Fall 2011

The Dangers of Digital Imaging

Russel Laska
Governors State University

The Dangers

of

Digital Imaging

Russel Laska

Spring 2011

IFDI MFA Program

Thesis Paper

In today's world, photography takes on a whole different meaning that it did 20-30 years ago. Whereas terms such as photograph and graphic used to have separate meanings that classified them from one another, these and many similar terms have been melded together to represent the same thing... a computer image. Due to the jump in technology over the past 10 years alone, digital cameras went from flashy novelties to a strong industry standard in photography, and swift computer alteration of photographs and images began with a very small amount of people to practically everyone who has a computer today. The digital revolution is now upon us, basically leaving analogue film for the die-hard nostalgic artists that once believed that film could never be replaced by digital images, but as it seems today, this swap of digital over analogue has definitely become reality. With this digital takeover at our feet, there is a very real threat of the lines between reality and trickery being blurred, and a considerable amount of information that we all need to be aware of. The dangers of digital imaging are all around us, slowly escalating in potency, and what we see now in the world today is only the beginning.

"A Photograph doesn't lie". This was a popular term in the past to verify that if it was captured by a camera, then it had to be true. Perhaps at one point in time (most likely over a century ago) this was a valid term, but nowadays this could not be further from the truth – in fact, it holds as the exact opposite. Even back over a half century ago, such dictators such as Hitler and Stalin had photographs altered to suit their own agenda. Any photograph that had any negative reflection on these leaders was manipulated. Here is what an article in Scientific American by Hany Farid states about the history of photographic manipulation:

“History is riddled with the remnants of photographic tampering. Stalin, Mao, Hitler, Mussolini, Castro and Brezhnev each had photographs manipulated--from creating more heroic-looking poses to erasing enemies or bottles of beer. In Stalin's day, such phony images required long hours of cumbersome work in a darkroom, but today anyone with a computer can readily produce fakes that can be very hard to detect.” *(Farid, Hany. "DIGITAL IMAGE FORENSICS." Scientific American p.66)*

Looking back, it is quite remarkable that simply the idea to alter photographs came to mind, let alone being able to carry out the task convincingly. It shows that the devious intentions to manipulate images began long before the age of computers, and most likely long before anyone took it into serious consideration and made it happen.

Before the modern-day technology of manipulating images as we know it today became a reality, there have been many events that have led us up to this point. From the earlier referred deception of tyrannical dictators, to the latest frauds that have made headlines (which have eventually blackballed dishonest photographers and photojournalists from ever working in serious media photography again), history is packed with endless examples of just what people will do to trick or deceive the public. Whereas the intentions mainly stayed the same, the techniques in doing so have changed drastically with the leaps in technology that our world has seen. Until just over 20 years ago, practically any photographic manipulation was done by hand. It was tedious and time-consuming, but in order to pull off a convincing phony, you had to be very skilled with a lot of experience under your belt. However, with today’s technology, just about anyone with a computer has some type of photo editing software that allows them to easily

change any photo in just a few simple steps. This is a far cry from in the past, when hours or days of work needed to be put into a photograph to achieve a desired result intended to fool any viewer.

Today's computer technology has advanced in ways that was only a dream several decades ago. Not only has digital *photography* jumped in technology, but the advances in manipulating imagery - whether it is a photograph, drawing or a computer-generated image - has made revolutionary advances as well. This is all due to computer applications that specialize in photo editing. There are many different types of photographic and image-based editing programs available to the public today, which are quite affordable as well, but one stands out as the pioneer and industry standard when it comes to manipulating imagery. I am of course referring to Adobe Photoshop. In my personal opinion (and many graphic designers would agree with me), there is no substitute or comparison - and although many other programs are increasing in competitive features, Photoshop still remains the leader of the pack with all other programs left behind in the swills of mediocrity.

In 1990, Adobe released the very first version of Photoshop exclusively for the Apple Macintosh, which began as a simple image editing program. Since the first version, several versions and updates have been released for both the Macintosh and Windows-based computers. The latest release, Adobe Photoshop CS5 (version 12) has incredible capabilities to manipulate imagery, compile complex compositions, work with 3D images, and even create small

animations. Every new upgrade or version that Adobe releases for Photoshop includes additional tools to assist and speed up the editing process. These numerous additions to the program since the very first version of the program makes it that much easier and user friendly for just about anyone to pick up very quickly on how to alter any image. While these advances in the software application does wonders for those who are in the digital artistry field, such as graphic designers, it also opens the door for a wide range of people who see a different type of opportunity besides using the program for strictly business.

