DIGITAL IMAGE MANIPULATION DETECTION ON FACEBOOK IMAGES

By

CHARINA G. MARRION

B.S., University of Alabama at Birmingham, 2001

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Recording Arts

2016

This thesis for the Master of Science

degree by

Charina G. Marrion

has been approved for the

Recording Arts Program

by

Catalin Grigoras, Chair

Jeffrey Smith

Marc Rogers

Date: April, 2016

Marrion, Charina (M.S., Recording Arts)

Digital Image Manipulation Detection on Facebook Images

Thesis directed by Professor Catalin Grigoras

ABSTRACT

One of the most popular social media sites being used by multiple generations from Baby Boomer to Generation Z, is Facebook. Facebook was founded in 2004 by Mark Zuckerberg, who was attending Harvard University at the time. While the site was initially designed to serve as a social media outlet for college attendees, the utility of it quickly spread to the common public, where it became a means of connectivity for individuals, regardless of locale. Today, Facebook has connected families and friends separated by varying degrees of distance in the past with about 250 billion photos uploaded by its users, averaging around 350 million uploads per day. With having to host this significant amount of photo images, Facebook compresses uploaded images in order to reduce the file size, as well as saving on storage [10]. The downside to the compression is that it leaves images, specifically JPEG (Joint Photographic Experts Group) images, with poor quality and creates compression artifacts which are noticeable distortions on the images [12]. JPEG or Joint Photographic Experts Group, are images that have a lossy compression algorithm which means the image compression rate can be adjusted to size and image quality. Since JPEG images are adjustable, they are also susceptible to alterations and manipulations. To investigate whether a JPEG image has been altered or manipulated, effects of the DCT or Discrete Cosine Transform on pixels and ELA or Error Level Analysis can be used to analyze the

image. This paper will investigate a combination of images that has been altered through Photoshop as well as Photoshop images compressed by Facebook. Since Facebook compresses JPEG images at a high rate, the question is whether the manipulation can be visually detected or not through DCT or ELA. Working with both analyses, the results should illustrate which method results in better quality and easy detection. DCT map provides better visibility than ELA where an object was removed in an image. Although after using Facebook, the results of the tampered area on the image cannot be detected using DCT map.

The form and content of this abstract are approved. I recommend its publication.

Approved: Catalin Grigoras

ACKNOWLEDGEMENTS

I'd like to thank my husband, Kevin, my daughters, Marley, Reese, and Avery, and my parents for their support and patience throughout the pursuit of my Master of Science degree. I'd also like to thank my friends who helped with the production of this research. Last but not least, thank you to Professor Catalin Grigoras for his patience and positive support.

TABLE OF CONTENTS

CHAPTER

LIST OF FIGURES

FIGURE

LIST OF TABLES

TABLE

CHAPTER I

INTRODUCTION

Over the last few of decades, digital media has dominated households all across the world. From Digital Video Discs or DVD's to digital televisions and digital cameras, people have adapted to a seemingly more convenient digital world. Digital cameras are similar to film cameras as they share the same optical system. Most cameras sold today are digital, perhaps the consumer favors digital over film for the convenience of displaying images immediately after being taken [4]. In addition, digital cameras are also capable of storing hundreds to thousands of images in a memory card rather than having to store hundreds and thousands of hard copies. With this type of technology, it is not surprising that illegal activities have increased significantly using digital media. On the other hand, law enforcement has also used digital media to their advantage. Not only have digital images help law enforcement solve crime, digital images have also helped prosecute all types of crime [5]. Multimedia forensics, also known as media forensics or digital forensics is a branch of digital evidence as a forensic science discipline which deals with the recovery and investigation of digitally recorded evidence. This paper will refer to the discipline as Media Forensics. Media forensics is the analysis of video, audio and image evidence. The concept of media forensics is derived from research, tested on known data, and applied within a methodological framework. The fundamental principle for forensic media analysis is to maintain the integrity and provenance of media upon seizure and throughout processing. Media manipulation is the application of different editing techniques to create an illusion or deception [2]. This paper will explore the challenges surrounding image authenticity

and detection of manipulation on digital images. The challenges will include examining Facebook compression on images as well as applying Adobe Photoshop editing tools and using varying compression rates on edited images. The experiment will include deleting objects from an original image in a manner where the edited image appears to be original. The question is whether image editing can be detected using several different forensic processes. The hypothesis is that if JPEG compression causes losing data in an image, then the tampered area in the image should also disappear due to lost data.

CHAPTER II

TECHNICAL OVERVIEW

The Scientific Working Group on Digital Evidence, also known as SWGDE, is an organization that was formed in 1998, that consists of members from law enforcement, academic and commercial organizations. These members collaborate in creating standards and guidelines for digital evidence. SWGDE's goal is to allow communications between law enforcement agencies and forensic laboratories around the world and to provide guidance on new technologies and techniques. During the first SWGDE meeting in July 1998, the group defined digital images as any information stored or transmitted in binary form, which is later renamed as digital form. In 2003, SWGDE published guidelines for training and best practices which resulting in approving digital evidence as part of the accreditation process for crime laboratories through the American Society of Crime Laboratory Directors, also known as ASCLD. The labs include computer forensics/mobile phone, audio, video, and image. The SWGDE organization currently holds about fifty members. Although SWGDE does not accredit laboratories or individuals, the group publishes best practices and standards for quality assurance [14].

SWGDE published the Image Processing Guidelines in February 2016. The objective of the article is to give guidance in assuring the proper use of image processing and the production of quality of a forensic image for the legal system. Since image processing has been historically used in the legal system, many of the processes with analog or non-digital images are similar with digital image processing. According to SWGDE, any changes made through forensic image processing must meet specific

criteria. These criteria include that the original image is preserved and any changes should be made on the working copy; processing steps are documented in detail that another trained examiner can easily follow the steps; the result is the processed image; and that the recommendations of the document is followed. There are three categories in SWGDE Image Processing Guidelines and they are image enhancement, image restoration, and image compression. Image enhancement is the process used to improve the quality of an image. Tools used in image enhancement are Brightness adjustment, Contrast adjustment, Cropping, Dodging and Burning, Color processing, High Dynamic Range or HDR, linear filtering, non-linear contrast adjustments, pattern noise reduction, and random noise reduction. Image restoration techniques include Blur removal, Graycale linearization, Color balancing, Warping, and Geometric restoration. Lastly, image compression techniques include Lossless compression and Lossy compression [20].

Joint Photographic Experts Group or JPEG is the most common file format used by digital cameras. JPEG was established in 1992 from a committee who wanted to standardize still pictures. JPEG is a lossy compression for digital images that has an algorithm based on an eight by eight pixel grid. Lossy compression refers to the adjustable characteristic of an image which can also discard some data. Lossy compressions can be adjusted to an image's storage size and its image quality whereas lossless compression retains all its original data. Common filename extensions for JPEG images are .jpg, .jpeg, .jpe, .jif, .jfif, and .jfi. JPEG File Interchange Format or JFIF is a file format standard that allows exchanging formats with JPEG files and uses the same compression techniques as the JPEG standard, therefore, it is likely to see JFIF referred

to as “JPEG/JFIF.” JPEG is the most common format used when saving digital images [14]. It’s no surprise that most images that are uploaded to social media use JPEG. Facebook, in particular, hosts over two hundred fifty billion photos in its site. Facebook allows their users to upload photos on their site free of charge although Facebook still pays for storing these photos. In order to make room for all these images worldwide, Facebook utilizes image compression to reduce their costs. For example, an image with a file size of five hundred kilobyte could be compressed to only one hundred kilobytes or less through Facebook. When a digital image is compressed through Facebook, it creates visible artifacts [10]. Artifacts are visible distortion of an image caused by lossy compression. JPEG compression is established on the discrete cosine transform [12].

The Discrete Cosine Transform, or DCT, is an algorithm using lossy compression specifically with JPEG images. DCT converts an image from spatial domain into frequency domain where it encodes a set of sixty-four signal based amplitudes called DCT coefficient. DCT coefficient has two signals, DC and AC components. There are sixty-four elements or coefficients in an eight by eight block. The first block which is located at the upper left corner of the block is the DC coefficient, the remainder sixty-three blocks are the AC coefficients [11]. The DC component is the average color of the eight by eight region while the AC component represents color change across the block. This is an example of what an eight by eight region of pixel looks like in Figure 1 [1].

Figure 1. 8x8 region of pixel

Every time a JPEG image is recompressed, the DCT coefficient modification is irreversible and undergoes a characteristic called double quantization or double quantization effect. These quantization effects are noticeable depending on how much or how little compression was applied. Image manipulation can be analyzed when an image is loaded and saved through a photo editing program due to the presence of image compression in DCT coefficient [19]. This paper will discuss the results of analyzing images using the DCT map technique which is also based on DCT coefficients [9].

The Error Level Analysis or ELA is another technique that may help in detecting manipulated images. ELA identifies different compression levels within an entire image. For instance, an original JPEG image should have consistent edges, textures, and surfaces as well as the same compression level throughout the image [21]. A JPEG image can be resaved approximated sixty-four times with virtually no change until an image has undergone modification [18]. If an area of a JPEG image shows a significantly different error level, then it is an indication that the image has been altered. Some issues when using ELA as an analysis technique include low JPEG quality, or an image with significant amount of recoloring can result in false identification. This paper will compare some ELA examples from images that were analyzed between original images and edited images [17].

CHAPTER III

MATERIALS AND METHODS

Over one hundred images were collected from ten different digital cameras. The images are divided into four folder categories and they are "Original images," "Edited images," "Original images uploaded to Facebook," and "Edited images uploaded to Facebook." Images from Canon PowerShot SD300, Nikon D60 and Nikon D200 were collected directly from a home computer. Images from Kodak Easyshare V1003 ZOOM and Sony HDR-AS30V were collected from Dropbox. Images from Olympus TG-3, Olympus C150 D390, Nikon D90, Nikon D3000, and Nikon COOLPIX P500 were all collected through email. Adobe Photoshop was used to edit the original images. Editing process included uploading an original image to Adobe Photoshop and removing an area of the image using the option Content Aware and some images used Content Aware and Clone tool. The image is then saved with the quality level of twelve.

