Chapter 21

FORENSIC ANALYSIS OF DIGITAL IMAGE TAMPERING

Gilbert Peterson

Abstract The use of digital photography has increased over the past few years, a trend which opens the door for new and creative ways to forge images. The manipulation of images through forgery influences the perception an observer has of the depicted scene, potentially resulting in ill consequences if created with malicious intentions. This poses a need to verify the authenticity of images originating from unknown sources in absence of any prior digital watermarking or authentication technique. This research explores the ability to detect image forgeries created using multiple image sources and specialized methods tailored to the popular JPEG image format. Four methods are presented for detection of image tampering based on fundamental image attributes common to any forgery. These include discrepancies in (i) lighting levels, (ii) brightness levels, (iii) underlying edge inconsistencies, and (iv) anomalies in JPEG compression blocks. These methods detected image forgeries with an observed accuracy of 60% in a completely blind experiment containing a mixture of 15 authentic and forged images.

Keywords: Image forgery, image forensics, image authentication

1. Introduction

Digital technologies allow for manipulation in photographic development; thereby making it necessary to verify the authenticity of a digital image. As digital cameras become more prevalent and accepted at an evidentiary level, an individual's conviction may depend on the authenticity of a digitalimage. The traditional technique for declaring image propriety and subsequently authentication applies a visible or invisible watermark [3] immediately after capture. Checking the presence of the watermark on the image verifies its authenticity. This procedure requires the image originate from a known and authenticating source.

This paper presents four techniques for detecting tampering in JPEG compressed images given images from unknown sources. These techniques consider the color and brightness of individual pixels as well as the JPEG image format. These techniques are then applied in a blind test on a set of 15 images consisting of real and expert forged images.

2. Related Work

This section discusses the JPEG digital image format and existing research in image forgery detection. To assist in this discussion forged image detection is separated into two classes, copy-move and copy-create. The reason for distinguishing classes of image forgeries is because some image processing techniques are better suited to a specific class.

2.1 JPEG Image Format

Digital image compression and storage fall into two categories, lossless and lossy. In lossless compression, techniques like GIF, TIFF and PNG, the image quality is maintained resulting in the uncompressed image being identical to the pre-compressed image. For lossy compression techniques like JPEG, the quality of the image is sacrificed for a smaller storage size.

Lossy JPEG compression exploits the fact that the human eye is less sensitive to higher frequency information (e.g., edges and noise) in an image than to lower frequencies. The jpeg encoding process [13], Figure 1, starts by breaking the raw image into blocks, usually sized to 8×8 pixels. A total of 64 Discrete Cosine Transform (DCT) coefficients are computed for each block, converting the block from the spatial domain to the frequency domain. The higher frequency DCT coefficients are then rounded off according to the values of the quantization matrix, which determines the tradeoff balance between image quality and compression ratio, also termed the quality factor. The matrix of quantized DCT coefficients is then encoded into a binary stream with lossless Huffman compression. An image is extracted from a jpeg file by reversing this process.

2.2 Copy-Move Forgery Detection

The first class of image forgeries includes images tampered by means of copying one area within an image and pasting it onto another, copy-move forgeries. Figure 2 illustrates an example in which copied parts of the foliage cover and mask the truck to completely hide it.

Existing methods developed to detect this type of forgery build on the intuitive suggestion of performing an exhaustive comparison search.

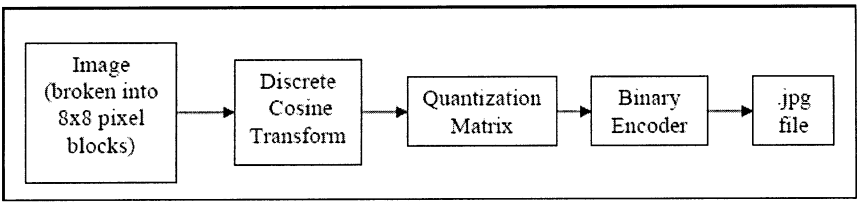

Figure 1. JPEG compression process.