Before this program was invented, manipulating images and photographs was quite the task. As stated earlier in Scientific American, in Stalin's day, it took "long hours of cumbersome work in a darkroom", but as the decades passed, and graphic design progressed, the task of creating a fake image became much more challenging to pull off with any sign of authenticity. What would take a half an hour or so on Photoshop nowadays, could easily take a graphic designer a number of hours or even days to complete just 20 years ago. Instead of physically cutting, pasting, masking, and many other tedious methods, Photoshop creates a digital atmosphere where the designer can easily complete these same tasks in a fraction of the time, effortlessly rearrange, refine or even quickly undo actions if the desired result is not achieved. All this can be done relatively quickly, and without destroying any original material. The original file can be copied and archived several times without degrading quality what-so-ever, due to the binary code, which writes these digital files in 1's ond 0's.

Photoshop has had such a powerful impact on society, that terminology regarding the program has been created exclusively for describing the application's graphic manipulation. Many advanced users can manipulate images to the point where there is no recognition that the image has been tampered with; but if even the slightest doubt exists, the image is usually labeled with the term “Photoshopped” , and I have even heard just "shopped". Many photographs that are taken in today's world are "photoshopped", which basically means that if there is any flaw in the photograph, then it is simply corrected, which is easily executed. Blemishes, scars, stains on clothing... plus any other imperfections are usually taken out to give people the perfect version of themselves. If someone wants to take a family picture, and all family members are not present, then they can just be "photoshopped" in. The possibilities of this powerful technology are literally endless, but this does not necessarily mean that the possibilities are always harmless or used for good intentions.

Most of the world uses Photoshop to manipulate photographs or create images that are found in advertisements, magazines, on the web… for example, it can be safely assumed that any magazine cover, and even photographs within any magazine have been doctored to fit an idealistic perception of what the photograph should look like. If a magazine cover model has a little darkness under her eyes, or if her thighs seem a bit too large, then changing the image so that the model comes across perfect is only a few brush strokes away. There have been fashion models who have come forth and even admitted to their photographs being airbrushed. However, with the use of this technology at one’s fingertips, the question needs to be raised – at what point does digital imaging defeat the purpose of reflecting that fraction of a second in time?

It may seem like a very minor act (perhaps because our society is so used to it), but something as simple as the manipulation of a photograph has such an impact on our lives. The original photograph should stand for a representation of a moment in time, but by changing it, we create a lie. It may not come off as that big of a deal, but when everything around us is constantly manipulated to make that moment more flattering, we are all lying to ourselves and to everyone around us when we make a small and seemingly insignificant adjustment to a photograph. For example, if a photograph is taken of a man who has a permanent scar on his cheek, and the scar is removed using photo editing software, then it immediately becomes a lie. It re-writes history. The original photograph stood as a replication for others to view, and now has displaced the time in which that the photograph could have been taken. There is no purity in this media anymore; it is all fake. I even look around my own home, and every photograph that hangs on the wall has been imaged to suit my own approval. In my opinion, it seems that it is a sickness that has spread out in the world that no photograph is good enough until it meets the standard of near perfection.

Although it was known that this type of technology was available, it was slowly uncovered that people were using these applications to deceive people on an unethical level. At the turn of the 21st century, when Photoshop really began to become a widely recognized program, not everyone knew its powerful capabilities, and there were some who took advantage of this. In an article written for Pediatric Dermatology in 2001, it warned of a future where respected institutions such as science and medical communities would utilize fraudulent images, and that it may have already been happening. This is a definite concern, for forgery of results, or

simply the enhancement of an image can be extremely misleading, and in some cases, very dangerous. Here is what Pediatric Dermatology had to say about this dilemma, which was just 10 years ago:

"The possible use of retouched images for fraudulent purposes in scientific articles, posters and conferences is not a future but a present possibility (probably already used) that poses serious questions as to the need for additional control mechanisms other than scientific peer quality review in evaluating and accepting articles."