In addition, ten out of the one hundred images were also chosen to process at different compression rates using Adobe Photoshop to determine whether the manipulation is affected by each compression rate. Adobe Photoshop provides an option to change the quality level from zero, being the worst quality, to twelve, being the best quality. A spreadsheet was created to list image name, camera name, description of the image, and what Adobe Photoshop tool was used. All the images were saved to a removable drive. Images were sent to the National Center for Media Forensics (NCMF) through WeTransfer.com and the removable drive was brought in person. The images were loaded to the lab's computer using the DCT and ELA map

software. Each of the four folder category was processed using the "Folder Batch" option in the software which populated DCT and ELA reports.

In order to successfully investigate the image compression and manipulation, this paper will utilize the ACE-V methodology. ACE-V stands for Analysis, Comparison, Evaluation, and Verification. The ACE-V method is used to distinguish unique and relevant information. The analysis phase is simply collecting information and data. The comparison phase is the testing phase to determine whether the result is valid, invalid or inconclusive. The evaluation phase is the conclusion of the study. The final phase is the verification phase or the peer review phase [3]. This paper will not discuss the Verification phase since this is a laboratory process.

Once the collection of DCT and ELA maps were complete, a folder was created for each image. The folder consisted of the image that was processed as well as several DCT and ELA results to choose from. Each folder was reviewed and the best DCT and ELA results were chosen from each folder for presentation purposes. Image 100_3297 was analyzed using the DCT map results to demonstrate the image's original state. The DCT map image represents identical characteristics as the original image that was processed shown in Figure 2. It should also be noted that the file size for Image 100_3297 is 2.57 megabytes. Once Image 100_3297 was uploaded to Facebook, obvious signs of compression are noticeable such as rough edges around the leaves and the pixels appear distorted when zoomed in displayed in Figure 3. The file size also changed to 102 kilobytes after Facebook compression. Hash values were generated and recorded for the "Original images," "Edited images," "Original images uploaded to Facebook," and "Edited images uploaded to Facebook" as addition tools used in the

analysis phase. Each image saved under these categories has different hash values from the original. Figure 4 shows image 100_3297 with different hash values under different category and the different file size. Images are resized and recompressed by Facebook when uploaded so that the same image when downloaded is a different version of the original.

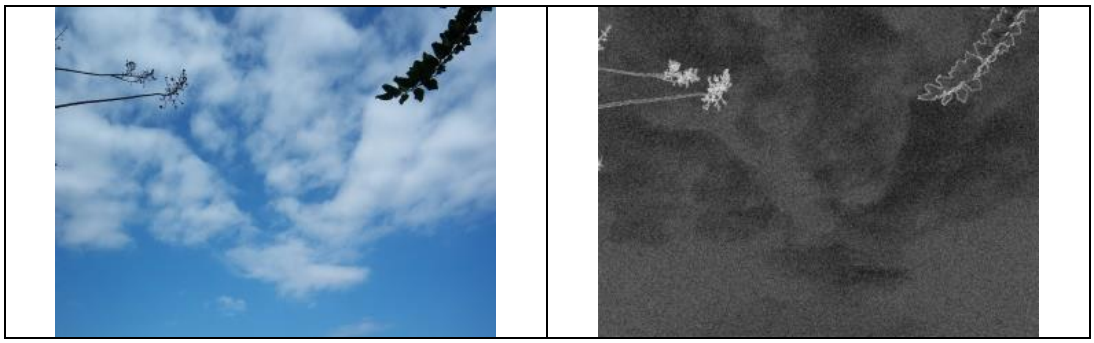


Figure 2.
Original Image 100_3297 (left) and DCT map results (right)

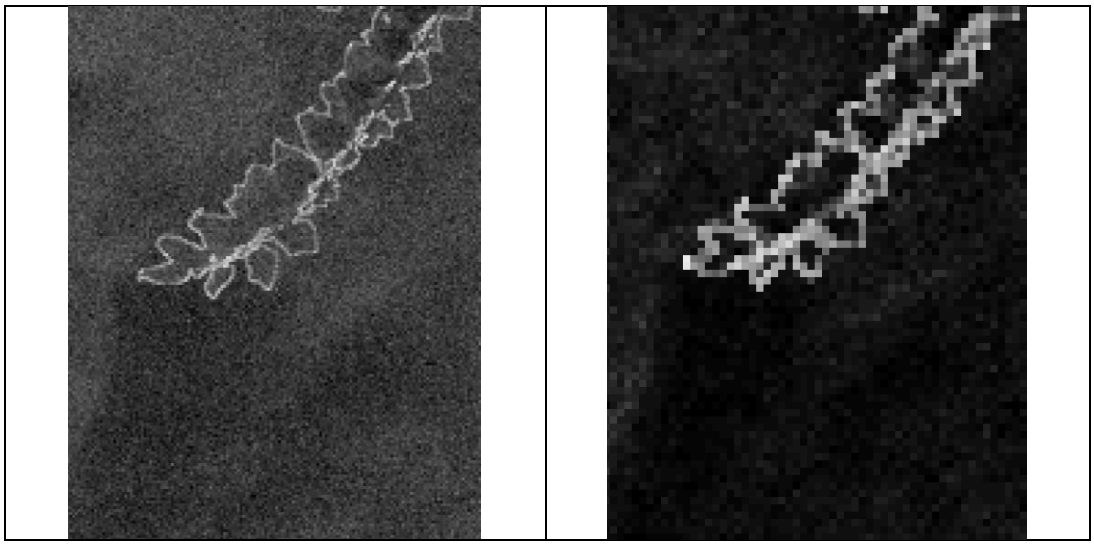


Figure 3.
Original image 100_3297 zoomed in before Facebook (left) and original image 100_3297 zoomed in after Facebook (right)

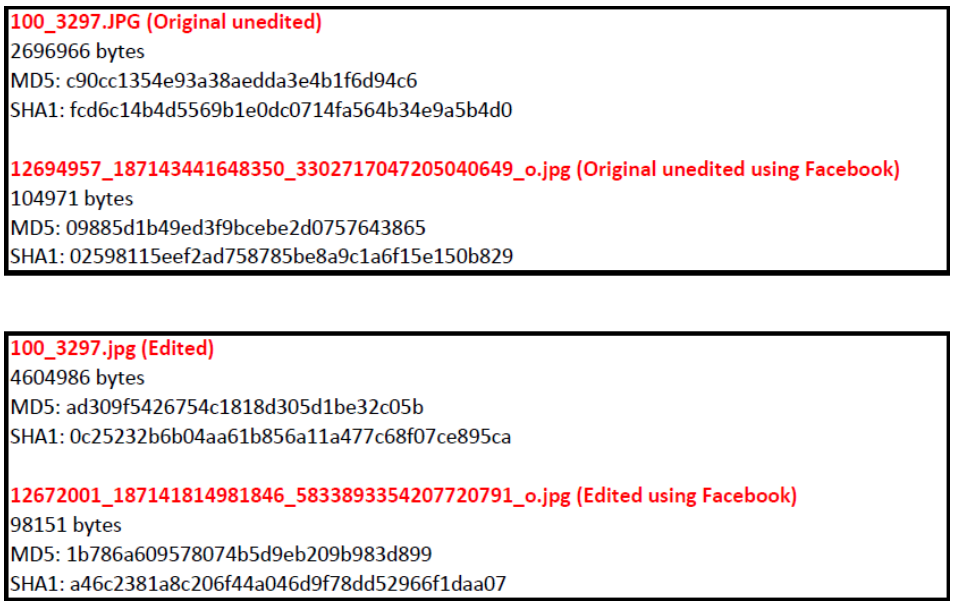


Figure 4.
Hash values for image 100_3297 indicating file size change

The same image, Image 100_3297, was edited through Adobe Photoshop where the branch towards the upper left side was deleted using Content Aware. The image was also analyzed through the software, DCT map produced a result showing where the manipulation was done shown in Figure 5(a). The black mass towards the upper left hand side of the image was where the editing was done. Once this image was edited through Adobe Photoshop, the file size changed to 4.39 megabytes. ELA on image 100_3297 was also analyzed. Since the software produces one hundred results with varying error levels, the best and most clear result was chosen. Figure 5(d) shows where the edit was done using ELA.

