International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390373

The Significance of Metadata and Video Compression for Investigating Video Files on Social Media Forensic

Mukesh Choudhary[1*], Anshuman V Ramani[1], Vishwas Bhardwaj[2]
[1]Department of forensic science, Vivekananda global university Jaipur, Rajasthan, India
[2]State Forensic Science Laboratory Jaipur, Rajasthan, India
*Correspondence author: - cmukesh2610@gmail.com

ARTICLEINFO

Article History:

Accepted: 10 May 2023
Published: 30 May 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
304-313

ABSTRACT

Digital forensics is an essential aspect of cyber security and the investigation of digital crimes. Digital recordings are routinely used as important evidence sources in the identification, analysis, presentation, and reporting of evidence. There has recently been concern that images and videos cannot be used as solid evidence since they may be altered very quickly due to the abundance of technologies available for the gathering and processing of multimedia data. The main goal of this endeavour is to comprehend advanced forensic video analysis methods to assist in criminal investigations. We first propose the acquisition extraction analysis in a forensic video analysis framework that employs efficient video and image enhancement techniques for low-quality video that would be transferred through social media applications and for CCTV footage analysis. The reliability of digital video recordings is essential in forensic science and other criminal investigation fields. Digital video forensic analysis is a technique that constantly faces new challenges. Currently, videos are authenticated using a variety of parameters, including pixel-based analysis, frame rate analysis, bit rate analysis, hash value analysis, and, most importantly, metadata analysis. It was believed that the development of technology required the development of a new method for the verification of digital video recordings. In this review study, we made a novel attempt by reviewing the media. Information and structural analysis of video containers in the MP4 file format have been used to distinguish between real and altered videos.

Keywords: -Digital forensic, Metadata, social media forensic, Video compression, social media application

I. INTRODUCTION

Social media networking refers to technological advances that enable the production and sharing of information, ideas, professional interests, and various sorts of expressiveness through virtual systems and communities. Their regular components include intelligence, user-generated content, and the generation of information through each online contact. Online networking users get profiles created and maintained by web-based social networking media for the website or application. [1] There have been quick increments in online communication within the last 7–8 years, particularly in versatile communication. Smartphones have taken up the showcase so well that everyone can connect, socialise, and share thoughts and data from any corner of the world. Today's youthful era is active in chatting and informing each other with comparisons and questions as well. Individuals are ceaselessly trading data like pictures, recordings, exercises, and occasions. But despite getting associated with comparison for more and more time, their security (2012 Alfred) is additionally becoming more vulnerable to dangers from hackers and fraudsters. Typically, since hoodlums know that doing wrongdoing utilizing online portable applications is secure, it is an exceptionally intense errand to extricate the data from the portable phone from which wrongdoing was committed. Usually, since mobile phones have exceptionally little memory as well, they have streak memory, which gets washed quickly and effortlessly on versatile phones. One more reason for utilizing portable applications for any illegal activity is that their application logs will not get spared at the web benefit supplier side. Social media platforms are also utilizing versatile applications, including Facebook, WhatsApp, Instagram, Skype, JioChat, and Viber, since it's simple for them to trade and share data, especially after committing illegal activity. [2] It's interesting to note that Indians use WhatsApp to communicate with businesses as well as their family and friends. There are 15 million active WhatsApp Business users in India each month. Additionally, three million people per month browse the WhatsApp Business catalogue. According to the survey, 487 million WhatsApp users are in India. The number is increasing annually at a rate of 16.6%. [3] Facebook is an online platform for social networking and long-distance communication that allows users to add other users as "companions" and conduct business. [4] Get updates on others, send messages, post announcements and digital photos, share advanced recordings and connections, use various applications, and more. The latest data ranking Facebook users by country shows that India is home to 314.6 million of them, making it the country with the highest number of Facebook users. This represents around 22.1% of the population. In other words, over one out of every five people in India is a Facebook user. [5] YouTube is a video-sharing website that also allows users to create and manage personal accounts. The statistical data shows in **figure.1** as well as in **figure.2**. The website also provides a platform for sharing video clips, network-programmed cuts, music recordings, short films, movie trailers, and other content like blogging, short original recordings, and e-learning videos that are transferred by individuals, media outlets, and other organizations as part of the YouTube business programming.[6]

