




Detection of Overlapping Passive Manipulation Techniques in Image Forensics

Gianna S. Lint
Purdue University

Umit Karabiyik
Purdue University

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Aviation Safety and Security Commons](#), [Computer Law Commons](#), [Defense and Security Studies Commons](#), [Forensic Science and Technology Commons](#), [Information Security Commons](#), [National Security Law Commons](#), [OS and Networks Commons](#), [Other Computer Sciences Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Scholarly Commons Citation

Lint, Gianna S. and Karabiyik, Umit, "Detection of Overlapping Passive Manipulation Techniques in Image Forensics" (2022). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 4.
<https://commons.erau.edu/adfsl/2022/presentations/4>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



DETECTION OF OVERLAPPING PASSIVE MANIPULATION TECHNIQUES IN IMAGE FORENSICS

Gianna S. Lint¹, Umit Karabiyik²
Purdue University
Computer and Information Technology
West Lafayette, IN 47907, United States
¹glint@purdue.edu, ²umit@purdue.edu

ABSTRACT

With a growing number of images uploaded daily to social media sites, it is essential to understand if an image can be used to trace its origin. Forensic investigations are focusing on analyzing images that are uploaded to social media sites resulting in an emphasis on building and validating tools. There has been a strong focus on understanding active manipulation or tampering techniques and building tools for analysis. However, research on manipulation is often studied in a vacuum, involving only one technique at a time. Additionally, less focus has been placed on passive manipulation, which can occur by simply uploading an image to a social media site. This research plots the path of an image through multiple social media sites and identifies unique markers in the metadata that can be used to track the image. Both Facebook and Twitter were utilized on both phone and web applications to fully understand any differences between direct and secondary uploads. A full metadata analysis was conducted including histogram and size comparisons. This paper presents several differences and unique metadata findings that allow image provenance to be traced to an original image. This includes a review of IPTC, ICC, and EXIF metadata, ICC profile and Color Profile Description, Encoding Processes, Estimated Quality Values as well as compression ratios. A checklist of variables is given to guide future evaluations of image provenance.

Keywords: Image Forensics, Metadata Analysis, Image Manipulation, Forensic Intelligence, Provenance, Social Media

1. INTRODUCTION

On average there are 1.8 billion images uploaded daily to social media sites such as Facebook, Instagram, Flickr, Snapchat and WhatsApp (Edwards, 2014). Images that are uploaded to social media sites are increasingly used in forensic investigations resulting in an emphasis on building and validating tools capable of detecting manipulated images (Fan, Cao, & Kot, 2013).

In recent years, social media has become a hub for the transmission of viral information and it has become imperative to build tools that al-

low us to validate the information within any piece of digital media (Pasquini, Amerini, & Boato, 2021). Digital image forensic techniques have provided information regarding the origin and truthfulness of an image as well as information regarding potential manipulation techniques that have been performed on the image (Bayram, Avcibas, Sankur, & Memon, 2006). In addition, research into image manipulation by way of uploading to social media has identified some of the mechanisms in which specific websites act upon the images that are uploaded (Moltisanti, Paratore, Battiato, & Saravo, 2015).

However, there seems to be a gap in understanding if these forensic tools are capable of differentiating between multiple sources of manipulation (Thakur & Rohilla, 2020). Manipulation techniques appear to be studied in a vacuum, one at a time, and validation of a tool is deemed successful only when the manipulation is identified vs. a non-manipulated image. It is however much more realistic to expect multiple forms of manipulation, thereby opening the possibility of hiding purposeful manipulation among the artifacts involved in uploading to social media.

Therefore we question if there are quantifiable measures to ascertain the movement of an image through social media? Are there specific markers in the metadata that can aid in the tracing of image provenance during forensic analysis? By understanding the complete path of a digital image through social media, investigators will be able to speak to the authenticity of an image as well as map the sources of intentional and unintentional manipulation.

This paper is organized as follows: Section 2 presents background and current work relevant to digital forensics and social media, Section 3 lays out data creation and feature extraction used in this analysis and Section 4 presents the findings of this research effort. Section 5 draws conclusions and identifies a checklist for metadata analysis. Limitations and potential future research will also be discussed in Section 4.