Cutrone, Mario, and Ramon Grimalt. "The True and the False: Pixel-Byte Syndrome." Pediatric Dermatology 18.6 (2001)

Scientific fraud has been ongoing for quite some time, but up until this point in time, it was extremely difficult to produce fraudulent imagery that could pass very heavy judgment. Before the current digital manipulation, unless an image was obviously flawed due to an attempt to manipulate it, the thought of it being a possibility would probably never cross the minds of most people. However, this is not the issue today – rather the exact opposite – perhaps the first thing to come to mind today is if in fact an image has been altered in any way, and even if it passes judgment, the skepticism usually still remains about the image.

In the art world, photographs are typically exaggerated to the point where manipulation is obvious. Surrealistic and painterly-quality images are created as works of art and sold in galleries. However, I myself tend to use the imagery to blend different scenes with contrasting elements to purposely trick the viewer into believing that these separate photographs are not separate at all, but actually taken at the same time, and the composited scene actually exists in

real life. I do not intend to maliciously fool people for profit or gain, yet merely to pull emotion and thought from the viewer, and to make them contemplate these contrasting images and how they relate to each other. Never-the-less, every piece I produce is nothing more than a lie in itself.

Whereas I do not wish any harm to come from my photographs, there are those who use photo editing as a means for pure deception. There have been many accounts of fraudulent photographs being submitted by all different types of people with different occupations. There have been photojournalists that have submitted fake images to win awards, criminals manipulating images to cover up a crime, and political activists that wish to bash an opposing candidate. Such images can easily appear in newspapers or magazines, are distributed over in the internet on websites, or circulated through emails to billions of people worldwide. Even with the renowned knowledge that digital imaging can alter any photograph, it is amazing how people will ignore the facts, and accepts images and photographs as truth without proceeding with any kind of skepticism.

As far as legitimate news is concerned, despite their strongest efforts, they frequently fall subject to a manipulated photograph. As there are many cases – too many to mention, I would like to bring light to just a few for exemplary purposes, to expose the nature and motivation of people submitting phony imagery to legitimate news establishments. Here is one example of a

fraudulent photograph making it into the news, and the aftermath, when the photographer and editor were basically blackballed from the industry:

"Barely a month goes by without some newly uncovered fraudulent image making it into the news. In February, for instance, an award-winning photograph depicting a herd of endangered Tibetan antelope apparently undisturbed by a new high-speed train racing nearby was uncovered to be a fake. The photograph had appeared in hundreds of newspapers in China after the controversial train line was opened with much patriotic fanfare in mid-2006. A few people had noticed oddities immediately, such as how some of the antelope were pregnant, but there were no young, as should have been the case at the time of year the train began running. Doubts finally became public when the picture was featured in the Beijing subway this year and other flaws came to light, such as a join line where two images had been stitched together. The photographer, Liu Weiqing, and his newspaper editor resigned; Chinese government news agencies apologized for distributing the image and promised to delete all of Liu's photographs from their databases."

(Farid, Hany. "DIGITAL IMAGE FORENSICS." Scientific American p.66)

This type of scandal is uncovered all the time… however, who is to say that everyone who tries to trick the public is caught? I myself can imagine that there have been countless images that have made it past the scrutiny of the public and Photoshop experts as well. There have been photos that I myself could not detect any manipulation with the naked eye, and needed to see the image with a magnifying glass, or the original document on the computer screen fully zoomed to even begin to figure out what was done to alter the photograph.

Sometimes the manipulation of a photograph does not call for, nor even need excruciating work done to it to cover up the flaws… in fact, there are many cases where the

flaws are hidden in plain sight. This brings to mind one of my own experiences when I worked on my wife's family picture a few years ago. There were 14 people in the photograph, and as in pretty much any picture with a group that large, there was not one picture where everyone had a smile. However, throughout the 5 or 6 photographs taken, I saw an opportunity to take faces from one photograph and meld them with the smiles and better expressions on the family members' faces from another photograph. In doing this, I used what is called a *layer mask*. This is a very handy tool in Photoshop, and one that some people probably can't remember living without.