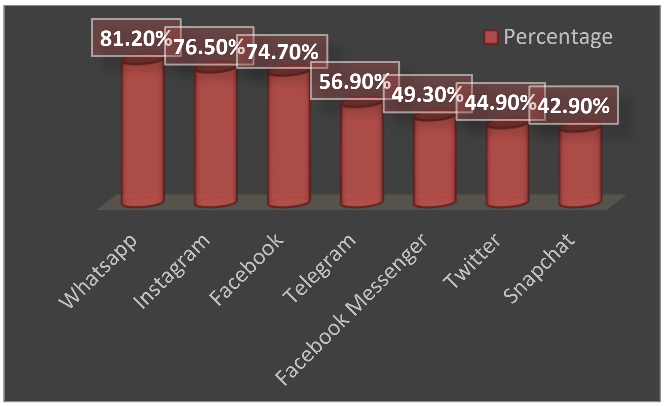

Figure: - 1 most used social media platform. [16]

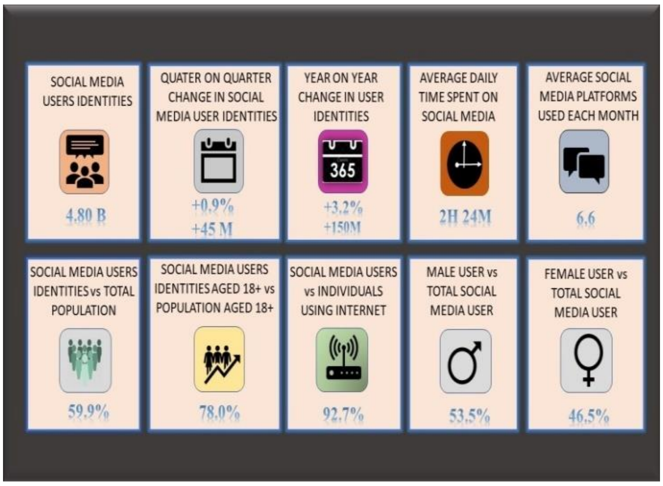

Figure: - 2 overview of social media use globally. [16]

1.1 Forensic Analysis of Instant Messaging Application: -

According to the United Nations Office on Drugs and Crime (2013), IM services are increasingly being utilised for both legal and illegal purposes. Criminals may use them to communicate with potential victims or with other criminals to avoid capture. Therefore, in the majority of investigations, IM applications have the potential to be a very rich source of evidence. We go over decoding and interpreting every artefact and piece of data produced by WhatsApp Messenger on Android smartphones. [7] The examination of videos these days depends on human retrieval. It is particularly ineffective because it depends on forensic experts' experience. To reproduce the crime scene and analyse forensic video evidence, object detection, identification, and tracking are crucial. A significant piece of technology that aids in inquiry specifically identifies the targeted objects in the source video, image, and audio as well as unearths more relevant information about the other key shreds of evidence, which is crucial to establishing links between key evidence. The object detection system extracts significant data about facial recognition, so it can be very useful in three different contexts:

I. Identifying objects in video surveillance that may pose a threat to the community or the country;
II. identifying unusual or malicious behaviours; and
III. Finding and recognising critical data based on the contents of footage or photographs

In this study, we tackle the issue of using object detection to analyse the visual data collected at a crime scene. Automatic detection and presentation of suspicious or particular subjects in the evidence are possible. This can help gather some information and create connections that can aid an investigation in connecting various pieces of evidence or even crime scenes. For video monitoring systems, intelligent highway systems, safety monitoring systems, etc., several video enhancement approaches have been developed over the last ten years. From a forensics perspective, the main goal is to extract as much data as possible from low-quality videos. This section focuses on methods that can be useful for extracting more data from improved videos. The likelihood of extracting more information from low-quality videos or images can be considerably increased by techniques based on histogram equalisation (HE). High-quality photographic evidence can be utilised to identify suspects in criminal investigations. According to an investigator, he can detect hidden information by using facial recognition to recognise images of invisible onlookers recovered from reflections in the subject's eye. Forensic video analysis allows for the mining of concealed formations, which then allows for the application of 3D reverse projection analysis, resulting in extremely accurate demonstrations of vehicle identification, suspect height, and crime scene reconstruction.