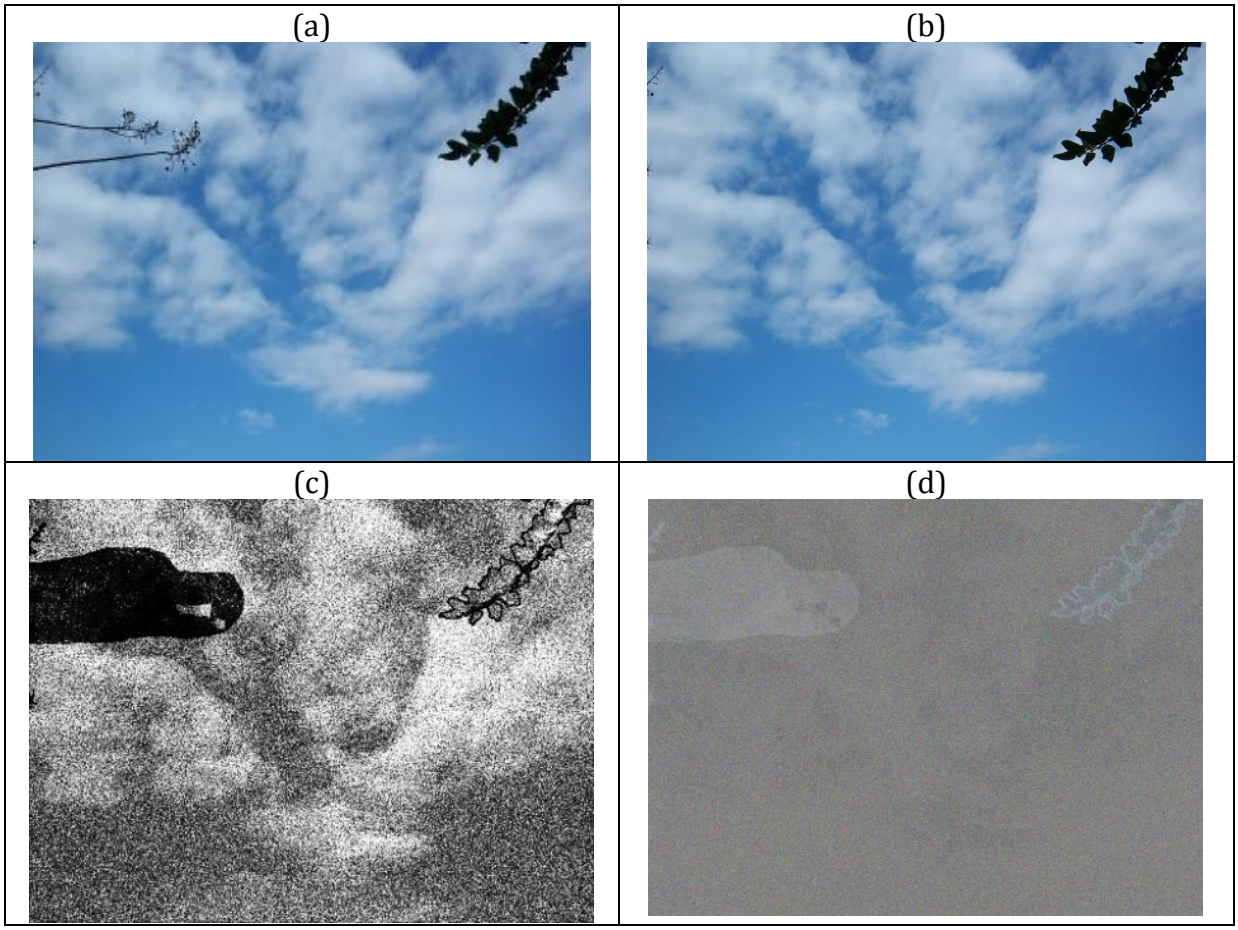


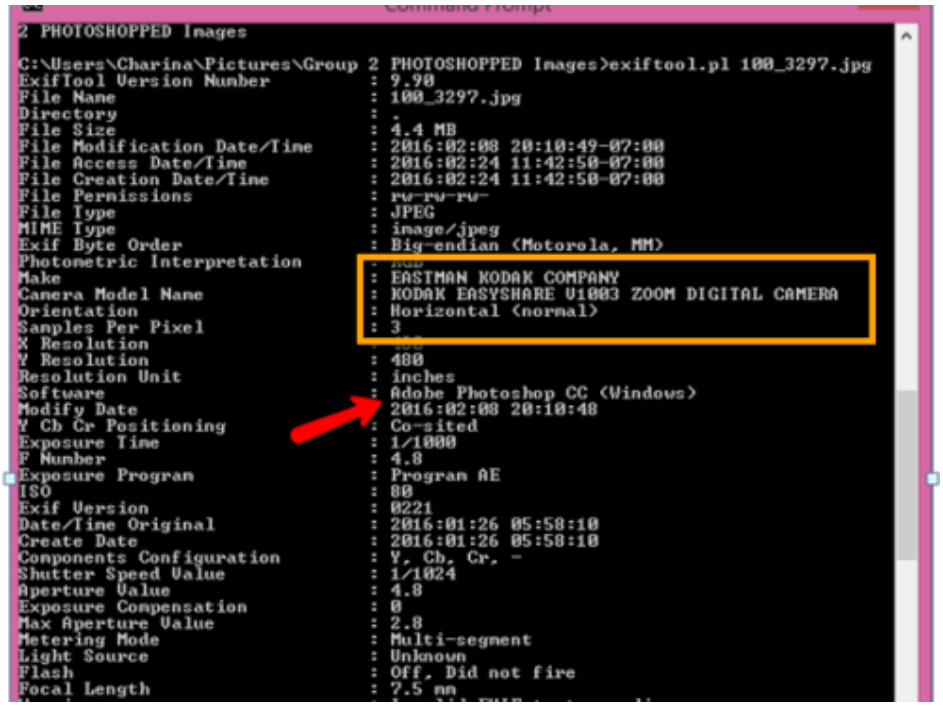
Figure 5 (a) Original image of 100_3297; **(b)** Edited image of 100_3297; **(c)** DCT map results of edited image 100_3297; **(d)** ELA results of edited image 100_3297

In addition to DCT map, ExifTool and WinHex were used to verify authentication. The metadata in image 100_3297 was analyzed which revealed traces of editing using Adobe Photoshop shown in Figure 5. "Metadata" is digital data that provides digital information about that data including file structure and location. Metadata facilitates the discovery of relevant information and helps organize electronic resources [15]. ExifTool is a free software program that reads metadata, in this case, an image's metadata [8]. ExifTool software was used on image 100_3297 which produced a report indicating and make and model of the digital camera that was used as well as the use of

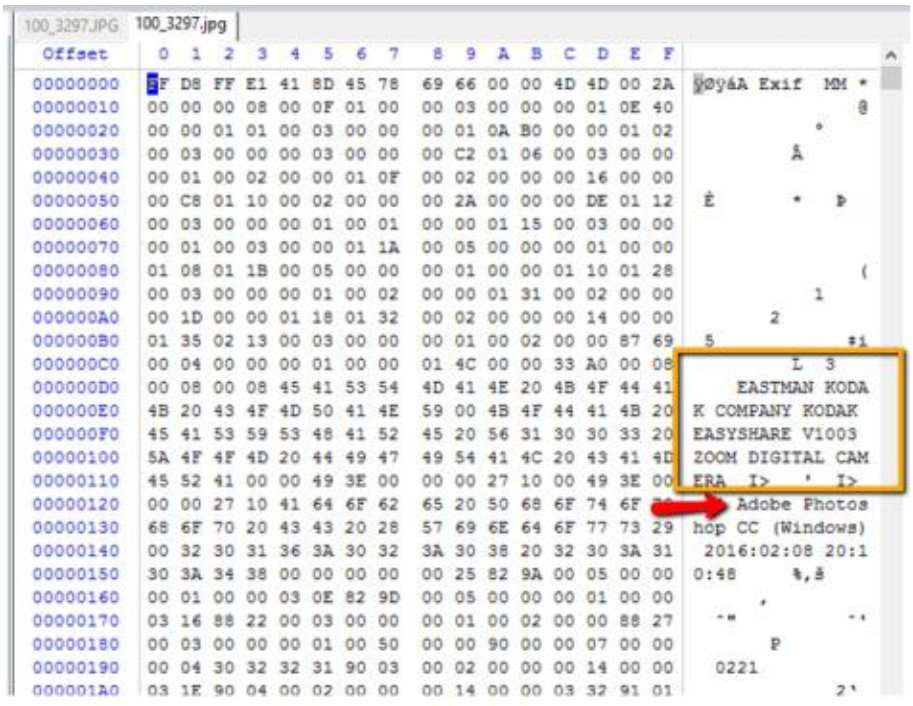
an editing software program such as Adobe Photoshop displayed in Figure 5a. WinHex is a hex editor used in data recovery. WinHex software was used on image 100_3297 that provides the image's hex analysis as well as the ASCII interpretation of the hex values. ASCII, which stands for American Standard Code for Information Interchange, uses codes that convert the hex values into text form [24]. The ASCII revealed the make and model of the digital camera used and that Adobe Photoshop was used on image 100_3297 shown in Figure 5b. Another tool used to analyze image 100_3297 is JPEGsnoop. JPEGsnoop is a window application that examines and decodes an image to include file size, camera make and model, EXIF information, and an assessment feature which indicates whether the application detected compressions [13].

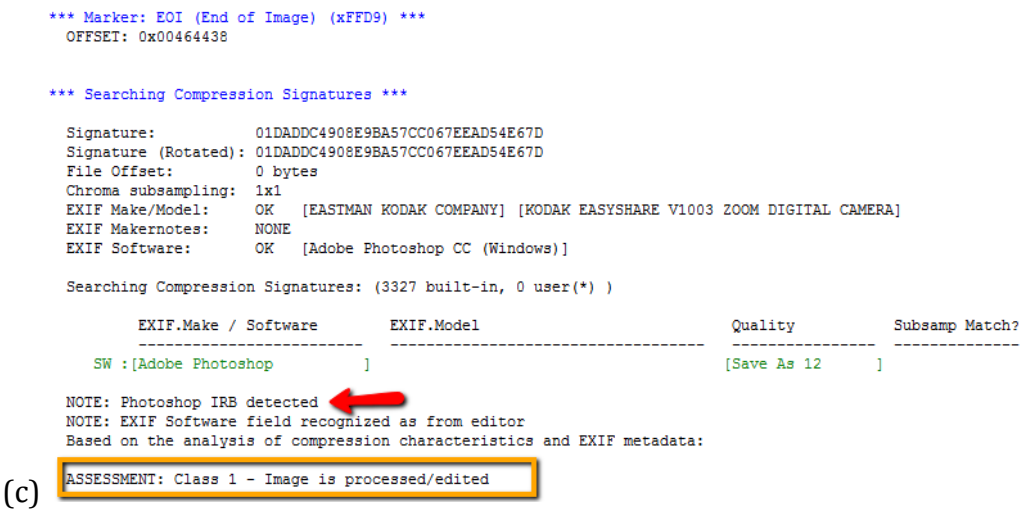
Since image 100_3297 original and edited versions were uploaded through Facebook, the analysis also included looking for traces indicative of Facebook use. None of the software applications used to analyze image 100_3297 provided any indication that the image had gone through Facebook. This information becomes important when making conclusions about detecting manipulation on Facebook images. It is also important to consider that original image 100_3297 was renamed "12694957_187143441648350_3302717047205040649_o" by Facebook and edited image 100_3297 was renamed "12672001_187141814981846_5833893354207720791_o." For the purpose of this paper, image 100_3297 will continue to be referred to as image 100_3297 instead of the renamed Facebook image name.