The way the layer mask works in Photoshop is by placing one photograph over the other on different layers, and "mask out" the not-so pleasant faces in the photograph. This is done by creating the layer mask, and then using the brush tool in Photoshop to "erase" the face from the top photograph, which uncovers the face from below. The reason why "erase" has quotation marks around it, is because you are in fact not erasing anything… you are actually hiding the face, and if you would like to replace it, then you can simply change the color of your brush and add it back… so this is a form of non-destructive editing. This is one technique that has made stitching two photographs together seamlessly extremely hard to detect, as was not the case in Liu Weiqing and his editor's mistake in leaving a flaw like that apparent to the naked eye.

After using the layer mask to mask out the faces in my wife's family picture, I refined the masks to the point where there were no apparent seam lines, and everyone in the photograph had a pleasant smile and expression on their face. However, when scrutinizing the photograph for

any flaws, I nearly missed the biggest flaw (and the only visible flaw) in the entire photograph, which was literally right in front of me. During the photo shoot, my wife's mother was holding a pair of sunglasses. At one point during the photo shoot, she had placed those same glasses on her head. So in one photograph, she was holding the sunglasses, and in another, they were on her head… and when I masked out her face, I revealed the shot with the glasses on her head, but in the original photo, she was holding them. This resulted with a family picture of my wife's mother holding her sunglasses, while simultaneously wearing that same pair on her head.

To this day, not one person who has viewed the family photograph (which is hanging in the living room of my wife's parent's house) has been able to discover the flaw by themselves, even with many hints to guide them. Even though harmless and quite humorous, this type of imaging is a perfect example of displacing time. Just as in the apparent time flaw in Liu Weiqing's composition with the antelopes being pregnant, only it was the wrong time of year, time displacement can be an effective tool for pinpointing a fake photograph. But what happens when someone creates a perfectly imaged photograph without any time issues? There are several other ways of determining the authenticity of a photograph – some happen by pure chance. In Scientific American, here are a few examples of photographic manipulation, and ways they have been discovered:

"Brian Walski was fired by the Los Angeles Times in 2003 after a photograph of his from Iraq that had appeared on the newspaper's front page was revealed to be a composite of elements from two separate photographs combined for greater dramatic effect. A sharp-eyed staffer at another newspaper noticed duplicated people in the image while studying it to see if it showed friends who lived in Iraq. Doctored covers from newsmagazines Time (an

altered mug shot of O. J. Simpson in 1994) and Newsweek (Martha Stewart's head on a slimmer woman's body in 2005) have similarly generated controversy and condemnation."

(Farid, Hany. "DIGITAL IMAGE FORENSICS." Scientific American p.66)

These are only a few examples of digital deception that have hit the headlines… one can only imagine that cases such as these are in such high numbers that volumes of encyclopedias could be filled with the amount of fraudulent photographs and the stories that surround them. What makes these examples unique is that there was no mention of finding any flaws from sloppy manipulation (cutting, pasting or stitching photographs together). In the first one, it was overlooked that there were duplicate people in a huge crowd (easy to miss when you've been working on a composition for a long time, staring at a computer monitor for too long – similar to my sunglass situation), and when it comes to famous people, usually the original photograph will surface somewhere, easily proving the falsehood of the altered image.

The author of this article in Scientific American, Hany Farid, is what you would call a digital forensic expert. He specializes in ultimately verifying the authenticity of an image or photograph. He has dedicated the last decade to locating and exposing digitally altered images, even testifying in court, and has recently developed a computer program to detect inconsistencies in altered photographs, which is explained more in depth in later pages. In addition to the methods already explained, Farid also describes many other ways to determine the legitimacy of a photograph. Such techniques include inconsistent lighting, eye position, eye shape, perspective

of the iris, and specular highlights. When looking at a photograph, the lighting can be a huge tell – tale as to if something has been imaged. The example he uses is a head cut and pasted onto a body with two obvious different light sources. Some examples can be obvious, yet there are some that are more challenging. Also, there is a wide range of color temperature that can affect an image, so even if you shoot several images on the same day and try to composite them into one image, the light may change over time, and the temperature might even have changed enough to trigger someone's attention.

