Xournals

Academic Journal of Forensic Science

ISSN: 2581-4273 | Volume 06 | Issue 01 | April-2023

Meta-Analysis of Images Clicked Using different Social Media Cameras

Oinam Olivia Chanu[1], Riya Bansal[2]

Available online at: www.xournals.com

Received 01st February 2023 | Revised 08th March 2023 | Accepted 24th March 2023

Abstract:

In the subject of study known as media forensics, many types of media, including audio, video, and digital pictures, are analysed and investigated using scientific methodologies and procedures. Finding evidence that can be utilised in court or other investigations is the main goal of media forensic. Experts in media forensics evaluate media files using a variety of tools and methods, such as data recovery, picture and audio enhancement, and authentication. In this paper we are going to trace the origin and properties of the files uploaded in different social media platforms. This paper situates such as framework and suggests a novel approach to determine whether a picture originates from a social network and, more specifically, to determine which image has been downloaded. The method is predicated on the idea that each social network employs an odd and mostly unknown alteration that yet leaves some recognisable traces on the image, and that these traces may be retrieved to showcase every site. The proposed technique successfully distinguishes distinct social network sources by using trained classifiers. Experimental findings on same image shot from different social media cameras and finding the differences in the pictures under varied operational circumstances attest to the feasibility of such a distinction.

Keywords: *Enhancement, Authentication, Retrieved, Recognisable, Feasibility.*

Authors:

1. *B.Sc, Forensic Science, Garden City University, INDIA*
2. *Junior Scientific Officer, Sherlock Institute of Forensic Science, INDIA*

Introduction

The collection, analysis, interpretation and presentation of audio, video, image evidence gathered during investigations and legal proceedings is known as media forensics **(www.artsandmedia.ucdenver.edu).** Social media is very important in today's digital environment and in daily life. Everyday numerous and various types of images, videos are uploaded in the social media platform every single second. However, we are not very sure about its properties and origin of the file, whether they are being manipulated or genuine. To study about this matter, media forensics is one of the greatest solutions to these uncertainties. It seems as though one cannot live without a social networking site. Growing worries about the reliability of digital media were caused in the previous ten to twelve years by the dissemination of simple editing tools that were available to a larger public. In this case, the problem has lately been made worse by the creation of new classes of artificial intelligence algorithms that enable people to create high-quality fake photos and videos (like Deepfakes) without the need for any specialised technical knowledge.

Additionally, multimedia material plays a crucial part in the digital lives of people and civilizations, substantially contributing to the viral transmission of information through social media and web channels. As a result, our society can no longer ignore the need to create tools to maintain the reliability of images and videos shared on social media and web platforms **(Pasquini *et al.*, 2021)**.

According to research, 1.81 trillion photographs are shot worldwide each year, and 6.9 billion of them are shared on WhatsApp daily. 1.3 billion photos are shared daily on Instagram, with around 100 million appearing in posts and more than 1 billion appearing in stories and conversations. 3.8 billion images are being shared everyday through snapchat, 2.1 billion in Facebook and 1 million images through Flickr **(www.photutorial.com)**. One-third of the population is able to access the internet and post photos to websites and social media. These data transmit a number of other things due to their digital characters. Details of their life history, such as the originating device and any processing they have undergone. When visual evidence is used in a crime, this information could become important. Multimedia forensics has been suggested as a possible remedy for this situation in order to examine photographs and videos in order to learn more about their life cycle. All these years, a number of methods are created to evaluate digital images, concentrating on problems with identifying the source device and judging the veracity of the material **(Shullani *et al.*, 2017)**.

An image may be taken and uploaded simultaneously to one or more social networks due to the increasing usage of smartphones. On the flip side, unlawful actions are mushrooming by abusing such digital stuff to accomplish different, occasionally ignoble, goals. Facing these increasing problems, related to different social media in our day today life, it is of great importance to know the origin and properties of images, videos uploaded in social media. By knowing the origin of the image like provenance of the image, from which camera it was shot, to which social media it was uploaded first, it would be of considerable assistance in media forensics, law enforcement and intelligence services in finding out the culprits responsible for creating misleading visual contents, manipulated and misused the images. More generally, it can assist in preserving the credibility of digital media and reducing the effects of misinformation by enforcing trustable sources by finding the properties details like checking out the hash value, metadata details, Exif information of the image, etc **(Caldelli *et al.*, 2017).**

Objectives

The main objectives of the research:

- To analyse the differences in images when taken from different social media cameras.
- To ascertain and discuss the characteristics of the photographs.