(a)


2 PHOTOSHOPPED Images
C:\Users\Charina\Pictures\Group 2 PHOTOSHOPPED Images>exiftool.pl 100_3297.jpg
ExifTool Version Number : 9.90
File Name : 100_3297.jpg
Directory : .
File Size : 4.4 MB
File Modification Date/Time : 2016:02:08 20:10:49-07:00
File Access Date/Time : 2016:02:24 11:42:50-07:00
File Creation Date/Time : 2016:02:24 11:42:50-07:00
File Permissions : rw-rw-rw-
File Type : JPEG
MIME Type : image/jpeg
Exif Byte Order : Big-endian (Motorola, MM)
Photometric Interpretation
Make : EASTMAN KODAK COMPANY
Camera Model Name : KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA
Orientation : Horizontal (normal)
Samples Per Pixel : 3
X Resolution
Y Resolution : 480
Resolution Unit : inches
Software : Adobe Photoshop CC (Windows)
Modify Date : 2016:02:08 20:10:48
Y Cb Cr Positioning : Co-sited
Exposure Time : 1/1000
F Number : 4.8
Exposure Program : Program AE
ISO : 80
Exif Version : 0221
Date/Time Original : 2016:01:26 05:58:10
Create Date : 2016:01:26 05:58:10
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value : 1/1024
Aperture Value : 4.8
Exposure Compensation : 0
Max Aperture Value : 2.8
Metering Mode : Multi-segment
Light Source : Unknown
Flash : Off, Did not fire
Focal Length : 7.5 mm

(b)


100_3297.JPG
100_3297.jpg
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 FF D8 FF E1 41 8D 45 78 69 66 00 00 4D 4D 00 2A
00000010 00 00 00 08 00 0F 01 00 00 03 00 00 00 01 0E 40
00000020 00 00 01 01 00 03 00 00 00 01 0A B0 00 00 01 02
00000030 00 03 00 00 00 03 00 00 00 C2 01 06 00 03 00 00
00000040 00 01 00 02 00 00 01 0F 00 02 00 00 00 16 00 00
00000050 00 C8 01 10 00 02 00 00 00 2A 00 00 00 DE 01 12
00000060 00 03 00 00 00 01 00 01 00 00 01 15 00 03 00 00
00000070 00 01 00 03 00 00 01 1A 00 05 00 00 00 01 00 00
00000080 01 08 01 1B 00 05 00 00 00 01 00 00 01 10 01 28
00000090 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00
000000A0 00 1D 00 00 01 18 01 32 00 02 00 00 00 14 00 00
000000B0 01 35 02 13 00 03 00 00 00 01 00 02 00 00 87 69
000000C0 00 04 00 00 00 01 00 00 01 4C 00 00 33 A0 00 08
000000D0 00 08 00 08 45 41 53 54 4D 41 4E 20 4B 4F 44 41
000000E0 4B 20 43 4F 4D 50 41 4E 59 00 4B 4F 44 41 4B 20
000000F0 45 41 53 59 53 48 41 52 45 20 56 31 30 30 33 20
00000100 5A 4F 4F 4D 20 44 49 47 49 54 41 4C 20 43 41 4D
00000110 45 52 41 00 00 49 3E 00 00 00 27 10 00 49 3E 00
00000120 00 00 27 10 41 64 6F 62 65 20 50 68 6F 74 6F
00000130 68 6F 70 20 43 43 20 28 57 69 6E 64 6F 77 73 29
00000140 00 32 30 31 36 3A 30 32 3A 30 38 20 32 30 3A 31
00000150 30 3A 34 38 00 00 00 00 00 25 82 9A 00 05 00 00
00000160 00 01 00 00 03 0E 82 9D 00 05 00 00 00 01 00 00
00000170 03 16 88 22 00 03 00 00 00 01 00 02 00 00 88 27
00000180 00 03 00 00 00 01 00 50 00 00 90 00 00 07 00 00
00000190 00 04 30 32 32 31 90 03 00 02 00 00 00 14 00 00
000001A0 03 1E 90 04 00 02 00 00 00 14 00 00 03 32 91 01
EASTMAN KODA
K COMPANY KODAK
EASYSHARE V1003
ZOOM DIGITAL CAM
ERA
Adobe Photos
hop CC (Windows)
2016:02:08 20:1
0:48
0221



(c)

Figure 6.
(a) ExifTool results; (b) WinHex results; (c) JPEGsnoop results

CHAPTER IV

THE RESULTS

In order to understand the importance of detecting manipulation on any images, it is as important to look at both original and edited images side by side to distinguish what type of editing was done to the image. In most cases, detectives and examiners don't have the privilege of having the original to compare with. Since this paper allows the opportunity to work with the original images, it will provide the comparison between an original and an altered image. For instance, Figure 7 shows an edited version of an image named Elk3. The picture appears to be original unless there was reason to believe this picture has been tampered with. When the original is presented next to the edited one, it is obvious that part of the image has been manipulated.

(a)  (b) 

Figure 7.
Elk3 edited image (a) and original image (b)

Then the comparison process moves on to the DCT and ELA results and those should also be compared next to each other as well. For this example, Figure 8 will demonstrate the significant amount of contrast that DCT map and ELA display. There is certain indication that the image was tampered in the areas where the pixel values

change significantly. To confirm this observation, both original and edited images were analyzed through WinHex where the analysis confirms the make and model of the camera and the results were compared side by side in Figure 9.

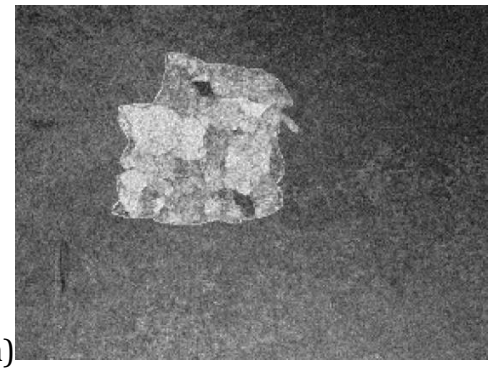
(a)  (b) 

Figure 8.
DCT map result (a) and ELA result (b)

(a)

Elk3.JPG

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E1	29	FE	45	78	69	66	00	00	49	49	2A	00	ÿØÿá)þExif II*
00000010	08	00	00	00	09	00	0F	01	02	00	06	00	00	00	7A	00	z
00000020	00	00	10	01	02	00	16	00	00	00	80	00	00	00	12	01	€
00000030	03	00	01	00	00	00	01	00	00	00	1A	01	05	00	01	00	
00000040	00	00	A0	00	00	00	1B	01	05	00	01	00	00	00	A8	00	¨
00000050	00	00	28	01	03	00	01	00	00	00	02	00	00	00	32	01	(2
00000060	02	00	14	00	00	00	B0	00	00	00	13	02	03	00	01	00	°
00000070	00	00	01	00	00	00	69	87	04	00	01	00	00	00	C4	00	i‡ Ä
00000080	00	00	94	08	00	00	43	61	6E	6F	6E	00	43	61	6E	6F	” Canon Cano
00000090	6E	20	50	6F	77	65	72	53	68	6F	74	20	53	44	33	30	n PowerShot SD30
000000A0	30	00	00	00	00	00	00	00	00	00	00	00	B4	00	00	00	0 ´
000000B0	01	00	00	00	B4	00	00	00	01	00	00	00	32	30	30	35	´ 2005
000000C0	3A	30	38	3A	30	37	20	31	31	3A	31	38	3A	34	30	00	:08:07 11:18:40

(b)

Elk3.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E1	1F	2C	45	78	69	66	00	00	49	49	2A	00	ÿØÿá ,Exif II*
00000010	08	00	00	00	0F	00	00	01	03	00	01	00	00	00	E0	08	à
00000020	00	00	01	01	03	00	01	00	00	00	A8	06	00	00	02	01	¨
00000030	03	00	03	00	00	00	C2	00	00	00	06	01	03	00	01	00	Â
00000040	00	00	02	00	00	00	0F	01	02	00	06	00	00	00	C8	00	È
00000050	00	00	10	01	02	00	16	00	00	00	CE	00	00	00	12	01	Î
00000060	03	00	01	00	00	00	01	00	00	00	15	01	03	00	01	00	
00000070	00	00	03	00	00	00	1A	01	05	00	01	00	00	00	E4	00	ä
00000080	00	00	1B	01	05	00	01	00	00	00	EC	00	00	00	28	01	ì (
00000090	03	00	01	00	00	00	02	00	00	00	31	01	02	00	1D	00	1
000000A0	00	00	F4	00	00	00	32	01	02	00	14	00	00	00	11	01	ô 2
000000B0	00	00	13	02	03	00	01	00	00	00	01	00	00	00	69	87	i‡
000000C0	04	00	01	00	00	00	28	01	00	00	64	04	00	00	08	00	(d
000000D0	08	00	08	00	43	61	6E	6F	6E	00	43	61	6E	6F	6E	20	Canon Canon
000000E0	50	6F	77	65	72	53	68	6F	74	20	53	44	33	30	30	00	PowerShot SD300
000000F0	40	77	1B	00	10	27	00	00	40	77	1B	00	10	27	00	00	@w ' @w '
00000100	41	64	6F	62	65	20	50	68	6F	74	6F	[redacted]					Adobe Photoshop
00000110	43	43	20	28	57	69	6E	64	6F	77	73	29	00	32	30	31	CC (Windows) 201
00000120	36	3A	30	31	3A	33	30	20	32	32	3A	34	39	3A	32	34	6:01:30 22:49:24
00000130	00	00	00	00	1F	00	9A	82	05	00	01	00	00	00	A2	02	š, ¢

Figure 9.
Elk original (a); Elk3 edited (b)

When the edited version of image Elk3 was uploaded through Facebook, the DCT map characteristic significantly changed. The edited portion of image Elk3 has disappeared in the DCT map results. Facebook's compression rate has caused the manipulation of the image to be undetected. The following tables are comparison between the image's original state and its DCT map results. The characteristics that were mentioned earlier in this paper remained consistent in regards to the by-product of Facebook compressions. Table 1 confirms the Facebook compressions effect on the pixels of the image shown in the lower right box. The DCT map for the original images using Facebook illustrates an object that is too distorted to make out but nonetheless, the object is visible.