1.2 Metadata Extraction Analysis: -

According to the studies, social video has a big impact on web video as a whole. According to the post, video duration has decreased and even demanded the propensity of social media gatherings of individuals who seize the chance to segment films. However, according to television and cinema expert Peter Hawley, this is something to look forward to. He continues by saying that modern recordings that have the most impact are condensed, to the point, and designed to be quickly shared. Generally speaking, the average amount of videos and images uploaded to a website page increases, while the increase in web speed does not correspond to the growth of the average page size. The web's growth in content has improved data compression without corresponding growth in the speed of web connections. [8] A characteristic of a video that has undergone video transmission is its quality, which is assessed to obtain video compression. The visual signal may be slightly distorted as a result of video processing frameworks, which adversely affects the user's perception of the system. The verification of video quality is a crucial task for service providers and system administrators. [6], [9] In this manner, there's an expanding conspiracy to investigate artefacts spared by OSN (Open Storage Network) applications on a smartphone inside memory. Versatile gadget forensics, by and large, includes an essential strategy for fruitful examination. The method comprises a procurement stage, an examination stage, an investigation stage, and a detailing stage. Most of the well-known portable scientific apparatus are intuitive programmes that were planned to create unmistakable data that's covered up or difficult to discover, such as oxygen, UFED, etc. forensic analysis tools. They permit the analysis to extricate the primary memory of smartphones and naturally analyse and generate a summarised report to be displayed to the court. These apparatuses are inviting but amazingly expansive. Be that as it may, most of the open-source devices are not inviting and don't incorporate all the portable gadgets at forensic stages. [10] We all know the Video-ACID (atomicity, consistency, isolation, and durability) database for camera identification and authentication. To develop and test video camera model identification algorithms, a database of carefully curated films was created. Although this database was specifically created with camera model identification techniques in mind, we should point out that due to its characteristics, such as its wide range of codec parameters, it can also be used for the development and testing of several forensic algorithms. In our digital age, techniques for determining the veracity of media data are becoming more important. Attacks against professional camera authentication systems have shown the shortcomings of existing in-device solutions, even though the majority of consumer devices have no practical authentication support at all. Different container formats and compression codecs are frequently used for encoding videos from digital cameras and mobile devices. Advanced compression methods are chosen by mobile phones (MP4V, H.26x). In our test set, the majority of digital cameras favour an amalgamation of AVI containers and straightforward MJPEG compression. For MJPEG-compressed (Motion Joint Photographic Experts Group) video frames, different camera types use various JPEG (Joint Photographic Experts Group) marker segment sequences. Compared to JPEG images, content-adaptive quantization tables appear to be more common. The compression settings and marker sequences for the same camera model's MJPEG frame and JPEG still image files can differ greatly. Lossless video editing doesn't change the actual video stream's compression settings, but it does bring unique artefacts to the way container files are built. [11]

II. METHODS AND MATERIAL

2.1. Acquisition of file systems: -

On each Android device, the file system extraction process was carried out. The extractions were carried out utilising the "Cellebrite UFED (Universal Forensic Extraction Device) Classic Ultimate", Autopsy, EXIF tools Magnate, EnCase, FotoForensic, etc. mobile acquisition device in a forensically sound setting. The phone's settings menu's "USB Debugging" option was "enabled" before the acquisition process began. File system extraction takes all of the directories and files from the Android phone's internal memory, which includes items like configuration files and database files. Every application's data is extracted by the file system and placed in a separate folder on the phone. Therefore, file system extraction was only performed once for both programmes on each phone.

2.2 Artefacts, properties, and storage facilities: -

Many files and folders will be produced after the file system extraction of Android devices, but it will be highly challenging and time-consuming for any forensic professional to analyse and look into every single file in every folder. The UFED physical analyzer can also be used to view the information that has been taken from the UFED, but it occasionally has trouble showing data for all applications. Therefore, the place in which forensic artefacts relating to instant messengers are kept [12] The whole process is shown in the below-mentioned **figure: - 3.**