2. RELEVANT RESEARCH

With the growing number of images across a growing number of social media sites, it is vital to not only understand the origin of an image but also its provenance or movements. According to Piva (Piva, 2013) “Doctored images are appearing with a growing frequency in different application fields so that ‘seeing is no longer believing’”.

Images stored on the Internet, especially on social media sites like Facebook and Twitter are stored as a JPEG image and undergo some form of compression unique to the social media site (Caldelli, Becarelli, & Amerini, 2017). JPEG is the most widely used lossy image compression

standard and can be found in most commercial digital cameras, wearable technology and smart phones (Wallace, 1992). The JPEG encryption process involves several components and can be summarized by the following (Iida & Kiya, 2018):

1. Color transform from RGB (Red Green Blue) to YCbCr (Green Blue Red)
2. Dividing an image into consecutive 8x8 blocks
3. Calculating 8x8 Discrete Cosine Transform (DCT) coefficients
4. Creating a quantization matrix
5. Applying Huffman coding

Digital forensic research has created a robust set of techniques to detect active manipulation or tampering of an image. Types of tampering involve region duplication, resampling, color filter array artifacts, inconsistencies in camera response function, lighting and shadows, chromatic aberrations, sensor noise and statistical features (Farid, 2009). Digital forensics, however, not only pertains to active manipulations of an image but also passive manipulations that tend to be much more benign and cannot be identified using these techniques. For example, the sole act of uploading an image to the Internet will manipulate and alter the image, and it is extremely valuable to understand if this type of behavior can be identified (Giudice, Paratore, Moltisanti, & Battiato, 2017). Depending on the privacy settings on an individual's social network, images that are uploaded can be browsed and downloaded by any user of the platform (Sun & Zhou, 2017). Forensic investigations will benefit from having a set of unique identifiers that can help plot the path of any image.

Current research in these passive manipulations has identified that the exchangeable image file format (EXIF) information (Farid, 2009) as well as components of the JPEG format can be used to identify how an image might have been altered. Moltisanti (Moltisanti et al., 2015), focused on Facebook, identified how the DCT coefficient and quantization tables varied based on

how the image was originally captured and uploaded to social media. Caldelli (Caldelli et al., 2017) further evaluated the DCT coefficient and potential differences between Facebook, Twitter and Flickr by training an ad-hoc classifier to successfully identify image provenance. In addition, Kee (Kee, Johnson, & Farid, 2011) identified quantization tables that Flickr frequently utilized while searching for a data set of images for JPEG header analysis.

Additional work in the digital forensics research field can be found in a parallel research group focused on OSINT (Open Source Intelligence). Image analysis techniques include focus on the hexadecimal file signature (Nixintel, n.d.) as well as IPTC metadata (IPTC, 2019) and geolocation, which uses features in an image to pinpoint the location the image was taken. Even though these techniques are often used to identify a location or a set of features, the combination of JPEG format components, headers and IPTC metadata should allow us to identify a set of variables that are unique to specific social media sites.

3. METHODOLOGY

This research focused on mapping how initial as well as consecutive uploads to a social media site results in passive image manipulation. The goal is to identify differences that are unique and that would assist forensic investigators in identifying how an image might have moved through social media.

3.1 Image Creation

With the prevalence of camera phones and quick access to social media through the same mobile device, it is imperative to understand the differences, if any, between media creation on a mobile phone application and desktop web application. All images were captured using an iPhone 13 Pro (iOS 15.1.1) and saved as as an HEIF (High Efficiency Image Format). Image settings can be changed to ‘Most Compatible’ resulting in images being saved in JPEG format, but this setting was not changed for this research. In addition, within the Apple ecosystem, HEIF is superior to JPEG as it takes up less space and

supports 16 bit color capture, compared to just 8 bit with JPEG (Pathak, 2020). Since all research was completed on Apple products this setting was not changed but should be revisited if further research is to include Android, Pixel or any additional operating systems. The content of the images were not of concern as this research focuses on the subsequent social media manipulation of the image and not the content itself. However, care was taken during image capture to insure that all images were unique with a variety of colors and features to allow for a complete histogram and color comparison. All images were taken using automatic settings and were not edited in any way.