Table 1. Original images of Elk3 with Facebook and without Facebook

Image	DCT Map results
	
	

Table 2. Edited image of Elk3 with Facebook and without Facebook

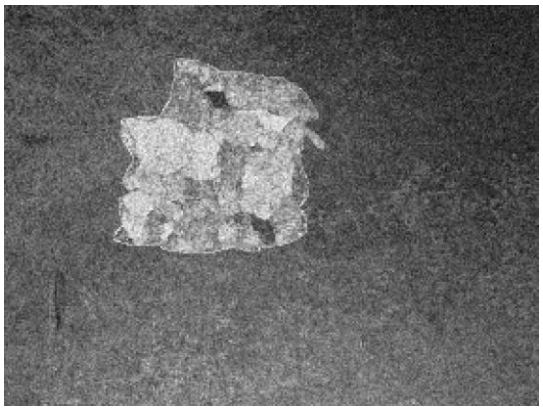
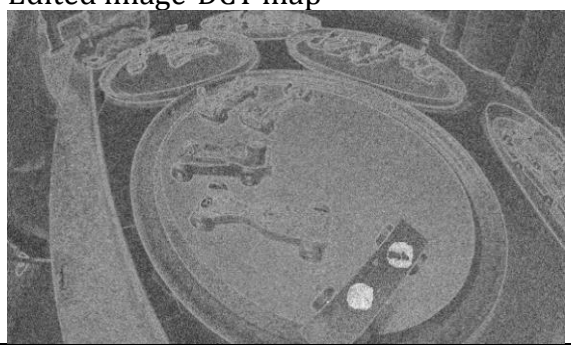
Edited image	
Before Facebook: 	
After Facebook: 	

Table 2 is the edited version of image Elk3. The top row is the images with an object removed before and after using Facebook. The bottom row displays the DCT map results for the edited versions before and after Facebook was used. The DCT map result for the edited version before using Facebook visibly indicates an area of the image that has been changed. However, the DCT map result for the edited version of the image after Facebook seems to have disappeared. When looking closer to this result, it is evident that the compression through Facebook may have caused the disappearance of the removed area although a small amount of the removed area may have left some traces on this specific image. Another image with a much smaller scale of editing was analyzed to conclude whether editing is detected or not. Image DSC00188 was tampered with by removing the two dots off of the black skateboard situated towards the front of the image. Image DSC00188 was also uploaded to Facebook then analyzed through the forensic software. The results show that editing smaller areas are as difficult to detect as the larger areas of editing shown in Table 3.

Table 3: Image DSC00188 and DCT map results

Original image 	Original image-DCT map 
Edited image 	Edited image-DCT map 
Original image using Facebook 	Original image using Facebook-DCT map 
Edited image using Facebook 	Edited image using Facebook-DCT map 

Another image with a smaller editing area, illustrates the DCT map with and without the use of Facebook. An object towards the center of the image was removed which is noticeable using the DCT map. The same object disappeared after the image was uploaded to Facebook as shown in Table 4.

Table 4: Image Pictures-451 edited using DCT map results before and after Facebook

Original image 	Original image-DCT map 
Edited image 	Edited image-DCT map 

Table 4 cont.

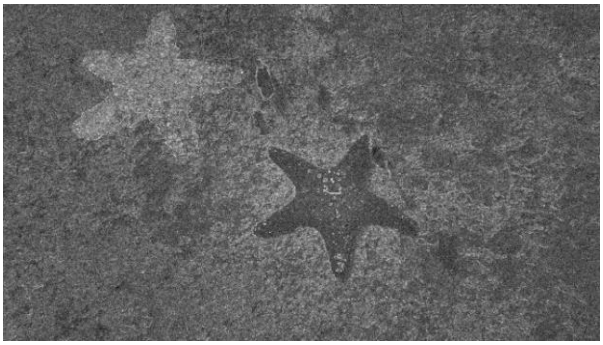
Original image using Facebook 	Original image using Facebook-DCT map 
Edited image using Facebook 	Edited image using Facebook-DCT map 

To further investigate this occurrence, another image with a bigger edited area was studied. Table 5 has two starfish in the original image and one of the starfish on the left was removed using Adobe Photoshop.

Table 5: Original image of P9230407 before and after using Facebook

Image P9230407	DCT map results
Before Facebook: 	
After Facebook: 	

Table 6: Edited image of P9230407 before and after using Facebook

Image P9230407	DCT map results
Before Facebook: 	
After Facebook 	

The images in Table 6 are the edited versions with their corresponding DCT map results. The starfish on the left that was intentionally removed can be seen in the DCT map results before using Facebook. The DCT map for image P9230407 after using Facebook has caused the editing evidence to disappear. The DCT map for edited image P9230407 after using Facebook has a similar characteristic change as the edited Elk3 image where both image's editing traces seem to have vanished.

The theory of whether manipulation can be detected through Facebook images will need to be proven based on compression. Since this paper has discussed the high compression rate that Facebook applies, the study will now shift towards tampering an

image at high compression rates without using Facebook. The experiment utilized Adobe Photoshop's ability to manipulate the compression rate used on an image. As mentioned earlier, Adobe Photoshop allows saving an image at different compression rates ranging from zero to twelve. Compression rate set a zero applies the highest compression therefore, the poorest quality. On the other hand, compression rate set at twelve will produce the best quality on an image. The following table of image P9230407 demonstrates the DCT map results of low, mid-level, and high compression rates using Adobe Photoshop.

Table 7: Adobe Photoshop images saved at different compression rates of image P9230407 and Facebook result at the same compression rates

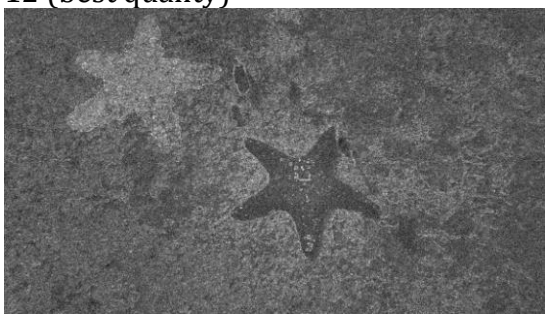
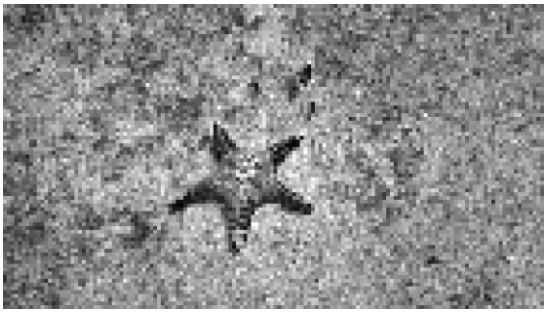
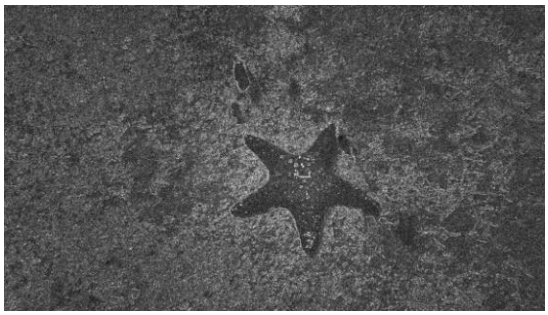
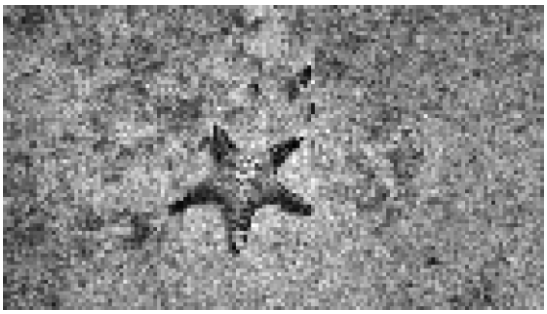
Adobe Photoshop compression	Adobe Photoshop compression using Facebook
12 (best quality) 	12 
11 	11 

Table 7 (cont.)

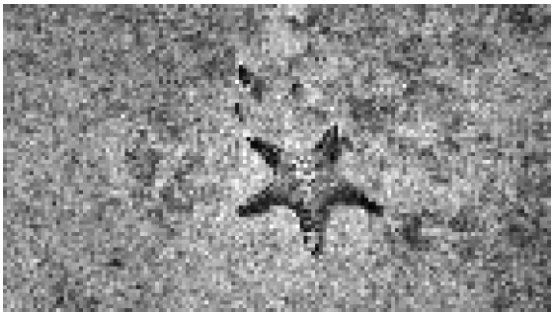
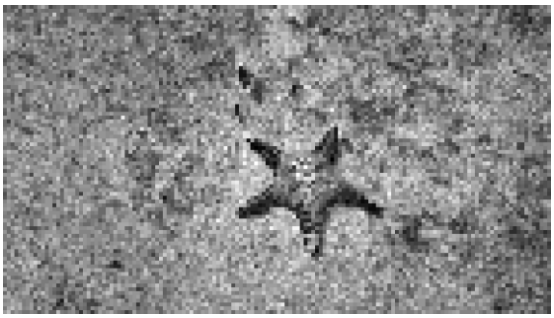
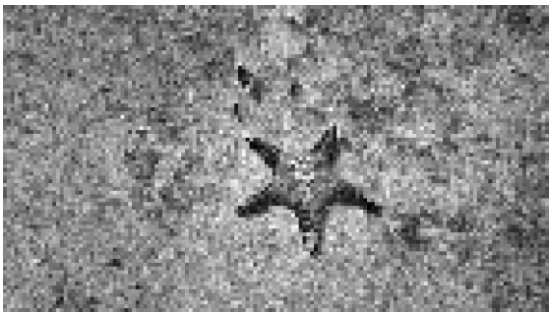
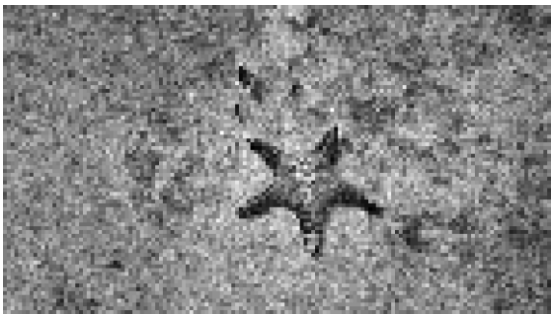
10 	10 
9 	9 
8 	8 
7 	7 

Table 7 (cont.)