Eyes can also tell a lot about a photograph. The position of the eye in relationship to the camera can be a dead giveaway if you are moving someone into a picture from another photograph, or even if you move that person far enough over within the same photograph. Hany Farid says many things about the eyes regarding authenticity of a photograph:

"Because eyes have very consistent shapes, they can be useful for assessing whether a photograph has been altered. A person's irises are circular in reality but will appear increasingly elliptical as the eyes turn to the side or up or down."

"Surrounding lights reflect in eyes to form small white dots called specular highlights. The shape, color and location of these highlights tell us quite a bit about the lighting."

(Farid, Hany. "DIGITAL IMAGE FORENSICS." Scientific American p.66)

However, photographs are not the only images to be altered using Photoshop, and although Photoshop is the most popular (and considered the best by most experts), Adobe does

make many other multimedia applications that can manipulate not only photographs, but documents as well. For example, Adobe Illustrator is a drawing program that creates non-pixel images called vector images. Pixels are basically very small dots that can eventually be broken down to the individual pixel (found in photographs – raster images), whereas vector images are mathematical calculations that make up the image, and there are no pixels, so there is no limit to how large the image can be enlarged without losing quality. This comes in handy when certain documents need cleaner and more exact shapes to mimic the original document.

With this in mind, this opens a whole new realm of digital deception. Things such as birth certificates, car titles, insurance papers, social security cards, drivers licenses, passports… and just about any other important document in this world can be easily duplicated. Of course, the more difficult the duplication, the more experience is needed of the person, but I myself have known people personally who have crossed the law in this area and have learned how serious of an offense it is. Just before the state of Illinois changed the format of their driver's licenses and state ID's, a friend of mine (who has asked to remain anonymous, so I will refer to him as Joe) was in the business of creating fake ID's for college students. At first, it started out with him just helping some underage friends get into bars (because at the time he was the only one experienced enough in Photoshop to pull off a fake ID), but soon the word spread of his abilities, and Joe saw a huge opportunity to make some money. Business was running very smoothly, until the FBI showed up at his door and confiscated Joe's PC and all the equipment that he used to create these fake documents.

In this case, the motivation was greed. It appeared as an easy way to make a quick buck, but at a huge risk. If Joe hadn't been arrested back then, he may have explored forging other documents, and instead of receiving the lenient sentence the judge graced him with (he did no prison time, just a fine and community service), he perhaps may have had to serve a few years in jail because of it and had a major conviction on his record. It might be considered by some that this is a 'victimless' crime, but laws are put in their place to protect citizens, and not necessarily to restrict them… people often forget this. If one of those underage college students visited a bar, and was granted entry due to one of Joe's fake ID's, then it could have caused serious complications. That student could have become severely intoxicated, and decided to drive a car home. At that point, a plethora of turmoil could ensue; that student could crash into another car, a light post, hit pedestrians… and then there would be the aftermath and consequences of these actions. It's the domino effect, and situations like this can be avoided by simply not creating the fake ID in the first place – and although Joe's intent was not malicious, the results can open themselves to be devastating never-the-less.

On a much larger scale, the latest digital imaging scam that has hit the news on a world-wide scale in recent weeks goes all the way to the top of the United States of America's government… the president. There has been much debate about whether or not president Barrack Hussein Obama is actually an American-born citizen. He has been accused several times of being birthed in Kenya, and has constantly denied this claim. He insists he was born in Hawaii, and has just released his long-form birth certificate recently. According to the NY Times, the reason for this long delay in releasing the certificate was because:

“President Obama said he had decided to release his full birth certificate because the country did not have “time for this kind of silliness.”

Shear, Michael D. “Obama Releases Long-Form Birth Certificate.” NY Times, April 27, 2011

The birth certificate is currently released on a website for all to view, and since its release, it has been torn apart by Photoshop experts everywhere. Several bloggers and political activists have pumped the internet full of videos and outraged editorials, claiming that the birth certificate is a fraud, and display exactly why it is a fraud. The videos show these ‘Photoshop experts’ downloading the document straight from the government website, they open it in Adobe Illustrator, and it reveals that there are several layers compiling the entire image. There are also many television shows and internet shows that have political commentary, assisted by the demonstration of a Photoshop expert to show the faulty nature of the document.