3.2 Feature Extraction

There is a variety of information that can be found in EXIF metadata and can be broken up into five main categories: primary, EXIF, Interoperability, thumbnail and GPS (Kee et al., 2011). As it is unknown how different social media sites will handle the metadata all categories were included in the initial data capture.

Data collection and analysis was conducted on an Apple M1 iMac (11.5.1). Even though Apple offers some easy to use and free image software, all images were analyzed using XnView MP (0.99.1). Below is a list of metadata categories that XnView MP displays per image.

- General file properties
- JFIF properties
- Histogram
- IPTC-IIM
- Full ICC Profile

In addition, the color histogram and luminance profile were compared between the original and social media site downloads.

3.3 Social Media Upload & Download

This research was conducted on Facebook and Twitter as they both have mobile and desktop functionality and are major social media sharing sites. While apps like WhatsApp and Youtube

see a large number of daily traffic, they are out of scope as either pure video media content or chat sites. This research focused on how an image circulates social media in a public, large audience environment, not person to person, but is noted for future research.

Instagram is owned by Facebook, with a much heavier focus on image sharing, but operates in very similar manner. File name creation, for example, is identical between the two. Unfortunately, Instagram can only be used on mobile devices to upload images, whereas the web application on computer has *read* and *like* functionality only. The biggest limitation regarding this research specifically is that Instagram does not allow for image download on either mobile or web applications. Secondary websites do provide this feature but would add additional unknown variables into this research. Therefore Instagram was not included as a Social Media variable in this research.

Fig. 1 depicts the process of data creation. After the images were captured on the iPhone the original images were uploaded to the corresponding social media sites through the native phone application as well as the web application. Note that, we use the terms “on computer” and “web application” interchangeably. Once the images were downloaded, they were uploaded and once again downloaded from the second site. All images were saved with their original file name, unique to the social media site, as well as a suffix to indicate their path, per Table 1.

Ten original images were taken on the iPhone and then uploaded and downloaded accordingly. This results in a total data set of ninety images, ten original with 8 variances of each. All ninety images were examined and all metadata was tabulated manually. Histogram analysis was conducted through screenshots by comparing ratios of the Red, Blue and Green distributions as well as the luminance.

4. RESULTS

Analysis of the data set was run through XnView MP and the main results can be seen in Fig. 2. The screenshot summarizes the Name, Info,

Properties, Ratio, Size and Created Date for all eight images (No. 0-7) and the original image (No. 8). Note that the dataset generated and used in this study is available upon request.

An MPF or Multi Picture Format section was present in several of the ten original images. This is due to when an image is taken in portrait mode on a current iPhone an auxiliary photo is included in the JPG file that provides a disparity map. This disparity map is stored in an XMP format and hosts camera depth parameters for the image. Even though this MPF format can be found in the metadata for the original image, this information is scrubbed when uploaded to any social media site both on phone and web applications. Several other groups of metadata are also scrubbed when uploaded to social media sites including specific camera model and lens information, image and component configurations, as well as GPS data.

4.1 Differences in Metadata

Fig. 2 identifies several variables in the metadata that seem to differ between uploading through web or phone applications as well as between the different social media sites. The original image consists of ICC information which is retained on web applications as well as EXIF information which is completely scrubbed from all images. However, when image upload and download occur through the phone application, EXIF information is always retained. A defining differentiator appears to be what metadata is scrubbed. A direct download to Twitter retains ICC and IPTC data, however a subsequent upload to Facebook scrubs that data. In comparison a direct upload to Facebook retains IPTC data, which is then scrubbed when uploaded to Twitter.

Twitter appears to be the only social media site to retain the original Color Profile Description on both computer and phone uploads. For example, Display P3, can only be found in the original image and direct Twitter uploads on both phone and web applications. Direct as well as secondary Facebook uploads through the web application appears to modify this data point to uRGB, whereas mobile applications scrub this