Methodology

The details of the used device are mentioned below:

Device name	:	realme 7i
Model	:	RMX2103

- All the images were captured using multiple social media cameras like Instagram, WhatsApp, Facebook, Snapchat, Telegram, in-built phone camera and LinkedIn of the above mentioned device.
- The hash values of the images were examined and computed using the software "HashCalc".
- To fully understand the information and nuances of a certain image, the metadata must be discovered. Consequently, the "Media Info" software was used to find and study the metadata of the images metadata was thoroughly examined.
- In order to determine the originality of the images, certain approaches were employed, such as examining the image's shadow, determining whether the border line was continuous, and

observing the negative of the images to check any kind of digital forgery.

Results and Discussion

Images captured with different social media cameras such as those on Instagram, WhatsApp, Telegram, Snapchat, LinkedIn, Facebook and in-built phone camera are meticulously examined with each individual detail being thoroughly examined. The images captured are referenced as shown in Figure No. 1 to Figure No. 7.

Upon close inspection of the collected images, it is discovered that the brightness of the photographs differs between each image, creating a visible distinction. It is observed that the image taken from the typical phone camera has the lowest brightness out of all those that were taken. It is due to the limited number of photons that cell phone cameras can capture due to their narrow apertures, the photos in low light are blurry. Additionally, they only have a modest number of sensor pixels, which dynamic range is constrained by the number of electrons that each pixel can hold **(Hasinoff *et al.*, 2016).**

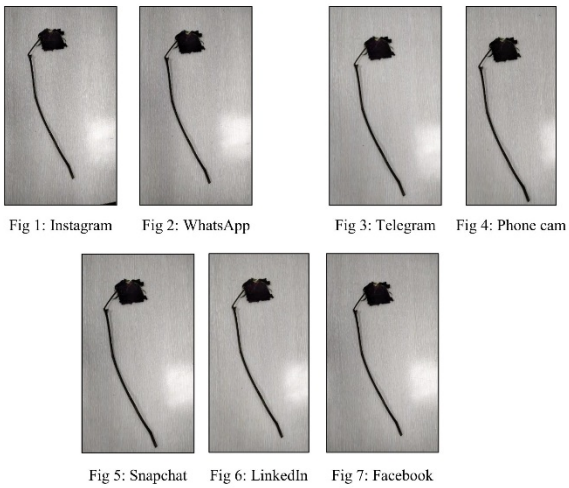


Fig 1: Instagram Fig 2: WhatsApp Fig 3: Telegram Fig 4: Phone cam

Fig 5: Snapchat Fig 6: LinkedIn Fig 7: Facebook

Figure No. 1-7: Images captured with different social media cameras

Any data, regardless of its size, may be transformed into a fixed length by using the cryptographic hash function. Hash value is the term used to describe the outcome. A hash value is crucial in the forensic industry to pretentiously show the reliability of any digital evidence. Any file's hash value may be compared to its digital fingerprint. It alters as soon as a minor file modification occurs **(Thakar *et al.*, 2021).** Likewise, the hash value of the photos used in this experiment varies for the same reason.

Each image has a distinct and unique hash value, which has been contrasted and analysed in the 'Table 1' shown below: -

Table No. 1: Comparing the hash value of images taken from different social media cameras

S. No	Camera Type	Hash Value
1	Instagram	1ddb497a63aee63a557297258b4ce58c
2	WhatsApp	0114b2cac4097b49e490e4fa18d0879a
3	Telegram	85c0554b9212edf4c812db53c42f308d
4	Phone camera	2b364e1f9c7a6cc29ba36087ab08d1d6
5	Snapchat	64eceab4e0c975bb614fcd270251bc0f
6	LinkedIn	dc1dca14191b1f193568593dbb6a3410
7	Facebook	da1b69955d6dae7a82581d7ac6debd2b

When the photographs' meta data is inspected using "Media Info", certain similarities and dissimilarities are observed. The focal length and aperture of the images captured in all the camera are same. The exposure time of LinkedIn, in-built phone camera and Telegram are same. In every image, the dimensions, the file size, and ISO are different. The metadata search does not provide the ISO and exposure time of Instagram, Facebook and Snapchat. Table 2 discusses the similarities and variations between the metadata of the images.