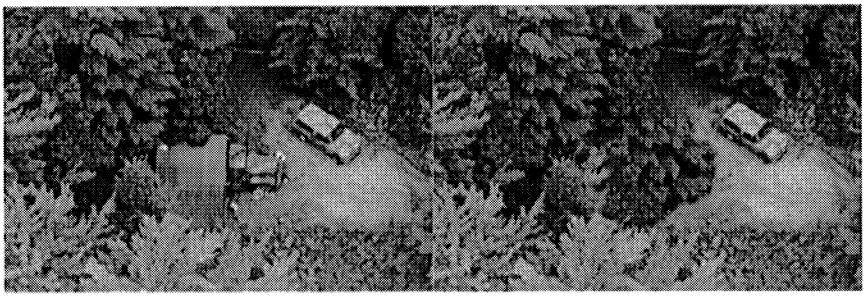

Figure 2. Example of copy-move image forgery [6].

Fridrich, *et al.* [6] overlay each circularly shifted position of the grayscale converted image, comparing it with the original to yield the areas copied and pasted. An improvement on the computational complexity is a block matching variation using a B×B block of pixels, which represents the minimal size considered for a match. This technique reduces the computational complexity of the technique and also dictates the desired accuracy of the image in question.

The application of block matching to lossy JPEG images makes use of blocks matched based on their representation consisting of quantized DCT coefficients. In this method, the same technique is used which creates a matrix from B×B blocks. The difference being the storage of computed DCT coefficients instead of pixel values [6].

2.3 Copy-Create Forgery Detection

The second class of forged images deals with creating the forgery by taking one or more images and copying and pasting from various areas within each to form a forged image. The image processing community refers to this as an image "composition," which is defined as the "digitally manipulated combination of at least two source images to produce an integrated result" [2]. The name for these types of images, in context

of this article, is copy-create forgeries. Figure 3 shows how the three images at the bottom can be merged into a single image.

Two methods currently exist for detecting copy-create forgeries, edge detection algorithms and spectral analysis. Edge detection techniques attempt to detect double or "ghost" edges around objects in the environment caused by the blurring of space around the tampered objects [8]. Alternatively, spectral analysis approaches utilize Discrete Fourier Transforms (DFTs) and their ability to detect brightness and intensity levels of an image to detect variations caused by resampling [5, 8].

Figure 3. Example of image forgery created from several sources [6].

An edge is an area in the image where the intensity of pixels moves from a low value to a high value or vice versa [9]. Edge detection in images is conducted by convolving first-order operators with the image in order to locate areas that are discontinuous. Previous masks used in analyzing images were the Roberts, Sobel and Prewitt masks [8].

Forged images that are the result of merging two or more host images together usually requires that at least one image be cropped, resized, or rescaled. This manipulation leads to underlying changes in the statistical nature of the image, which spectral analysis captures. By calculating the discrete Fourier transform (DFT) of suspected areas of manipulation in the image, the analyst looks for a periodic pattern and local maximums suggesting that an area has been re-sampled [8].

Farid and Popescu [5] extend the spectral analysis approach by calculating a high-pass filtered "probability map" of the forgery, and then filtering the image to gain high detection accuracy. The probability map is calculated as a correlation between pixel neighbors estimated against several periodic samples, thereby removing the low frequency noise from the image which may return false positives. In the forgery detection algorithm, areas of this probability map are blocked off and used for comparison. One blocked area should encompass the suspected tampered portion and a second blocked area should cover an assumed authentic region [5].

Spectral analysis has been shown to work best on uncompressed or losslessly compressed images and requires the analyst to already anticipate where in the image the forgery exists. Images saved in the lossy JPEG format with quality factors less than 97 exhibit much lower detection accuracy, becoming a hit or miss occurrence [5]. It should be noted that most JPEG images are generally set to a quality factor of approximately 80/100 for optimal high quality, with medium to low quality images using much lower quality factors.

3. Analyzing JPEG Images

A person's expectation of an image is sometimes the best detection method in determining if an image is forged. As, the human eye usually picks up on copy-create forgeries because this type of forgery consists of several images, each of which may have different lighting, color patterns, quality, or shadows.

The first two techniques attempt to assist the analyst's eye by augmenting these differences, targeting the luminance and HSV values of the images. The third technique builds on the ideas behind convolution masks augmenting the double edge present in copy-create forgeries. The final technique examines the compression of the different JPEG compression blocks, searching for variations on the assumption that in a copy-create image the source images may have different quality factors.