While demonstrating the different layers of the document does in fact show that the image definitely has been compiled from several different images and text layers, the greater question here would be: Is this the actual image released by the White House? There is not only the possibility that the document that is up for debate was in fact released by the White House, but many other possibilities as well – none which have anything to do with the validity of the birth certificate itself. The website could have been hacked, and the document replaced with a faulty one, the website could have been re-directed to a completely different, identical site with the altered document waiting for people to download it and stir up controversy... after all, if

these are Photoshop experts, then what would stop them from creating a fake website and purposely sabotaging the birth certificate to make it look like it came from the White House this way? This goes beyond simply detecting if a document or a photograph is authentic or not… this intensifies the already growing problem into a larger and more psychological dilemma. Who's to say that the White House did not purposely release the fake document in order to deliberately generate several conspiracy theories amongst the public, so that nobody knows what to believe?

Conspiracy theories aside, when using this information, along with the several previous methods for detecting phony images, it is quite possible to easily detect a fake when it presents itself. This is, of course, if the person altering the image makes any of these mistakes. What if every single element in the photograph that has been tampered with has been successfully executed to the point where experts cannot even use these traditional techniques? Due to the escalating problem with difficulties in determining the validity of a well done manipulation, there are many new techniques out there that have recently been developed. The continual advancements in the digital revolution have demanded the need for cameras to generate watermarks and computer programs that create mathematical algorithms to help aid in the ongoing struggle of determining if a photograph is original, or manipulated.

As mentioned in earlier, Hany Farid had explained many different techniques for uncovering inconsistencies in photographs, and one method was referred to as an 'algorithm'. This is basically a mathematical system developed to compare pixels in a photograph, which

exposes inconsistencies in the relationship between original pixels and pixels that have been altered in some way. Here is a better explanation of how it works:

"The operation results in a correlation of each pixel with its neighbors; however, the amount of correlation is not uniform, but varies periodically across the lattice. What the Dartmouth researchers have done is to apply an algorithm – called an expectation/maximization (EM) algorithm – that reveals resampled areas by determining the amount of correlation each pixel has with its neighbors."

Wallace, John. "Algorithm detects non-watermarked digital forgeries." Laser Focus World 40.10 (2004): 17-20.

Many advances have been made since, including a full-blown computer application specifically engineered to detect digitally altered images. It was created by Hany Farid in 2010, who has been at the forefront of research on this topic with his team at Dartmouth College in Hanover, NH. Farid claims that this application is "like gun ballistics", meaning that just like a gun makes a distinctive mark on a bullet, this program can not only determine if the image has been altered, but also what make and model of what camera captured it.

"Farid and his students received permission from photo-sharing site Flickr to download millions of images and build a signature database of every one of the 10,000-plus digital camera models ever made. To verify a picture, Farid's system checks it against that database to identify the equipment used. It then looks for any variations in the signature, which would indicate fakery. If the system finds traces of Adobe Photoshop (ADBE), which also leaves a signature (and is the most common image manipulation program), that's a sure sign of picture alteration."

Staley, Oliver. "Hany Farid vs. Photoshop." Bloomberg Businessweek. Innovator. December 29, 2010

This appears to be an extremely valuable tool that would assist law enforcement agencies that need validation for admissible photographic evidence for court cases, and newspapers and magazines which also need verification of authenticity for photographs from photojournalists. However, it is only a matter of time before someone figures out how to defeat the program. This means that the application will need frequent updates with the latest camera releases, and be able to identify the latest trends in covering up images so that the program will not see it. Also, the application does seem to be geared more towards determining alterations made in Adobe Photoshop… there are several other applications that can be used, which are free to the public, such as freeware rival Gimp. Gimp is a photo editing application similar to Photoshop, however, it is free of charge and available for download at any time. Whereas it does not have the full power that Photoshop does, this program and other rivals do offer several of the same tools used to manipulate any image.

Never the less, this application is a step in the right direction, regardless of people developing ways around it. As mentioned earlier, the problem with photojournalism cranking our faulty photographs is everywhere we look, and photographic evidence in courtrooms is always up for debate on whether or not it is real. This presents a very precarious situation, because when evidence of this nature is crucial to a court case, the outcome of someone's verdict could be based on not only whether or not the photograph is in fact authentic, but if an expert can indeed prove that it hasn't been altered. So seeing how photographic evidence can serve justice

where it is needed, making a mistake judging a photograph could either put an innocent man in jail, or a criminal back on the streets.