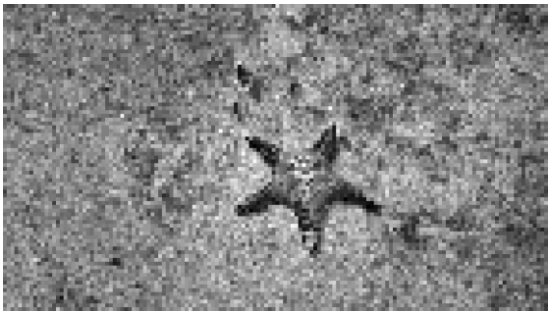
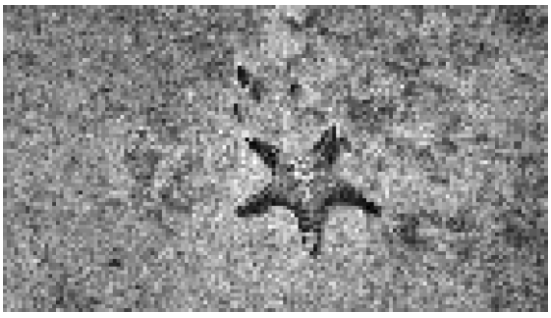
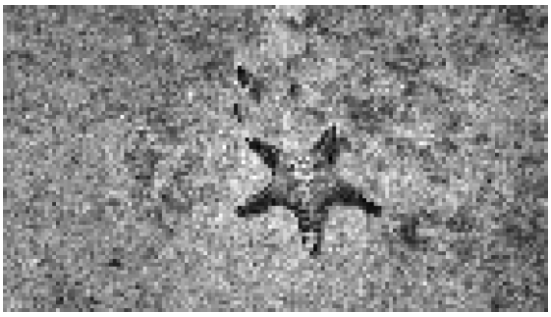
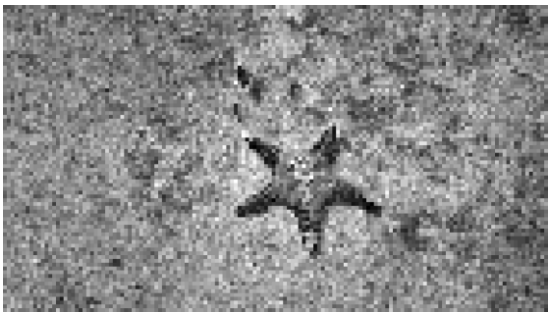
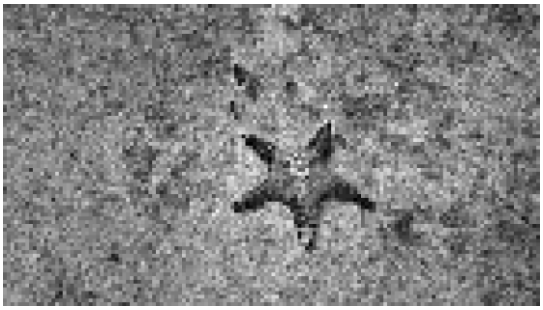
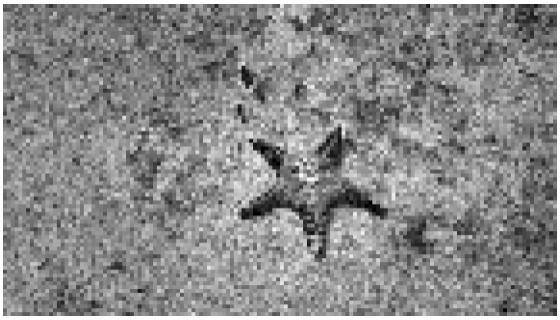
6 	6 
5 	5 
4 	4 
3 	3 

Table 7 (cont.)

2 	2 
1 	1 
0 	0 

The results indicate that when the image was saved at the compression rate 12, the editing is visible through DCT map whereas the image saved at a compression rate of 11 or below, the editing area becomes less visible and more difficult to detect. Different compression rates noticeably produced different DCT map results and seemingly the compression rate set at zero formed the darkest results. The Facebook results using the same compression rates also indicate that the tampered area is difficult and almost impossible to detect. Additional testing was done on another image to further study the effects of compression. Image DSC-1661 was edited through Adobe Photoshop where an area towards the left side of the image was removed shown in Figure 10. Note that all images that were saved using Adobe Photoshop were automatically saved using compression rate 12 unless otherwise noted.

Figure 10. DCT map results for edited image DSC-1661

The following comparison was conducted between the DCT map of image DSC-1661 at compression rate of twelve and zero. Again, the evidence of editing is more visible

when low compression rate is used and less visible when a higher compression rate is used as it shows in Table 8.

Table 8: DCT map results on DSC-1661 between compression rates 12 and 0.

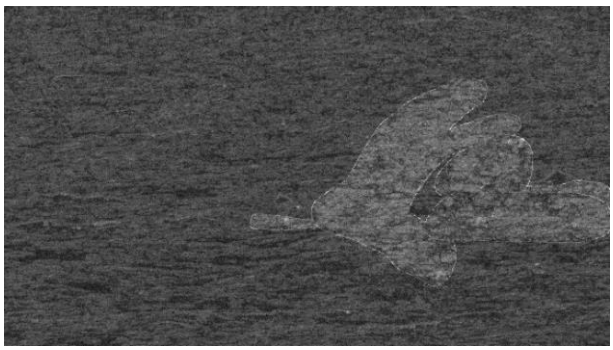
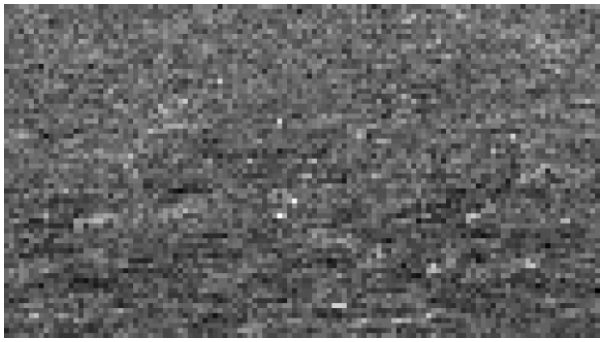
 Compression rate at 12	 Compression rate at 0

The next step is to validate the theory whether compressions actually affect the detection of image manipulation. The study has confirmed that Facebook compression affected the ability to detect tampering. In addition, using high compressions in Adobe Photoshop resulted in difficulty detecting tampering. Table 9 compares the results due to Facebook compressions and Adobe Photoshop compressions.

Table 9: Comparison between Facebook compression and Adobe Photoshop compression on image P9210122

Original	

Table 9 (cont.)

Edited	
Edited (DCT map)	
Facebook Compression	
Adobe Photoshop compression rate set at 0	

The comparison between the Facebook compression and Adobe Photoshop compression may not look the same but it is obvious that both results do not display any signs of manipulation. Although it is unknown how much compression Facebook applies, the results are apparent that the pixels in the image are distorted with rough edges whereas Adobe Photoshop compression appears to have slightly less pixel distortion than Facebook. Both types of compressions seems to have different compression rates based on the observations mentioned earlier but both compressions produced identical results which caused the editing to disappear therefore confirming the comparison is valid.

The evaluation process of this study will address the conclusion whether manipulation on Facebook images can be detected. As previewed, the compression that Facebook applies on images results in artifact production and distortion. When an image has been tampered with, DCT map provides indication of the tampered area. This becomes important during investigation as it validates any questionable image. Facebook, on the other hand, uses compressions on images in order to make room for the billions of photos they host. This becomes an issue when trying to analyze a questionable image as this paper has presented. The images that were analyzed were processed through different application confirming they were altered. In addition to that process, the images were also processed through the DCT map and ELA which also confirmed traces of tampering. Each procedure authenticates manipulation done on the images. It appears that any high compression applied to images resulted in losing evidence of tampering. This validates that detecting manipulation on edited Facebook images through DCT map is not possible even when other processes are used such as

WinHex, ExifTool and JPEGsnoop. Using the varying compression rates in Adobe Photoshop also confirmed that the highest compression rate can cause the editing to disappear.

CHAPTER V

CONCLUSION

Image manipulation can easily be done by anyone having experience with editing software such as Adobe Photoshop. In this case, a tampered image may be used to fabricate a story to deceive the audience or simply to remove unwanted objects in an image. Nonetheless, an observer will not be able to decipher between an original image from an altered one. Fortunately, forensic tools are able to detect editing software to verify authentication. WinHex, ExifTool, JPEGsnoop, and DCT and ELA map software are all useful to investigators to build their case. The results clearly indicate traces of editing tool as previously illustrated. Some software specifically produces apparent traces of manipulation in the DCT map as shown in this paper. Unfortunately, when images are used in Facebook, high compression rates are applied and artifacts are formed. In addition to artifacts, Facebook's compression has also produced rough edged pixels, which has resulted in making the image look distorted. As the analysis progressed, it was discovered that Facebook's compression affected the DCT map results causing the edited areas to disappear. To further study this occurrence, some images were saved in Adobe Photoshop in varying compression rates. DCT map results show that Adobe Photoshop's high compression rate produced identical DCT map result as Facebook compression where the traces of manipulation have disappeared. The limitation in this study should be mentioned that this was not a blind study, and that the researcher was aware where the alterations on the image were done. Even though ELA was also utilized during the analysis process, the DCT map results provide a stronger distinction on where the manipulation was applied. In conclusion, detecting

manipulation on Facebook images is difficult to accomplish. Further research should include studying the changes in pixels when exposed to high compression rates and how it is affecting the DCT map's tampered area to disappear. Additional study should also be done analyzing the compression results producing different pixel characteristics shown in Table 9 between Facebook compression and Adobe Photoshop compression. It should also be considered that knowing Facebook's compression rate would be beneficial to the study. This information allows the research to look into the characteristic changes in pixels.