3.1 Luminance Levels

The luminance of an image is the measurement of the perceived brightness levels [11]. Intuitively, if two images are taken from different cameras with different lighting, some sort of discrepancy may occur in those areas which were copied and pasted. In particular, analyzing a forged image looks for areas that are approximately the same distance away from the lens but have different luminance levels. This analysis is heavily dependant on the skill level of the person creating the forgery and

the resources available to perform the manipulation. Newer versions of image processing software make it easy for even a novice user to create forgeries based on automated "auto-brightness" adjustments.

The luminance level detector converts a color image to grayscale and then to binary by setting pixels 'on' if they exceed a user set luminance threshold and 'off' otherwise. The luminance threshold is a value between 0.0 and 1.0. To determine an appropriate threshold a value of approximately 0.50 is a good starting point with subsequent tests performed in both directions. One could also choose to use Otsu's method for finding greyscale thresholding values which minimizes the intraclass variance between black and white pixels [10]. The ultimate goal is to look for results depicting an area of suspected tampering, which are witnessed by unnatural or abnormal luminance levels in an area. Figure 5 shows the luminance results of Figure 4 based on a luminance threshold of 0.60, and revealing an abnormal pattern in the tampered area.

Figure 4. Tampered Lena Image.

3.2 Hue-Saturation-Value (HSV)

The hue of a color is described as the "tint," saturation or "shade" is the level of purity or intensity of a color; the value is the level of brightness or how light or dark it is [11]. As with luminance, if an area of an image is copied and pasted from a different source, the color and brightness, as captured from each respective image, may be different.

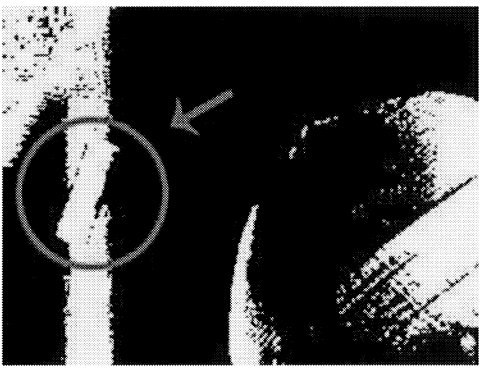

Figure 5. Result of luminance level test on forged Lena image.

Thorough analysis of a color image converted to HSV levels [12] helps determine this.

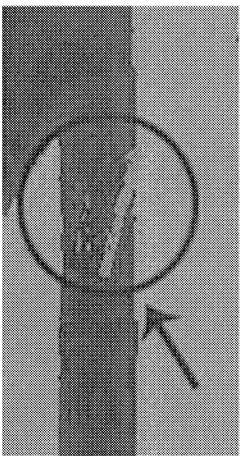

Figure 6. Result of converting forged Lena image into HSV color-space.

Figure 6 shows the results of a HSV color-space test performed on Figure 4. Again, the magnified area in this figure illustrates the tampered portion by showing an uneven color pattern and shape compared with the surrounding area. The abnormal color "bleeding" also indicates some form of tampering has occurred.

3.3 Alternative Filtering Mask

Several convolution filtering methods were analyzed by Lukas [8], including the Roberts, Sobel, Prewitt and Marr masks. These methods

have been limited in their detection of image forgeries due to their targeting of specific types of edges. Since what is of interest in forgery detection is not in detecting edges but in image discrepancies such as double edges, a custom convolution mask is created which places emphasis on a particular image's distinct contrasts. The created mask uses a 3×3 block size which is the best size for capturing the trends in an image without introducing too much pixel variation.

$$\begin{bmatrix} -1 & -2 & -1 \\ -2 & 12 & -2 \\ -1 & -2 & -1 \end{bmatrix}$$

The weight of 12 is placed on the center pixel along with all other neighbors' weights summing to -12. This filters out all areas in an image that are similar and magnifies those that vary greatly. These varying areas arise from prominent edges, and locations victim to image tampering. The analyst then looks for portions within the image that are noisy or contain "hidden" and "ghost" edges. Figure 7 shows this filtering method on Figure 4. In this example, the magnified portion shows the tampered area which exhibits a distinctive abnormal pattern in comparison with the surrounding area.