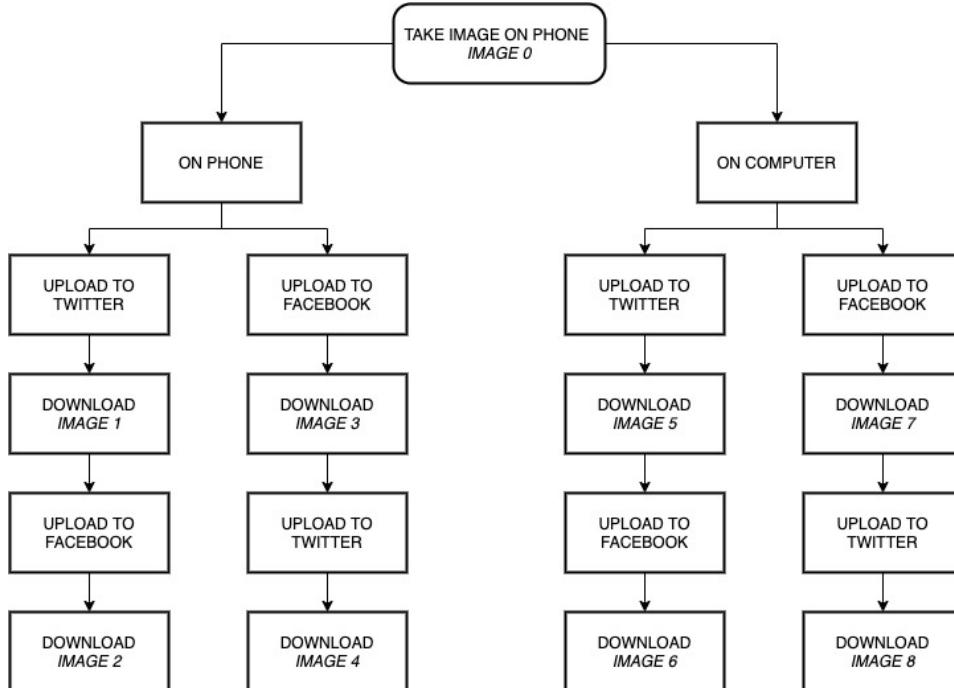


Figure 1: Process flow for data creation.

Table 1: Suffix Assignment for Data Set Naming Methodology

	Twitter (T)	Facebook (F)	T → F	F → T
Phone	Tp	Fp	TFp	FTp
Computer	Tc	Fc	TFc	FTc

data point entirely. Similarly, within the ICC profile, the Profile Type, Manufacturer and Profile Copyright seem to only be retained by a direct upload to Twitter. Facebook modifies this data point in its web application to Unknown and completely scrubs this data point on mobile applications.

File Permissions do not seem to identify type of social media, however, read and write permissions differ based on web versus phone application. Images saved from the phone application only retain owner read and write permissions (rw-----) compared to images saved from the web applications (rw-r--r--).

4.2 Unique Metadata

Information regarding the encoding process can be found both in the image properties as well

as the EXIFTool properties for all images. Even though the original image utilizes Baseline DCT and Huffman coding, Twitter uniquely substitutes Progressive DCT coding in place of Baseline DCT for direct Twitter as well as F-T uploads. This can be seen on all web application downloads, and specifically only on F-T uploads through the phone application. Direct Twitter uploads on a phone retain Baseline DCT coding. All direct Facebook as well as T-F uploads retain Baseline DCT coding for its encoding process.

The Current IPTC Digest is a unique data point found only in images downloaded from phone applications and is based on the MD5 hash of any legacy IPTC-IIM values. Within XnView MP this value is identified under the header Photoshop and indicates that both the Twitter and Facebook phone applications apply some level

No.	Name	Info	Properties	Ratio	Size	Created date
0	IMG_0048 - TfP.JPG		1534x2048,16M	0.75	457.74 KiB	12/6/21 12:42:31 PM EST
1	IMG_0047 - Tp.JPG	ICC IPTC EXIF	1898x2532,16M	0.75	740.06 KiB	12/6/21 12:42:30 PM EST
2	IMG_0046 - FTp.JPG		1536x2048,16M	4:3	349.69 KiB	12/6/21 12:39:04 PM EST
3	IMG_0045 - Fp.JPG		1536x2048,16M	4:3	464.13 KiB	12/6/21 12:39:04 PM EST
4	259753337_206533111656901_687859126207262170_n - TfC.jpeg	ICC	1512x2016,16M	4:3	441.44 KiB	12/2/21 3:07:22 PM EST
5	FFoLlCtYXsAcVRKY - Tc.jpeg	ICC	3024x4032,16M	4:3	2.70 MiB	12/2/21 2:58:02 PM EST
6	FFoKL7nXoAMKBca - FtC.jpeg	ICC	1512x2016,16M	4:3	452.84 KiB	12/2/21 2:53:55 PM EST
7	258869420_206524381657774_5021294225047822046_n - Fc.jpeg	ICC	1512x2016,16M	4:3	460.52 KiB	12/2/21 2:47:18 PM EST
8	IMG_0017.jpeg	ICC EXIF	4032x3024,16M	3:4	2.90 MiB	12/2/21 2:39:56 PM EST