Since the lines tend to be blurred on what is acceptable when adjusting an image to make it more pleasant or viewable, there are certain rules and guidelines when it comes to submitting photographic evidence for a court case; which is the same as in the scientific and medical communities, when submitting a photograph for an article, or as supporting proof in a theory. According to Law Practice Today, there are other digital signatures other than the in-depth search program that Hany Farid created. Although Farid most likely included this type of signature in his application, the metadata from JPEG and RAW digital camera files can be analyzed to determine if the file has been tampered with. Whereas RAW files are generally very difficult to alter without disturbing the metadata, JPEG files (the most commonly used in the consumer market) can be easily manipulated and passed off as original by most Photoshop users. Below is actual example of 'Evidence Rules" for submitting a digital photograph for evidence in court. This excerpt is from an article in *Law Practice Today* by Joe Kashi:

"Under Evidence Rules 1001 through 1004, an "original" document (including a photograph) is required to prove the truth of the facts for which any document is offered. However, over many years, the definition of an "original" has been greatly expanded, particularly with regard to electronically stored information, and the requirement for an "original" is honored more in the breach than to the letter. Indeed, duplicates, including electronically made prints or digitally identical electronic file duplicates, are typically admissible to the same degree as an original document unless admitting the duplicate would prove inaccurate or unfair."

"However, when photographs are to be used as the basis for expert witness testimony or to actually prove the existence of an allegedly depicted condition, then they will be held to a

higher standard and you will need to be much more cognizant of subtle technical and photographic parameters."

Kashi, Joe. "Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata." Law Practice Today. June, 2006

In general, photographic evidence that has been altered can be submitted as well… however, the same rules apply – as long as it is not meant to deceive or be misleading. Photographs may need to be adjusted for exposure, contrast and color correction before they are able to be viewed as evidence. Also, key points of the photograph may be highlighted to signify an important part of the photograph. These adjustments are allowed, as long as the photograph is accompanied by a list of all alterations that were performed and accepted by the court.

Another area for scrutiny in admitting a photograph as evidence would be the timeframe in which the photograph was taken. Since digital cameras leave a timestamp in their digital signature, then it is apparent as to exactly the time and day when the photograph was taken. This is where the metadata comes in really handy, and there are laws in the works today that will require the metadata to be available in case the court needs access to this information:

"It appears that the new federal rules will also generally require the production of an electronic file's "metadata," that is, the electronic file's internally stored information about the creation and alteration of any electronic file. Although privilege reviews will become more complex when you must produce metadata, the production of document metadata may be the most readily available, although not entirely fool-proof, means of determining the authenticity or alteration of electronically stored photographs. Most native format files,

including the JPEG photographic files made by most modern digital cameras, will include the document's metadata unless it is rather obviously stripped out with one of the numerous metadata removal programs now on the market."

Kashi, Joe. "Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata." Law Practice Today. June, 2006

Metadata is a great way to determine a photograph's authenticity, but once again, where the photograph comes from creates another issue. A lawyer who has photographic evidence from what the police have gathered, opposed to a defense attorney who has attained his photographic evidence from an expert witness presents two sides of the spectrum. Whereas the police would not typically tamper with evidence, an expert witness who is being paid to testify may just alter the metadata to help the defendant's case. Whether or not the person is guilty is besides the point… when the decision is made to alter a photograph that will be used as evidence that could sway a jury – no matter what the justification – it becomes a huge ethical issue and may just destroy someone's life, even if they're innocent. In addition, although police do not *typically* tamper with photographic evidence, the prosecution just may want to see the defendant behind bars at any cost and hire their own expert witness…

The amount of problems that can and have been created by digital imaging are staggering, and we are still only in its infancy. Perhaps one of the biggest downfalls we face in image manipulation is skewing our history to such a degree that our future generations misunderstand our images and documents and can never stitch together a clear picture of what their history really was. As stated earlier, altering the timeline may seem miniscule right now,

but over the course of decades, it can build up to furnish history to become on huge lie. In 2007, Scot Macdonald warns of the dangers that may come of our ability to seamlessly image any image (or video for that matter) in his book "Propaganda and information warfare in the twenty-first century: Altered images and deception operations":