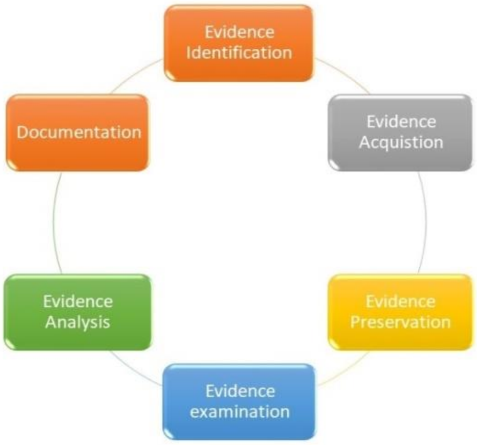

Figure: - 3 examination of process of digital evidence

2.3 Forensic video analysis framework: -

I. Format conversion and forensic video capture: - Many digital video evidence does not come in common file types like Avi, MP4, etc. These videos must be converted to a standard format without losing any of their features.

II. Tag and hash pertinent photos and videos: - To combine a variety of multimedia shreds of evidence, including combinations of video sources from multiple channels, the detection of suspects, and the extraction of pertinent images, it is essential to separate case-related video clips from the original video and group them into organised groups.

III. Enhancement: - It is necessary to improve the bundled video frames or clips to add new features and reveal hidden data.

IV. Analysis of Video as Evidence: - Thorough forensic video analysis at this point should be able to minimise a variety of noises that may be present during video capture, editing, extraction, filtering, etc.

V. Highly efficient evidence extraction: - To extract more potential evidence, scene reconstruction and object detection are combined with already-existing data from social networks, 3D scene geometry, AI, and machine learning technologies.

VI. Presentation of Concrete Evidence: - Using existing video and image c technology, such as enhancement algorithms and machine learning approaches, an investigator can easily apply advanced enhancement techniques to their evidence, generating better-quality video for examination. [13]

2.4 Forensic video type and content analysis: -

- Video/image feature extraction;
- Devices for sensor pattern noise extraction;
- Match the video and image features to the device features. The source identification video can be very useful in real-life scenarios.

I. Quality of video: - To detect relevant evidence from distorted contents in low-quality images and videos, a range of processing techniques, such as enlargement, re-scaling, etc., are frequently utilised in traditional forensic video examination. Resizing an image won't, however, make it easier to see more details. In general, low-resolution imaging has relatively little room for improvement.

II. Brightness: - The brightness can have a big impact on how well a CCTV surveillance system examines low-quality video and images because it can make the video captured over- or underexposed depending on the environment. In certain circumstances, changing the video's or image's brightness can make more information visible.

III. Compression: - To save file size, many digital camera systems aggressively compress video and photos. [13]

IV. Resolution: - The pixels utilised to indicate a video's width and height define the resolution of the image. The movie's filename additionally includes an "I" or "P" suffix to further identify the scan type. The quantity of data that must be saved is reduced to a minimum when presenting a video with an interlaced scan by updating every other row of a frame. In a progressive movie, every row of the display needs to be updated for every frame.

V. Codec profile: - Video complexity is determined by the purpose. Speed. In contrast to "Main" and "High," which employ **context-based adaptive binary arithmetic coding** (CABAC), "Baseline" and "Constrained Baseline" films use CAVLC (**context-based adaptive variable length coding**). Both algorithms encrypt and decrypt data without any loss; however, CABAC uses more computing power than CAVLC. B-frames are supported by the "Main" and "High" profiles. While level determines bitrates, profile represents the complexity of the decoding process. A Level 4 or above decoder is needed for 30 frames per second (1080p) video. Point-and-shoot cameras utilise "main" or "baseline" profiles, whereas high-end smartphones use "high."

VI. Frame rate: - Both footage with a variable and fixed frame rate is part of video-ACID. Movies with a fixed frame rate display each frame for the same amount of time. The frame time is altered by varying frame rates. A camera could increase the frame rate to better capture fast activity.

VII. Duration: - Every video that was recorded for the Video-ACID dataset has at least five seconds in it. There were several constraints on the choice of this number. Movies need to be at least several GOP sequences long to represent forensically significant action. Second, rather than analysing the whole video, certain forensic algorithms focus on particular frames. In light of this, we want to increase the number of frames that are accessible for each movie. Not to mention, collecting data costs money; therefore, we try to film as many videos as we can in a certain amount of time. Five-second videos were discovered to be immune from all of these restrictions.