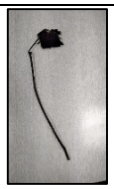
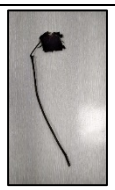
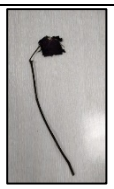
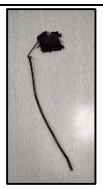
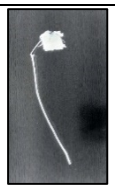
The table 2 shows that even though the pictures were same, taken at the same time, with same focal length and aperture, yet there are several differences in the characteristics of the images which distinguish images from each other. Every social media platform offers their own camera to the users with variable features. As shown in the data table 2, every social media has their own set of attributes which makes the images different. Hence, the images can be easily distinguished and identified when examined appropriately.

Table No. 2: Metadata comparison of the images captured with different application's camera

S. No	Camera Type	Dimensions	Size	Focal length	Aperture	ISO	Exposure time
1	WhatsApp	2160 x 3840 pixels	1.7MB	4.71mm	f/1.8	102	1/40s
2	Instagram	720 x 1280 pixels	344 KB	4.71mm	f/1.8	-	-
3	Facebook	1080 x 1920 pixels	413 KB	4.71mm	f/1.8	-	-
4	LinkedIn	800 x 1600 pixels	363 KB	4.71mm	f/1.8	286	1/100s
5	Snapchat	1440 x 2554 pixels	1.0 MB	4.71mm	f/1.8	-	-
6	Phone camera	2080 x 4608 pixels	2.7 MB	4.71mm	f/1.8	273	1/100s
7	Telegram	720 x 1280 pixels	428 KB	4.71mm	f/1.8	269	1/100s

After rigorous inspection, it is determined that the photographs are indeed genuine. The first thing that demonstrate the originality of the photographs is the observation of the shadow in each image. The shadow of the image will not be apparent in any tampered images. Additionally, the consistency of the border line in all the images demonstrates the authenticity of the images. When the negative of the photographs is thoroughly inspected, it is determined that they are original ones without any evidence of tampering. The negative of the images along with the original image is shown in Table 3.

Table No. 3: Comparison of the original image with its negative.

Camera Type	Instagram	WhatsApp	Telegram	Standard phone	Snapchat	LinkedIn	Facebook
Original Image							
Negative Image							

Conclusion

In this paper, the notion of identifying variations in pictures captured with various social media cameras is put forth. Here, the significance of determining an image's originality is also highlighted and debated. In order to determine the authenticity and integrity of an image, the "HashCalc" tool is crucial. Digital evidence's hash value is one of the most accurate techniques to assess the data integrity of the evidence. The "Media Info" software is used to get a file's comprehensive metadata. When determining a file's

integrity, the metadata offers a high level of comprehensive information about the digital file. The paper highlights that all the social media applications may have camera with different specifications resulting in varied attributes of the images. Hence, when viewed properly, they can be identified and the camera from which they have been clicked could be easily determined by assessing their metadata analysis.

References:

ByMatic Broz | March 10, 2023 (2023) How many photos are there? (2023) 50+ photos statistics, Photutorial. https://photutorial.com/photos-statistics/ (Accessed: April 4, 2023).

Caldelli, Roberto, et al. "Image Origin Classification Based on Social Network Provenance." IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, Institute of Electrical and Electronics Engineers, June 2017, pp. 1299–308. https://doi.org/10.1109/tifs.2017.2656842.

College of Arts & Media (no date) About The National Center for Media Forensics. https://artsandmedia.ucdenver.edu/areas-of-study/national-center-for-media-forensics/about-the-national-center-for-media-forensics#:~:text=Media%20forensics%20is%20scientific%20study%20into%20the%20collection%2C,during%20the%20course%20of%20investigations%20and%20litigious%20proceedings. (Accessed: April 4, 2023).

Hasinoff, Samuel W., et al. "Burst Photography for High Dynamic Range and Low-light Imaging on Mobile Cameras." ACM Transactions on Graphics, vol. 35, no. 6, Association for Computing Machinery, Nov. 2016, pp. 1–12. https://doi.org/10.1145/2980179.2980254.

Pasquini, Cecilia, et al. "Media Forensics on Social Media Platforms: A Survey." EURASIP Journal on Information Security, vol. 2021, no. 1, Springer Science+Business Media, May 2021, https://doi.org/10.1186/s13635-021-00117-2.

Shullani, D. et al. (2017) "Vision: A video and image dataset for source identification," EURASIP Journal on Information Security, 2017(1). Available at: https://doi.org/10.1186/s13635-017-0067-2.

Thakar, A.A., et al. "An Empirical Study Illustrating Effects on Hash Value Changes in Forensic Evidence Appreciation," International Journal of Science and Research (IJSR), 10(4), 2021, pp. 1356–1357. Available at: https://doi.org/10.21275/SR21501151311.