The results in the study show that detecting tampering could depend on several variables such as the quality of the original JPEG image as well as the size of the tampered area. Each camera used in this study also has different image quality therefore may possibly affect the results of the manipulation. Another consideration that detecting manipulation may be influenced by the algorithm used for tampering and the JPEG compression settings to save the tampered image as shown in Table 7. Each compression rate shows different results in the DCT map. Facebook, as well as other social media websites, also use their own JPEG compression rates that may determine the detection of image manipulation. Nonetheless, any or all of the explanations mentioned above could certainly affect whether or not a tampered area in a digital image is detectable.

REFERENCES

1 "ACM_MIFOR09_DCT.pdf," n.d.
2 Catalin Grigoras. "Foundations in Media Forensics." n.d. https://ucdenver.instructure.com/courses/10068/files/folder/Lectures?preview=834638.
3 Craig Coppock. "Universal Definition of ACE-V Updated," December 11, 2006. http://fingerprintindividualization.blogspot.com/2012/06/universal-definition-of-ace-v-updated.html.
4 "Digital Camera," n.d. https://en.wikipedia.org/wiki/Digital_camera.
5 "Digital Evidence and Forensics." National Institute of Justice, October 28, 2015. http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.
6 "Error Level Analysis," n.d. https://sites.google.com/site/elsamuko/forensics/ela.
7 "Error Level Analysis," n.d. https://en.wikipedia.org/wiki/Error_level_analysis.
8 "ExifTool," n.d. https://en.wikipedia.org/wiki/ExifTool.
9 Grigoras, C, and Smith, JM. "Digital Imaging: Enhancement and Authentication," n.d.
10 James Barker. "Avoiding Facebook Image Compression," 2004. http://www.freedigitalphotos.net/blog/tutorials/avoiding-facebook-image-compression/.
11 "JPEG." n.d. https://cseweb.ucsd.edu/classes/sp03/cse228/Lecture_5.html.
12 "JPEG," n.d. https://en.wikipedia.org/wiki/JPEG.
13 "Jpegsnoop." Accessed March 14, 2016. https://sourceforge.net/projects/jpegsnoop/.
14 Mark Pollitt. "https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf," n.d.
15 "Metadata," n.d. https://en.wikipedia.org/wiki/Metadata.
16 Neal Krawetz. "A Picture's Worth...Digital Image Analysis and Forensics Version 2." n.d. https://www.blackhat.com/presentations/bh-dc-08/Krawetz/Whitepaper/bh-dc-08-krawetz-WP.pdf.
17 ———. "Http://www.wired.com/images_blogs/threatlevel/files/bh-Usa-07-Krawetz.pdf." 2007. www.hackerfactor.com.
18 Pierluigi Paganini. "Photo Forensics: Detect Photoshop Manipulation with Error Level Analysis," n.d. http://resources.infosecinstitute.com/error-level-analysis-detect-image-manipulation/.
19 Scott Anderson. "Digital Imaging: Enhancement and Authentication," n.d.
20 "SWGDE Image Processing Guidelines," February 8, 2016. https://www.swgde.org/documents/Current%20Documents/2016-02-08%20SWGDE%20Image%20Processing%20Guidelines.
21 "Tutorial: Error Level Analysis." FotoForensics, n.d. http://fotoforensics.com/tutorial-ela.php.
22 "Understainding Metadata." Bathesda, MD, 2004. http://www.niso.org/publications/press/UnderstandingMetadata.pdf.
23 "Who Is SWGDE and What Is the History?," n.d. https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf.
24 "WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor," n.d. https://www.x-ways.net/winhex/.

APPENDIX

a. Image name, camera make , editing process (Adobe Photoshop edting tool "content aware" set at compression rate 12.

Image	Camera	Photoshop Process
100_3292	KODAK EASYSHARE V1003 ZOOM	removed upper left branches
100_3293	KODAK EASYSHARE V1003 ZOOM	removed cloud lower right
100_3294	KODAK EASYSHARE V1003 ZOOM	removed tree reflection bottom right
100_3295	KODAK EASYSHARE V1003 ZOOM	removed clouds upper left
100_3296	KODAK EASYSHARE V1003 ZOOM	removed branch top center
100_3297	KODAK EASYSHARE V1003 ZOOM	removed branch upper left
100_3298	KODAK EASYSHARE V1003 ZOOM	removed house reflection left side
100_3299	KODAK EASYSHARE V1003 ZOOM	removed bush towards the left
100_3300	KODAK EASYSHARE V1003 ZOOM	removed branch upper left
100_3301	KODAK EASYSHARE V1003 ZOOM	removed cloud center
BuffaloFromField	Canon PowerShot SD300	removed one buffalo in center
DSC_0001	NIKON D3000	removed small tree towards the right
DSC_0003	NIKON D60	removed flag pole on the right
DSC_0004	NIKON D60	removed shrub/weed towards the bottom left
DSC_0007	NIKON D3000	removed tree trunk towards bottom right
DSC_0008	NIKON D3000	removed tree branch towards the center of pic
DSC_0009	NIKON D3000	removed shrub bottom center
DSC_0014	NIKON D3000	removed branches top left of pic

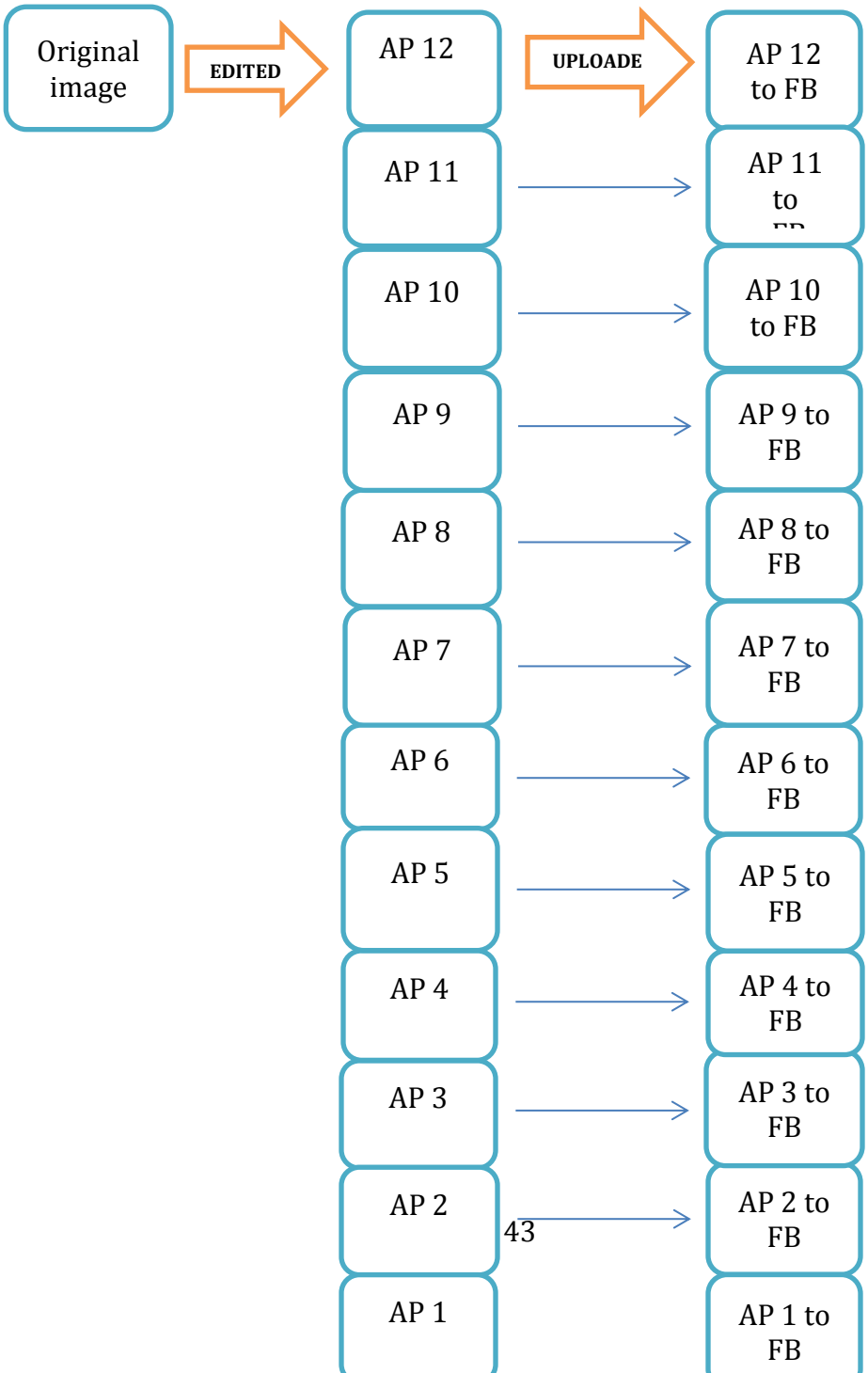
DSC_0020	NIKON D3000	removed trees towards the left and center of pic
DSC_0027	NIKON D90	removed center apple
DSC_0029	NIKON D3000	removed car in the front
DSC_0034	NIKON D90	removed broken glass middle window
DSC_0035	NIKON D60	removed chain towards bottom left
DSC_0040	NIKON D60	removed writing on the bottom of sign
DSC_0044	NIKON D90	removed girl
DSC_0062	NIKON D60	removed flash spot
DSC_0063	NIKON D60	removed traffic barrell in road
DSC_0066	NIKON D60	removed flag pole and flag on the right
DSC_0072	NIKON D90	removed tree shadow to the left of pic
DSC_0075	NIKON D60	removed signs on pier
DSC_0079	NIKON D60	removed beach lounge chairs
DSC_0083	NIKON D3000	removed clouds center
DSC_0087	NIKON D60	removed bush in front
DSC_0091	NIKON D60	removed branch on the right hand side
DSC_0107	NIKON D90	removed numbers on podium
DSC_0121	NIKON D90	removed top of column on right side
DSC_0148	NIKON D90	removed paint can
DSC_0171	NIKON D90	removed second letter H
DSC_0175	NIKON D90	removed necklace on girl on left side
DSC_0180	NIKON D90	removed upper middle wire
DSC_0390	NIKON D90	removed bolts bottom right
DSC_1228	NIKON D60	removed woman and stroller to the left