VIII. Content: - Content diversity is essential for many forensic activities. Each camera was used to record videos in a variety of situations, such as close- and far-field focus, indoor and outdoor settings, different lighting conditions, lateral and vertical filming, and a variety of backdrops, such as flora, urban sprawl, frozen landscapes, etc. Every movie has some kind of motion or variation in the scene's content to lessen the repetition of frames throughout a single film. This movement often entails panning, rotating, or changing the angle of the camera relative to the object in the photograph. [14]

A. Automatic detection of suspicious objects in video:

To track for more activity or information regarding certain suspect objects that have previously been found through evidence. In forensic investigations, weapons that are often used and dangerous, such as knives, firearms, etc., may be classified as suspicious objects that may be utilised in criminal activities. Automated weapons identification over real-time video (like that from a CCTV system or an asynchronous system of video files) may be very useful for a quick response or criminal alerts.

Basic steps:

- **a)** Extract frames from the video;
- **b)** Background detection;
- **c)** Canny edge detection;
- **d)** Sliding window, scaling, PCA (principal component analysis), and NN (neutral network);
- **e)** Candidate regions;
- **f)** MPEG (Moving Picture Experts Group) classification;
- **g)** Filtering and decision-making.

B. Tracking and Object Detection Based on Colour and Shape:

It is now possible to carry out precise object detection and tracking on video or even live cameras thanks to improvements in computing capabilities and graphic processing using Open CV (Open-Source Computer Vision Library) and GPU (Graphics Processing Unit). In this section, we'll concentrate on utilising an open CV to detect objects based on their colour and shape. Because the red-green-blue (RGB) colour space cannot effectively distinguish between colour and intensity information, we use the Hue Saturation Value (HSV) and YCrCB systems for object detection and tracking. These systems allow for the detection of each colour by using a specific range in the hue channel. To enable real-time video streaming from a camera, Open CV and CUDA (Compute Unified Device Architecture) features are offered.

C. Deep learning-based key object detection in the footage:

In numerous cases, the colour of a particular protest in the video is not steady due to different components, such as the alteration of light, the quality of the video, other objects with comparative colour, etc., which can essentially influence the recognisable proof. Luckily, the development of machine learning can offer many ways to better distinguish between proof and execution. The profound learning appears to be an incredible point of interest in image-based protest discovery. In measurable examination. The conventional strategies, as a rule, physically audit and extricate related outlines and highlights from the available film. Which needs encounters through a long time of aggregation? Techniques can use a lot of existing data to automatically extract and learn characteristics. A deep learning model that has been carefully created and trained can analyse video and picture information with accuracy. To identify suspicious actions, events, images, or frames in the video, we introduce the Yolo network model in this study. The detection procedure includes the following four phases:

a) ***Frame selection:*** - The frame picker phase selects objects from a set of existing object images. This means that in a forensic investigation, we must first identify suspicious objects at the crime scene and take as many labelled pictures as we can. The frame picker phase then selects images of objects belonging to the class and crops the annotated regions; this can be done automatically using scripts.

b) ***Scale modifier:*** - To improve the efficiency of feature learning, this step aims to scale down the size of objects that were cropped in the previous phase.

c) ***Object marker:*** - The updated picture is pasted into base images with backgrounds and sizes that are similar during this stage.

d) ***Annotation creator:*** - During this stage, the major emphasis is on noting the size and location of freshly added items over the base. The newly created annotation annotations can be calculated based on the tasks applied in the image marker phase. [13]

III. DISCUSSION

Through the extraction of metadata from various application networks, the analysis of this review paper took into account the video compression of social networks and identified significant similarities and differences between the compression rates. It is important to remember that the video and sound compression in various social media applications is higher since video transferring transforms into extra features on the social network. For a short verification of the video's integrity, many writers have used meta-data and container analysis. The forensic examination of the artefacts left by various instant messaging programmes on smartphones was covered in this review article, and it was demonstrated how these artefacts might offer various information with evidential value. This study was specifically designed to analyse and discover changes in any video file's attributes when transferred over multiple instant messaging programmes on a smartphone. A study also showed how the characteristics of a video message, such as its hash value, codec, audio-video characteristics, frame rate, bit rate, sampling rate, aspect ratio, and audio amplitude statistics, among others, vary as it is delivered across various instant messaging services. This deterioration in quality, quantity, etc., might result in the loss of important information that can be obtained from these kinds of brief recordings that are interesting to examine in any criminal case. As the hash value of the received video matched that of the original video, it was determined that QQi had transferred the video file in its original state without any alterations or compression. However, compression was seen when the same file was sent through Telegram, Facebook Messenger, and many other social media applications. By taking into account the behaviour of file compression on the basis of the application utilised, this kind of study will aid forensic investigators and investigative agencies in reviewing such video files in any criminal situation. In this study we confine the best methodology to establish the authenticity of the video file system as a remake mentioned in above **figure: 4**.