Figure 2: XnView MP metadata results for original image and 8 variances.

of photo editing to an image even if the user does not specify edits during the upload. It is also noted that the value for the IPTC Digest reads d41d8cd98f00b204e9800998ecf8427e for all images, regardless of source. This MD5 hash value is unique and known to be an empty hash string (a NULL character). Regarding future research, there is some value in identifying if different types of image editing result in unique hash values.

An additional section of metadata that is unique to images downloaded from phone applications is Thumbnail and Compression metadata. However, there does not seem to be any differentiating factors regarding social media within this data set.

4.3 Image Size & Histograms

One component of the Image Properties, the Estimated Quality of an image, appears to be the best identifier to the source of an image. If an image is uploaded to Twitter through the web application the estimated quality will match the original image and if an image is uploaded from Facebook to Twitter, through the web application, Twitter will match the value assigned by Facebook. Essentially, Twitter does not specify its own estimated quality in the web application, it accepts whichever value had already been specified, be it from the original image or a previous social media site.

However, when images are uploaded on the phone application Facebook assigns an estimated quality that matches the original image, regardless of the source. Therefore, an image downloaded first to Twitter, and assigned a lower estimated quality, will be overridden by Facebook with the estimated quality value of the original

image. Similarly, Twitter will override this value both on a direct upload as well as on the image uploaded from Facebook. Table 2 summarizes the Estimated Quality of an image value for all 8 images compared to the original image (IMG_0017.JPEG), which is 93.

Image compression on both web and phone applications appears to also allow social media differentiation. Through its web application, images that are directly uploaded to Twitter retain the dimensions of the original image. Facebook, however, implements a 50% compression ratio. Additionally, an image uploaded to Twitter from Facebook retains the Facebook compression. The Twitter web application tends to retain the metadata in an image rather than substituting its own. In comparison, a direct upload to Twitter on a phone implements a compression ratio of around 63% whereas Facebook implements a ratio of 51% close to the 50% seen through the web application. A subsequent upload to Twitter does not seem to implement any additional compression, whereas Facebook will implement a further compression to the image uploaded from Twitter, for a final compression ratio of 51%. Again, close to the 50% compression ratio seen in the web application. Table 3 summarizes the image sizes for all 8 images compared to the original image size of 3024x4032.

Fig. 3 compares the RGB and Luminance Histograms for all eight images to the original file (Image 0). Subtle differences between the histograms can identify the source (phone vs. web application) as well as social media site ($F, T, F \rightarrow T, T \rightarrow F$). Direct uploads to Twitter using both a phone and web application match the original histogram well. A direct upload to Facebook using a phone results

Table 2: Estimated Quality of an Image on Phone and Web Applications

	Twitter (T)	Facebook (F)	T → F	F → T
Phone	85	93	93	85
Computer	93	86	85	86

Table 3: Image Size Compression on Phone and Web Applications

	Twitter (T)	Facebook (F)	T → F	F → T
Phone	1898x2532	1536x2048	1534x2048	1536x2048
Computer	3024x4032	1512x2016	1512x2016	1512x2016

in a choppy and stepped histogram, which can be seen in the multiple choppy peaks in both the red and blue histograms. Direct uploads to Facebook using a web application retains the overall shape of the histogram but tends to sharpen its peaks. As seen with some of the other variables discussed, Twitter tends to keep features regardless of source, therefore, an upload to Twitter from Facebook results in the histogram matching that of the histogram from Facebook. This can be seen both on phone and web applications. Facebook, however, will edit the image uploaded from Twitter, resulting in a more choppy histogram.