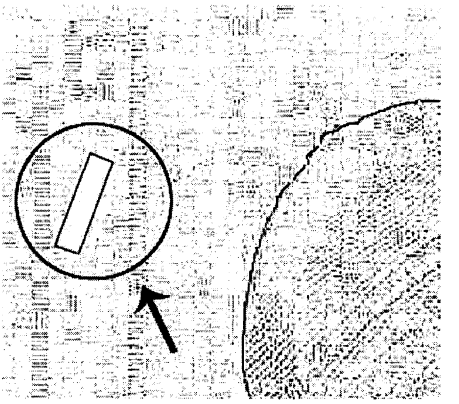

Figure 7. Inverted result of performing custom filter mask on forged Lena image.

3.4 JPEG Compression Forgery Detection

During the JPEG compression process (Figure 1), the image is broken into disjoint 8×8 blocks. These blocks then form a "fingerprint" of the image. When creating a copy-create forgery, it is composed of several pieces of other images which are cropped, scaled, and rotated to make the forged image's authenticity more believable. These pieces may have

originated from images that have previously been JPEG compressed with differing quality factors (QF).

This technique analyzes a JPEG image with respect to the 8×8 blocks used by the JPEG compression scheme and detects these QF differences. Performing a calculation on the boundaries of these blocks builds upon the technique presented by Fan and Queiroz [4] for detecting prior JPEG compression in a BMP image. Figure 8 shows an abstract representation of an 8×8 block of pixels in a JPEG image with letters representing interested pixel values.

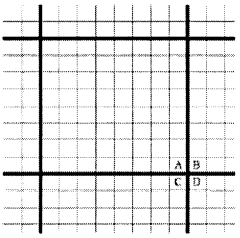

Figure 8. Abstract representation of an 8×8 block used by JPEG compression.

The calculation of $R(i,j) = |A - B - C + D|$ for each 8×8 block intersection, Figure 8, represents the degree of pixel variation present between the 8×8 block and its 3 neighbors. Variations in the block differences between image area are the result of differences in the compression levels across the image. To verify a suspected image of forgery, all $R(i,j)$ values are calculated for each block. Each block is then white if $(|R(i,j) - R(i,j+1)| > t) \vee (|R(i,j) - R(i+1,j)| > t)$ where t is a user definable threshold. This compares the intersection difference between the intersection to the right and to the bottom with black blocks indicating a large variation in the compression levels between intersections.

Figure 9 illustrates the proposed JPEG Block Technique using a threshold of 15. The result of the block analysis technique has uncovered a definitive pattern in the differing compression levels of the image. This is a good example of how the naked eye is fooled by the authenticity of a forged image, but the "fingerprint" of the JPEG compression scheme leaves pixel level differences.

The determination of the proper threshold starts with a value equal to 50. The result should then be analyzed with further testing using threshold values in increments/decrements of 5 or 10. Each test should look for distinctive patterns in the binary image or focus on areas suspected of tampering. As the threshold value decreases, the black pixels center on areas of image tampering. This is because high levels of JPEG block variability are usually seen in areas with prominent edges or that

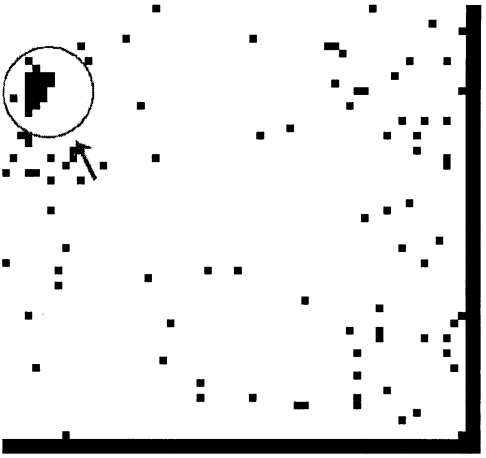

Figure 9. Result of performing JPEG block test on forged Lena image.

have been digitally tampered. The alternative occurs when the threshold is raised, the white pixels center on the tampered area which was pasted from a higher quality factor image.

4. Results

In order to obtain objectivity in testing the methods, the techniques are tested on a set of 15 images consisting of real and expert forged images where no information is provided about the authenticity of the images. For this test, each of the methods is applied to an image, for the luminance and JPEG compression forgery detection methods, the thresholds are adjusted in the effort of verifying a forged area. An image is declared a forgery if one of the techniques definitively demonstrates that there is an anomaly present.