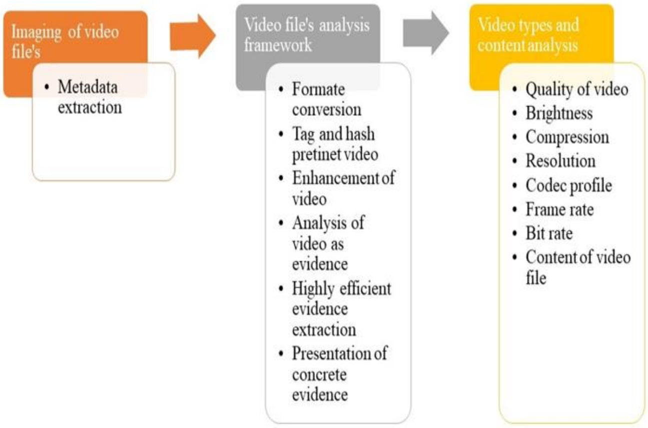
Imaging of video file's
Metadata extraction
Video file's analysis framework
Formate conversion
Tag and hash pretinet video
Enhancement of video
Analysis of video as evidence
Highly efficient evidence extraction
Presentation of concrete evidence
Video types and content analysis
Quality of video
Brightness
Compression
Resolution
Codec profile
Frame rate
Bit rate
Content of video file

Figure: - 4 Remake of video file analysis

IV. REFERENCES

[1]. Obar, et.al, (2015). Social media definition and the governance challenge: an introduction to the special issue". Telecommunications policy. 39 (9): 745–750.

[2]. Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic analysis of instant messenger applications on android devices. arXiv preprint arXiv:1304.4915.

[3]. https://www.oberlo.com/statistics/facebookusers-by-country

[4]. Davis, M. (2015). Facebook close sets speed record for $250 billion market cap". Retrieved from:https://www.bloomberg.com/news/articles/2015-07-13/facebook-sclose-sets-speed-record-for-250-billion-market-value. Retrieved January 28, 2017

[5]. https://www.statista.com/forecasts/1146773/whatsapp-users-in-india

[6]. Calibo, D. I., &Niguidula, J. D. (2019). Metadata Extraction Analysis: A Review of Video Data in Effect to Social Media Compression. JOIV: International Journal on Informatics Visualization, 3(1), 54-58.

[7]. Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201-213.

[8]. Greenemeier, L., (2013). When will the internet reach its limit (and how do we stop that from happening)? Retrieved from: https://www.scientificamerican.com/article/when-will-the-internet

[9]. Rodriguez, et. Al., (2012). Quality metric to assess video streaming service over tcp considering temporal location of pauses (pdf). IEEE Transactions on Consumer Electronics. IEEE. pp. 985– 992. doi:10.1109/TCE.2012.6311346. Retrieved November 25, 2016.

[10]. Ayahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. Procedia Computer Science, 109, 1035-1040.

[11]. Gloe, T., Fischer, A., & Kirchner, M. (2014). Forensic analysis of video file formats. Digital Investigation, 11, S68-S76.

[12]. Xiao, J., Li, S., & Xu, Q. (2019). Video-based evidence analysis and extraction in digital forensic investigation. IEEE Access, 7, 55432-55442.

[13]. Hosler, B. C., Zhao, X., Mayer, O., Chen, C., Shackleford, J. A., & Stamm, M. C. (2019). The video authentication and camera identification database: A new database for video forensics. IEEE Access, 7, 76937-76948.

[14]. https://datareportal.com/social-media-users

[15]. Ali, R. R., Mohamad, K. M., Jamel, S. A. P. I. E. E., & Khalid, S. K. A. (2018). A review of digital forensics methods for JPEG file carving. J. Theor. Appl. Inf. Technol, 96(17), 5841-5856.