DSC_1231	NIKON D60	removed island to the left
DSC_1234	NIKON D60	removed 4 holes under the sign
DSC_1655	NIKON D60	removed building on the left side of pic
DSC_1660	NIKON D60	removed tree
DSC_1661	NIKON D60	removed writing on left side of building
DSC_1664	NIKON D60	removed light on top of light post
DSC00188	SONY HDR-AS30V	removed dot on skateboard towards front of pic
DSCN4814	NIKON COOLPIX P500	removed shirt writing
DSCN4980	NIKON COOLPIX P500	removed writing on card
Elk3	Canon PowerShot SD300	removed elk
Elk5	Canon PowerShot SD300	removed horn shadows
IMG_0205	Canon PowerShot SD300	removed two branches upper left
IMG_2768	Canon PowerShot SD300	removed wall sign
IMG_2769	Canon PowerShot SD300	removed watch
IMG_2770	Canon PowerShot SD300	removed bottom left shirt, ink on arm, flash spots on wall and on table
IMG_2771	Canon PowerShot SD300	removed flash spots on wall
IMG_2772	Canon PowerShot SD300	removed watch
IMG_2773	Canon PowerShot SD300	removed table on bottom left corner and removed flash spot
IMG_2774	Canon PowerShot SD300	removed right trophy
IMG_2775	Canon PowerShot SD300	removed glare top center of pic
IMG_2776	Canon PowerShot SD300	removed upper left square
IMG_2779	Canon PowerShot SD300	removed flyer on left side
IMG_5974	SONY HDR-AS30V	removed splash mark

MammothSprings	Canon PowerShot SD300	removed house to the left of rock
MiniGeyser4	Canon PowerShot SD300	removed tree in foreground
More Buffalos	Canon PowerShot SD300	removed buffalo towards the left of pic
P1010048-1	OLYMPUS C150, D390	removed branches top left of pic
P1010078-1	OLYMPUS C150, D390	removed smudge op left, removed line under 'Lutheran'
P1020029-1	OLYMPUS C150, D390	removed 2 shoes upper right
P9160009	OLYMPUS TG-3	removed blue pillows middle design
P9170013	OLYMPUS TG-3	removed 2 lounge chairs on left
P9170022	OLYMPUS TG-3	removed leaf on top of flower
P9170025	OLYMPUS TG-3	removed clouds upper left
P9180040	OLYMPUS TG-3	removed writing on crate
P9210122	OLYMPUS TG-3	removed whale tail
P9220174	OLYMPUS TG-3	removed fin
P9220207	OLYMPUS TG-3	removed fish
P9230407	OLYMPUS TG-3	removed starfish
P9270708	OLYMPUS TG-3	removed straw
Pictures 030	OLYMPUS C150, D390	removed exit sign above door, removed flas spot
Pictures 069	OLYMPUS C150, D390	removed two crosses
Pictures 451	OLYMPUS C150, D390	removed white puck in the center, removed flash spots
Pictures 482	OLYMPUS C150, D390	removed writing in front of red train
Pictures 490	OLYMPUS C150, D390	removed shadow towards upper right of pic
Pictures 492	OLYMPUS C150, D390	removed cross on orange paper
Pictures 508	OLYMPUS C150, D390	removed black strip bottom left of pic
Roosevelt1	Canon PowerShot SD300	removed branches on left

September 2009 001	Nikon D200	removed "Saturday" on inviatation
September 2009 048	Nikon D200	removed two flowers
September 2009 066	Nikon D200	removed one flower right side
September 2009 069	Nikon D200	removed suit pocket
September 2009 072	Nikon D200	removed flag, pole, and shadow
September 2009 076	Nikon D200	removed heart on white bag
September 2009 078	Nikon D200	removed flowers on second tier of cake
September 2009 080	Nikon D200	removed leaf on right side
Smoke	Canon PowerShot SD300	removed cloud
Viewof UpperFalls	Canon PowerShot SD300	removed two clouds upper left
YellowstonRiver	Canon PowerShot SD300	removed rocks in river

b. Process for Table 7 Adobe Photoshop (AP) compression rate uploaded to Facebook (FB)



c. Results summary

Edited image	DCT detected ?	ELA detected?
100_3292	Y	Y
100_3293	Y	Y
100_3294	Y	Y
100_3295	Y	Y
100_3296	Y	Y
100_3297	Y	Y
100_3298	Y	Y
100_3299	Y	Y
100_3300	Y	Y
100_3301	Y	Y
BuffaloFromField	N	N
DSC_0001	N	N
DSC_0003	N	N
DSC_0004	N	N
DSC_0007	N	N
DSC_0008	N	N
DSC_0009	N	N
DSC_0014	N	N

Edited image using Facebook	DCT detected ?	ELA detected ?
100_3292	N	N
100_3293	N	N
100_3294	N	N
100_3295	N	N
100_3296	N	N
100_3297	N	N
100_3298	N	N
100_3299	N	N
100_3300	N	N
100_3301	N	N
BuffaloFromField	N	N
DSC_0001	N	N
DSC_0003	N	N
DSC_0004	N	N
DSC_0007	N	N
DSC_0008	N	N
DSC_0009	N	N
DSC_0014	N	N

DSC_0020	N	N	DSC_0020	N	N
DSC_0027	N	N	DSC_0027	N	N
DSC_0029	N	N	DSC_0029	N	N
DSC_0034	N	N	DSC_0034	N	N
DSC_0035	N	N	DSC_0035	N	N
DSC_0040	N	N	DSC_0040	N	N
DSC_0044	Y	Y	DSC_0044	N	N
DSC_0062	N	N	DSC_0062	N	N
DSC_0063	N	N	DSC_0063	N	N
DSC_0066	N	N	DSC_0066	N	N
DSC_0072	N	N	DSC_0072	N	N
DSC_0075	N	N	DSC_0075	N	N
DSC_0079	Y	Y	DSC_0079	N	N
DSC_0083	N	N	DSC_0083	N	N
DSC_0087	N	N	DSC_0087	N	N
DSC_0091	N	N	DSC_0091	N	N
DSC_0107	Y	Y	DSC_0107	N	N
DSC_0121	N	N	DSC_0121	N	N
DSC_0148	Y	Y	DSC_0148	N	N
DSC_0171	Y	N	DSC_0171	N	N
DSC_0175	Y	Y	DSC_0175	N	N

DSC_0180	Y	Y	DSC_0180	N	N
DSC_0390	Y	Y	DSC_0390	N	N
DSC_1228	N	N	DSC_1228	N	N
DSC_1231	N	N	DSC_1231	N	N
DSC_1234	N	N	DSC_1234	N	N
DSC_1655	N	N	DSC_1655	N	N
DSC_1660	N	N	DSC_1660	N	N
DSC_1661	Y	Y	DSC_1661	N	N
DSC_1664	N	N	DSC_1664	N	N
DSC00188	Y	Y	DSC00188	N	N
DSCN4814	N	N	DSCN4814	N	N
DSCN4980	Y	Y	DSCN4980	N	N
Elk3	Y	Y	Elk3	N	N
Elk5	N	N	Elk5	N	N
IMG_0205	N	N	IMG_0205	N	N
IMG_2768	N	N	IMG_2768	N	N
IMG_2769	N	N	IMG_2769	N	N
IMG_2770	N	N	IMG_2770	N	N
IMG_2771	N	N	IMG_2771	N	N
IMG_2772	N	N	IMG_2772	N	N
IMG_2773	Y	Y	IMG_2773	N	N

IMG_2774	Y	Y	IMG_2774	N	N
IMG_2775	N	N	IMG_2775	N	N
IMG_2776	N	N	IMG_2776	N	N
IMG_2779	N	N	IMG_2779	N	N
IMG_5974	Y	Y	IMG_5974	N	N
MammothSprings	N	N	MammothSprings	N	N
MiniGeyser4	N	N	MiniGeyser4	N	N
More Buffalos	N	N	More Buffalos	N	N
P1010048-1	N	N	P1010048-1	N	N
P1010078-1	N	N	P1010078-1	N	N
P1020029-1	N	N	P1020029-1	N	N
P9160009	N	N	P9160009	N	N
P9170013	N	N	P9170013	N	N
P9170022	N	N	P9170022	N	N
P9170025	N	N	P9170025	N	N
P9180040	N	N	P9180040	N	N
P9210122	Y	Y	P9210122	N	N
P9220174	Y	Y	P9220174	N	N
P9220207	Y	Debatable	P9220207	N	N
P9230407	Y	Y	P9230407	N	N
P9270708	N	N	P9270708	N	N

Pictures 030	N	N	Pictures 030	N	N
Pictures 069	N	N	Pictures 069	N	N
Pictures 451	Y	Y	Pictures 451	N	N
Pictures 482	N	N	Pictures 482	N	N
Pictures 490	N	N	Pictures 490	N	N
Pictures 492	N	N	Pictures 492	N	N
Pictures 508	N	N	Pictures 508	N	N
Roosevelt1	N	N	Roosevelt1	N	N
September 2009 001	N	N	September 2009 001	N	N
September 2009 048	N	N	September 2009 048	N	N
September 2009 066	N	N	September 2009 066	N	N
September 2009 069	N	N	September 2009 069	N	N
September 2009 072	N	N	September 2009 072	N	N
September 2009 076	N	N	September 2009 076	N	N
September 2009 078	N	N	September 2009 078	N	N
September 2009 080	N	N	September 2009 080	N	N
Smoke	N	N	Smoke	N	N
Viewof UpperFalls	N	N	Viewof UpperFalls	N	N
YellowstonRiver	N	N	YellowstonRiver	N	N