"Technology will soon provide the ability to alter images perfectly with little or no chance of detection, especially if the time frame for analysis of the image is short, such as during an election campaign or a foreign policy crisis. When that point is reached – if it has not been reached already, the quality of an alteration will depend solely on the skill of the manipulator, and some of them will be exceptionally talented. When the combined with the capability of television and the Internet to disseminate images rapidly around the world, the future for the use of altered images for propaganda and deception operations in politics, diplomacy, espionage and warfare is wide open, unstudied and rife with threats."

Macdonald, Scot. "Propaganda and information warfare in the twenty-first century: Altered images and deception operations." Routledge. New York, NY, 2007

What makes this statement remarkable is that it was written in 2007. I can only imagine what attitudes and opinions Macdonald has with the leaps in technology that has led us to today's predicament. In his book, Macdonald goes in very deep detail about the past, and how propaganda has used deception in imagery (and other forms of multimedia) to promote policies in government, and to sway voters one way or another. He is correct when mentioning that the shorter period of time to analyze a photograph and determine its eligibility really matters – because if it is not proved fast enough, even though it may be a fake, people may be leery to believe the proof (no matter how convincing) if it is after the fact.

It definitely appears as though the future of digital imaging is uncertain. As technology escalates, so does our multimedia capabilities, and the methods to manipulate that media. Also, this does not solely point to photography alone; this includes video and audio as well… and soon enough, virtual reality will most likely become an issue. It all points to a world in where nobody can trust anything they see, read or hear – much like the world we live in today, however, I anticipate it will be much worse. The lies we create today will eventually confuse our future generations, and psychologically change their perception of how we lived. People may become confused in their own worlds, not knowing what is real or fantasy. There will always be that temptation to change even the smallest flaw in a photograph, or to alter an image to get away with something – or to sway public opinion. Even though the methods to combat the fake representations of life become stronger as the digital revolution evolves, there will always be those who will battle back to preserve their deceitful nature. Where the future is headed regarding digital imaging is definitely uncertain, but we can only hope that regiment is placed on this industry for the sake of our sanity and the generations of our children to come.

Works Cited

Works Cited

Farid, Hany. "DIGITAL IMAGE FORENSICS." *Scientific American* 298.6 (2008): 66. *MAS Ultra - School Edition*. EBSCO. Web. 20 Apr. 2011.

Works Cited

Prince, Patric D. "Imaging by Numbers: A Historical View of Digital Printmaking in America." *Art Journal* 68.1 (2009): 90-103. *Advanced Placement Source*. EBSCO. Web. 27 Apr. 2011.

Works Cited

Crepeau, Philip J. "Photo Inspection . . . A Key Player In Averting Vehicle Insurance Fraud." *Insurance Advocate* 114.36 (2003): 22. *Advanced Placement Source*. EBSCO. Web. 27 Apr. 2011.

Works Cited

Cutrone, Mario, and Ramon Grimalt. "The True and the False: Pixel-Byte Syndrome." *Pediatric Dermatology* 18.6 (2001): 523. *Advanced Placement Source*. EBSCO. Web. 3 May 2011.

Works Cited

Wallace, John. "Algorithm detects non-watermarked digital forgeries." *Laser Focus World* 40.10 (2004): 17-20. *Advanced Placement Source*. EBSCO. Web. 3 May 2011.

Works Cited

Shear, Michael D. “Obama Releases Long-Form Birth Certificate.” *NY Times*, April 27, 2011

Works Cited

Staley, Oliver. “Hany Farid vs. Photoshop.” *Bloomberg Businessweek. Innovator*. December 29, 2010

http://www.businessweek.com/magazine/content/11_02/b4210037408918.htm

Works Cited

Kashi, Joe. “Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata.” *Law Practice Today.* June, 2006

http://apps.americanbar.org/lpm/lpt/articles/tch06061.shtml

Works Cited

Macdonald, Scot. “Propaganda and information warfare in the twenty-first century: Altered images and deception operations.” *Routledge.* New York, NY, 2007