5. DISCUSSION

This in-depth metadata analysis presents several unique identifiers that can be utilized to understand how an image might have traveled through social media. It is important to note that even though an original image is not always available for analysis, there are multiple investigative scenarios where a comparison is crucial. A recent increase in revenge porn investigations for example will find it extremely useful to be able to track how an image was wrongfully shared. In these cases, as well as fraud examinations for example, an original would be available for comparative analysis.

This analysis shows that metadata within an image can tell us a lot about how an image has traveled through social media. The following can

be used as a basic strategy when analyzing an image. First, identify what type of metadata an image contains, namely ICC, EXIF, IPTC, etc. Twitter will retain much of this, whereas Facebook only retains IPTC and EXIF data. Second, check the Color Profile Description as well as the ICC profile. An Unknown value identifies a Facebook edit to the metadata, whereas original device information indicates Twitter. Third, within the EXIFTool properties, the encoding process tends to be Baseline DCT in original images and Facebook sources, whereas Twitter implements Progressive DCT encoding. Fourth, find the Estimated Quality value and calculate the image compression ratio. Facebook applies a 50% compression ratio on both web and phone applications whereas Twitter tends to utilize images in their original size on web applications and at 63% compression on phone applications. Also note, that metadata information like file permissions, Current IPTC Digest and Thumbnail data can identify if a web or phone application was used to share the image in question.

5.1 Limitations & Future Research

As this research was focused on the Apple ecosystem it is crucial to extend this methodology to Android applications. As the original image on the iPhone is not a JPEG, and has specific metadata variables unique to Apple it would be beneficial to compare this process between Apple and Android.

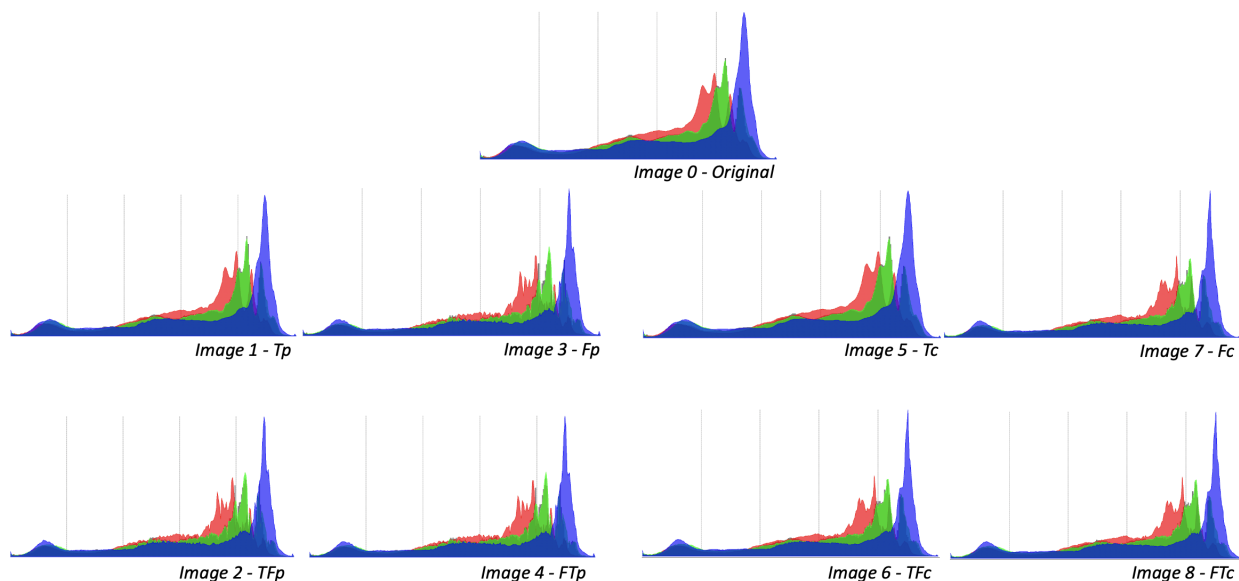


Figure 3: Histogram comparison between Original and Image 1 - 8 per process flow.

Any editing of the image was also out of scope in this research, therefore, understanding the impact of editing software like those found on a device as well as external software like Photoshop or Lightroom would be extremely beneficial. Editing within the application also allows the user to tag other individuals, tag a location and add alt text. Any of these edits could have an impact on the metadata and would be extremely valuable to study.