Overall, 6 of the 15 test images were found to be incorrectly identified. This included 2 identified as false positive and 4 as false negatives. Therefore, an overall observed accuracy of this experiment is 60% with a 13.33% false positive result and 26.67% false negative result. It is interesting to note that the two images that were false positives were both trick camera shots, one failed the luminance and HSV tests was a night photograph with a very slow shutter speed. The other failed the JPEG compression detection was a photograph taken with a fisheye lens.

The results of this experiment raise some important points about performing the proposed methods to detect image tampering. When performing each technique on an image of unknown origin, some subjective analysis is required of each method's result. In the case of JPEG images

with low quality factors, one has to determine if a flagged area is due to actual image tampering or if high compression introduced the distortion, as can be the case with many images found on the web. Also, it is preferable to get a second opinion of each result to aid in the decision making process. This experiment overall proved to be interesting and found a respectable accuracy percentage compared to declaring authenticity without the help of any detection methods.

5. Conclusions

The detection of image tampering relies on one assumption, that the tampering performed by a forger introduces some detectable anomaly. This can be some inconsistent color or brightness pattern, abnormal edge, or other by-product of image tampering.

The four techniques presented in this paper extend image authentication to provide verification methods for the previously uninvestigated area of copy-create image forgeries in the lossy JPEG compression format. The JPEG compression detection method makes use of the JPEG "fingerprint" to determine if an image is a forgery. Subsequently, the other three methods developed work on any digital image due to their specialization in fundamental attributes of any digital image.

Testing these four methods in a blind experiment of 15 authentic and expert forged JPEG images revealed a detection accuracy of 60%. Detection accuracy was found to be heavily dependent on the amount of time spent analyzing the results of each method as well as any preexisting tampering knowledge of the image in question.

During the testing and development for this research no one technique was found to be best at detecting every image forgery and enforces the idea that a multilayered approach is required for image authentication. Additionally, the ability to detect a forgery is tied to the amount of creativity and effort of the forger given there are an infinite number of possibilities to create, alter, and digitally manipulate any given image. Some of the methods a forger could employ to avoid detection are to manipulate the luminance and HSV levels to match the remainder of the image, and perform the manipulation on a larger lossless image that is then compressed on completion.

6. Acknowledgements

This work paper was supported by the Digital Data Embedding Technologies group of the Air Force Research Laboratory, Information Directorate. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright no-

tation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Air Force Research Laboratory, or the U.S. Government.

References

[1] Associated Press, Britain says soldier held in photo probe, *Newsday*, May 18, 2004.

[2] R. Brinkmann, *The Art and Science of Digital Compositing*, Academic Press, San Diego, California, 1999.

[3] R. Chandramouli, R. Memon and M. Rabbani, Digital watermarking, in *Encyclopedia of Imaging Science and Technology*, J. Hornak (Ed.), John Wiley, New York, 2001.

[4] Z. Fan and R.L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, *IEEE Transactions on Image Processing*, vol. 12(2), pp. 230-235, 2003.

[5] H. Farid and A. Popescu, Exposing digital forgeries by detecting traces of resampling, *Proceedings of the IEEE Transactions on Signal Processing*, 2004.

[6] J. Fridrich, J. Lucas and D. Soukal, Detection of copy-move forgery in digital images, *Proceedings of the Digital Forensics Research Workshop*, 2003.

[7] K. Guggenheim, New prison abuse photos outrage lawmakers, *Phillyburbs*, May 13, 2004.

[8] J. Lukas, Digital image authentication using image filtering techniques, *Proceedings of the Fifteenth Conference of Scientific Computing*, 2000.

[9] C.M. Luong, *Introduction to Computer Vision and Image Processing*, Department of Pattern Recognition and Knowledge Engineering, Institute of Information Technology, Hanoi, Vietnam, 2004.

[10] N. Otus, A threshold selection method from gray-level histograms, *IEEE Transactions on Systems, Man and Cybernetics*, vol. 9(1), pp. 62-66, 1979.

[11] J. Sachs, *Digital Image Basics*, Digital Light & Color, Cambridge, Massachusetts, 1999.

[12] A. Smith and E. Lyons, HWB – A more intuitive hue-based color model, *Journal of Graphics Tools*, vol. 1(1), pp. 3-17, 1996.

[13] Society for Imaging Science and Technology, Jpeg tutorial (www.imaging.org/resources/jpegtutorial/index.cfm).