square waves. In addition, extreme values (black and white) are difficult to approximate. In contrast, wavelets are very good at approximating "natural" colors and noisy images, such as those generated by digital cameras.

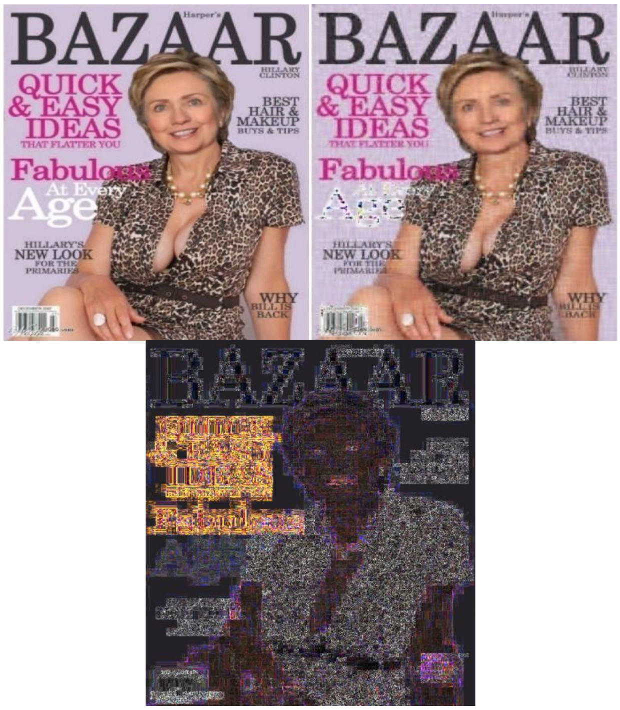

Figure 7. Photo-shoped image with *Hillary Clinton*, resolved with 5% of wavelets and ELA

In the case of digital photos, the picture is the signal and wavelets approximate the image. Rendering an 800x600 pixel image requires up to 480,000 wavelets per color channel to perfectly recreate the picture. However, if only a small percentage of the wavelets are used, then the main attributes of the picture become visible, even if they are blurry. As more wavelets are included in the rendering, the image sharpens. And even more wavelets fine - tune the sharpened colors.

This property of wavelets – from blurry to sharp to correct colors – can be used to identify image manipulations [9]. In particular, the entire image should sharpen at the same rate. If the picture components are scaled or merged from different focal lengths, then the components will sharpen at different rates [8].

The left image from Figure 7 was created by "redcard" as part of an image manipulation contest. Rendering the image with 5% of the available wavelets shows a crisp torso and near-crisp arms and legs. However, the face remains fuzzy. The fuzziness ends just below the chin. The wavelet analysis suggests that the head is from a picture of *Hillary Clinton*, the neck and torso comes from a second source, and the arms and legs may be from a third source.

V. CONCLUSION

Digital photography almost completely replaced analogue pictures. As there are many techniques for counterfeiting digital photography, several tools for multimedia forensics have considered. In image forensics, researchers aim to provide computational tools to support human experts in deciding about the authenticity of an image. The process of detecting image manipulation can be complex, thus there is need for the concentration on the precious details in the picture. The same tool is iteratively applied to observe discrepancies between image regions, as a good forensics tool.

ACKNOWLEDGMENT

This work was partially supported by the Ministry of the Science, Education and Technological Development of the Republic of Serbia (projects TR 32025 and 32048).

REFERENCES

[1] S. Lian, D. Kanellopoulos, and G. Ruffo, ”Recent advances in multimedia information security”, Informatica, vol. 33, pp. 3-24, 2009.

[2] R. Bohme, F.C. Freiling, T. Gloe, and M. Kirchner, ”Multimedia forensics is not computer forensics”, Proceedings 3rd International Workshop on Computational Forensics (IWCF 2009), The Hague, Netherlands, pp. 1-14, 13-14 August 2009.

[3] A. Samčović, ”Recent advances in digital image forensics”, XXXII Simposium on new technologies in postal and telecommunications traffic (PosTel 2014), Belgrade, Serbia, pp. 299-308, 2-3 December 2014.

[4] H. Farid, ”A survey of image forgery detection”, IEEE Signal Processing Magazine, vol. 26, No. 2, pp. 16-25, 2009.

[5] W. Ku, „Exploiting ”The world is flat” syndrome in digital photo collections for contextual metadata”, Proceedings 8th International Symposium on Multimedia (ISM 2006), pp. 1-7, 2006.

[6] Y.Q. Zhao, F.Y. Shih, and Y.Q. Shi, ”Passive detection of paint-doctored JPEG images”, Proceedings IWDW 2010, Lecture Notes on Computer Science 6526, pp. 1-11, 2011.

[7] A. Samčović, ”Review of multimedia passive forensic techniques for image forgery detection”, VI Conference on Business Information Security (BISEC 2014), Belgrade, Serbia, pp. 54-60, 18 June 2014.

[8] N. Krawetz, ”A picture's worth...digital image analysis and forensics”, Texas, United States, Hacker Factory Solutions, pp. 11-16; 52-64, 2007.

[9] Y.J. Ming, ”A method of the hiding fingerprint image data based on wavelet coefficients redundancy”, Proceedings 3rd International Conference on Computer Science and Information Technology (ICCSIT 2010), Chengdu, China, pp. 441-444, 9-11 July 2010.