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

A Study on Video-Files Sent Through Popular Instant Messaging Applications on Smartphones for Forensics Investigation

Ritika Verma*[1], Anju Pathania[2]

[*1]Central Forensic Science Laboratory, Directorate of Forensics Science Services, Ministry of Home Affairs, Government of India, Amberpet Post, Ramanthapur, Hyderabad, Telangana, India

[2]Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs,Government of India, Plot # 2, Sector 36-A, Dakshin Marg, Chandigarh, India

Dr. Ritika Verma* : ritikaverma.2@gmail.com (*Corresponding Author)

Article Info
Volume 7, Issue 4
Page Number: 484-491

Publication Issue :
July-August-2021

Article History
Accepted : 01Aug2021
Published : 08 Aug2021

ABSTRACT

With the advent of smartphones and cheaper internet services, internet-based communication via instant messaging applications has become very widespread in today's world. As a result, cybercrime has risen as well. Thus, forensic investigators should understand how data files are altered when they are transferred via these popular instant messaging apps through smartphones. In the present paper, our aim is to focus on the study of variation in the properties of sample short video message when exchanged through popular instant messaging applications i.e. WhatsApp, Facebook Messenger, QQi and Telegram. Any video recorded on a smartphone has various parameters linked to its audio and video properties. This paper presents a methodology of extraction and analysis of these video files using freewares available online. It was found that every instant messaging application has its unique compression format which affects the properties of any data file accordingly. Comparison of the parameters of received video file obtained from this study shows that when such files get transmitted through Facebook Messenger and Telegram, it faced maximum degradation in both audio and video parameters. But when transferred through QQi and WhatsApp application, audio and video parameters of file has not got affected for used sample short video of ~18 sec. Furthermore, with QQi, we have observed that even the Hash value of file has also not got changed. Utilizing the results presented in this paper, forensic investigators can study the authenticity of such instant messages in cases involving legal matters by considering facts about data compression.

Keywords: Instant messaging, Digital audio-video forensics, Metadata, Smart Phone Forensics.

I. INTRODUCTION

Over the past decade, there is a rapid increase in online communications due to its cost effectiveness as compared to other modes of communication services provided by mobile operators. Moreover, with the advent of Smartphones the way people connect with each other and the manner in which

information is shared & distributed has further transformed. Nowadays, smartphones have numerous types of applications which allow users to exchange instant messages in the form of text, video, audio, images etc. As compared to traditional methods of communication, these applications are able to send content like images, videos etc. instantly to a large scale very efficiently. Though, these instant messaging facilities have given us an opportunity to connect with the world very easily, some people are using it in illicit activities. At present, various social media platforms are interlinked, due to which it becomes very challenging to control spread of any such illicit information and fake multimedia files.

Because of admissibility of electronic evidences in the present legal framework, these types of instant messaging applications have become a rich source of evidentiary information in most of the forensic investigations. One of the most commonly received cases includes investigation of viral videos and their authenticity. In this type of investigation, evidences left by these applications on smartphones can play an important role in retrieving those probable evidences forensically. Thus, the knowledge of retrieving of data artifacts linked with data files of various applications from smartphones is necessary. This attracted attention of many researchers towards this regime of mobile forensics. Aditya Mahajan et.al, [1] and CosimoAnglano [2] in their papers have discussed about forensic analysis of Instant Messenger Applications like WhatsApp and Viber on Android Devices. However, no one has discussed in detail about how the properties of any video file gets changed when transferred through different popular instant messaging applications. Thomas Gloe et.al.[3] in their paper have discussed the data related to forensic analysis of video file formats only. During literature review, we have observed that video files compression is common in different types of social media platforms when any video is uploaded on it. In the research papers of Y.-J. Chen et al.[4] and D. Calibo et.al. [5] analysis about how different formats of video compression affect the quality of any such videos was discussed. Nowadays manipulation of any video is very easy and common people encounter numerous number of fake videos every day. In investigation of such viral videos, video-authentication techniques can play crucial role. J. Randolph Hall [6] in his thesis has discussed a method for video authentication using file structure and metadata of MPEG-4 video files.