[16]. Alyahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. Procedia Computer Science, 109, 1035-1040.

[17]. Cahyani, N. D. W., Rahman, N. H. A., Glisson, W. B., & Choo, K. K. R. (2017). The role of

mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. Mobile Networks and Applications, 22, 240-254.

[18]. Chang, M. S., & Yen, C. P. (2019). Forensic Analysis of Social Networks Based on Instagram. Int. J. Netw. Secur., 21(5), 850-860.

[19]. Eriş, F. G., & Akbal, E. (2021). Forensic Analysis of Popular Social Media Applications on Android Smartphones. Balkan Journal of Electrical and Computer Engineering, 9(4), 386-397.

[20]. Gangwar, D. P., & Pathania, A. AUTHENTICATION OF DIGITAL MP4 VIDEO RECORDINGS USING FILE CONTAINERS AND METADATA PROPERTIES.

[21]. Hamdi, D., Iqbal, F., Baker, T., & Shah, B. (2016, August). Multimedia file signature analysis for smartphone forensics. In 2016 9th international conference on developments in eSystems engineering (DeSE) (pp. 130-137). IEEE.

[22]. Jiang, J., Kasem, H. M., & Hung, K. W. (2019). Robust image completion via deep feature transformations. IEEE Access, 7, 113916-113930.

[23]. Koenig, B. E., & Lacey, D. S. (2015). Forensic authentication of digital audio and video files. Handbook of digital forensics of multimedia data and devices, 133-181.

[24]. Kumar, N., & Sharma, S. (2016). Survey Analysis on the usage and Impact of Whatsapp Messenger. Global Journal of Enterprise Information System, 8(3), 52-57.

[25]. López, R. R., Luengo, E. A., Orozco, A. L. S., & Villalba, L. J. G. (2020). Digital video source identification based on container's structure analysis. IEEE Access, 8, 36363-36375.

[26]. Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., &Tubaro, S. (2012). An overview on video forensics. APSIPA Transactions on Signal and Information Processing, 1, e2.

[27]. Raghavan, S. (2013). Digital forensic research: current state of the art. Csi Transactions on ICT, 1, 91-114.

[28]. Rangaswamy, S., Ghosh, S., Jha, S., & Ramalingam, S. (2016, October). Metadata extraction and classification of YouTube videos using sentiment analysis. In 2016 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 1-2). IEEE.

[29]. Serhal, C., & Le-Khac, N. A. (2021). Machine learning based approach to analyze file meta data for smart phone file triage. Forensic Science International: Digital Investigation, 37, 301194.

[30]. Suhardjono, S., Handayani, P., Sugiarto, H., Aisyah, N., & Putra, A. S. (2022). FORENSIC ANALYSIS VIDEO METADATA AUTHENTICITY DETECTION USING EXIFTOOL. Journal of Innovation Research and Knowledge, 1(12), 1727-1734.

[31]. Tian, N., Ling, B. W. K., Qing, C., & Yang, Z. (2018). Camera identification based on very low bit rate videos with overall noise pattern having time varying statistics. Multimedia Tools and Applications, 77, 1299-1322.

[32]. Tri, M. K., Riadi, I., & Prayudi, Y. (2018). Forensics acquisition and analysis method of imo messenger. International Journal of Computer Applications, 179(47), 9-14.

[33]. Verma, R., & Pathania, A. (2021). A Study on Video-Files Sent Through Popular Instant Messaging Applications on Smartphones for Forensics Investigation.

[34]. Vyas, B. R. (2016). The value of mobile device metadata for investigations (Doctoral dissertation, Utica College).

[35]. Wilson, R., & Chi, H. (2018, March). A framework for validating aimed mobile digital forensics evidences. In Proceedings of the ACMSE 2018 Conference (pp. 1-8)

Cite this article as :

Mukesh choudhary, Anshuman v ramani, vishwas bhardwaj, "The Significance of Metadata and Video Compression for Investigating Video Files on Social Media Forensic", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.304-313, May-June-2023. Available at doi : https://doi.org/10.32628/CSEIT2390373
Journal URL : https://ijsrcseit.com/CSEIT2390373