Expanding the data set to include additional social media sites as well as other types of social networking sites will allow for a more robust set of metadata that may be unique to each. In 2021 the top 15 social network sites include: Facebook, Instagram and Twitter as well as WeChat, WhatsApp, MeWe, Tumblr, Reddit, LinkedIn, Snapchat, Pinterest, Telegram and Meetup. This list also includes YouTube and TikTok which is based on video content (Gismondi, 2021). Adding services like Flickr, SmugMug, Imgur and Google Photos, which all offer free online photo hosting should also be considered (Software Testing Help, 2021).

REFERENCES

Bayram, S., Avcibas, I., Sankur, B., & Memon,

N. D. (2006). Image manipulation detection. *Journal of Electronic Imaging*, 15(4), 041102.

Caldelli, R., Becarelli, R., & Amerini, I. (2017). Image origin classification based on social network provenance. *IEEE Transactions on Information Forensics and Security*, 12(6), 1299–1308.

Edwards, J. (2014). Planet selfie: We’re now posting a staggering 1.8 billion photos every day. *Insider*. Retrieved from <https://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day-2014-5>

Fan, J., Cao, H., & Kot, A. C. (2013). Estimating exif parameters based on noise features for image manipulation detection. *IEEE Transactions on Information Forensics and Security*, 8(4), 608–618.

Farid, H. (2009). Image forgery detection. *IEEE Signal processing magazine*, 26(2), 16–25.

Gismondi, A. (2021, January). *Top 27 social media apps for your 2021 strategy*. <https://www.kubbco.com/top-27-social-media-apps-for-your>

- 2021-strategy/. ((Accessed on 12/10/2021))
- Giudice, O., Paratore, A., Moltisanti, M., & Battiato, S. (2017). A classification engine for image ballistics of social data. In *International conference on image analysis and processing* (pp. 625–636).
- Iida, K., & Kiya, H. (2018). Robust image identification without visible information for jpeg images. *IEICE TRANSACTIONS on Information and Systems*, 101(1), 13–19.
- IPTC. (2019). *Social media sites photo metadata test results 2019 - iptc*. <https://iptc.org/standards/photo-metadata/social-media-sites-photo-metadata-test-results-2019/>. ((Accessed on 11/22/2021))
- Kee, E., Johnson, M. K., & Farid, H. (2011). Digital image authentication from jpeg headers. *IEEE Transactions on Information Forensics and Security*, 6(3), 1066-1075. (doi: 10.1109/TIFS.2011.2128309)
- Moltisanti, M., Paratore, A., Battiato, S., & Saravo, L. (2015). Image manipulation on facebook for forensics evidence. In *International conference on image analysis and processing* (pp. 506–517).
- Nixintel. (n.d.). *The secret life of jpegs – nixintel*. <https://nixintel.info/osint/the-secret-life-of-jpegs/>. ((Accessed on 11/18/2021))
- Pasquini, C., Amerini, I., & Boato, G. (2021). Media forensics on social media platforms: a survey. *EURASIP Journal on Information Security*, 2021(1), 1–19.
- Pathak, K. (2020, April). *How to convert heic photos to jpg on iphone and ipad*. <https://www.howtogeek.com/666363/how-to-convert-heic-photos-to-jpg-on-iphone-and-ipad/>. ((Accessed on 11/22/2021))
- Piva, A. (2013, January). An overview on image forensics. *ISRN Signal Processing*, 2013, 1–22. (doi: 10.1155/2013/496701)
- Software Testing Help. (2021, November). *15 best free image hosting sites: Best photo hosting of 2021*. <https://www.softwaretestinghelp.com/best-free-image-hosting-sites/>. ((Accessed on 12/10/2021))
- Sun, W., & Zhou, J. (2017). Image origin identification for online social networks (osns). In *2017 asia-pacific signal and information processing association annual summit and conference (apsipa asc)* (pp. 1512–1515).
- Thakur, R., & Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Science International*, 312, 110311.
- Wallace, G. K. (1992). The jpeg still picture compression standard. *IEEE transactions on consumer electronics*, 38(1), xviii–xxxiv.