Therefore, if we know the compression behaviour of any instant messaging application, we can investigate the authenticity of any video on the basis of simple metadata analysis. But to carry out the investigation, it is important to know about the compression behaviour of different instant messaging application on any video file. By considering this, in the present paper we have prepared a study plan which focuses on studying the properties of video messages sent by widely used instant messaging applications. As per statistics published by J. Clement on statista.com on topic “Most popular global mobile messaging apps 2020” we found that WhatsApp messenger is most popular and approximately 2 billion users were accessing it on a monthly basis. The second most popular application is Facebook messenger with 1.2 billion monthly users followed by QQi with 694 million and Telegram with 400 million monthly active users [7]. Therefore, in the present study we have picked these four most popular instant messaging applications i.e. WhatsApp, Facebook Messenger, QQi and Telegram.

II. METHODS AND MATERIAL

The present paper aims to evaluate the factors that affect quality and metadata properties of video file and its structure, especially when a short video message is transmitted through different android based instant messaging applications on smartphones.

Details of smartphones and their Operating System used in present study is listed in Table .1. For filming sample short video, rear video camera of source mobile phone was used with picture size: 4:3 (13MP) and video size - VGA 640X480.

TABLE 1
Details of Source and Receiving devices

Devices	Make	Model	Android Version
Source of Video	Samsung	Galaxy J7 Prime SM-G610F	7.0
Receiving Device 01	Unknown Receiver/Sender		
Forwarded Video Receiving Device 02	Samsung	Galaxy J7 Prime SM-G610F	7.0

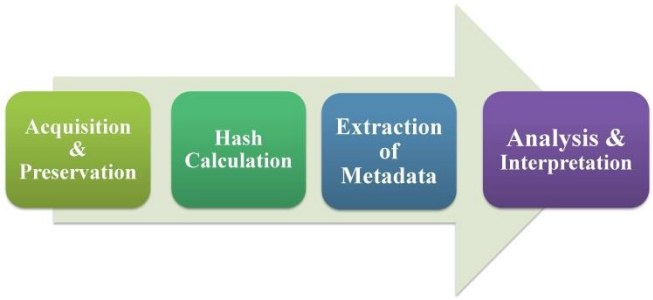

Figure1. Methodology used to Examine Video files Extraction and Examination from Smartphone's.

Methodology used to extract and examine the video files exchanged through four different android based instant messaging applications on smartphones using freeware available online is shown in Figure. 1 and its stepwise details are as follows:

Step 1: Acquisition and preservation

Due to the proprietary nature of mobiles it is often not possible to acquire data in powered off condition, thus mostly mobile device acquisition is performed live. Most acquisition tools for mobile devices are commercial in nature and consist of a hardware and software component, often automated. But in the present study we have acquired the required files from application folders by connecting the phone to PC.

Step 2: Hash Calculation

A Hash Value is a string value of specific length, which is the result of calculation of a Hashing Algorithm. Hash Value is used to determine the Integrity of any Data i.e. work as its fingerprint. In order to study the variation in properties of video messages we have calculated hash value of these files using SHA-256 which is considered as one of the strongest hash function. Hash value for all these video files were generated by using *HashCalc* Software to check hash value (SHA256) by connecting the phone to PC.

Step 3: Extraction of Metadata

Metadata is a kind of highly structured summary of any data file. Many distinct types of metadata exist, including descriptive metadata, structural metadata, administrative metadata, reference metadata and statistical metadata. To extract metadata of original video file and transmitted (or received) video files via different instant messaging applications, two different freeware i.e. *Media info* and *Gold wave* software's were used.

Step 4: Analysis & Interpretation

After collecting metadata of these video files, we have analyzed and compared the results obtained to find out any possible variation or compressions in parameters related to video and audio data such as; average bitrate, frame rate , duration and audio sampling rate etc. Discussion and Interpretation based on comparison of extracted metadata and analysis of

result is presented in detail under *Results and Discussion* heading.

III. RESULTS AND DISCUSSION

Forensic properties like Metadata, Hash Value and audio Amplitude Statistics of the original video were analyzed using freely available Software and results so obtained are tabulated in Table.2, Table.3 and Table.4 separately.

TABLE 2
Hash Value generated for all video files received through various instant messaging apps.

Application/ Source Name	Hash Value (SHA256)
WhatsApp	352f732547fce7379f16f676c9f893afebb59634ee19682d5bbd755317719168
Telegram	2a850db474f3504229d7a5c4ad28a829c725d1f4901635ee7d7d585829b8057f
Facebook Messenger	af6f70869bd44777b59d25e5c011282df944248561e06ff35f2dd5f91d28d40f
QQi	4f951e9337bbdd71afe89a21c7e625f07340a17ffb54ca9843659824038524ed
Original Video	4f951e9337bbdd71afe89a21c7e625f07340a17ffb54ca9843659824038524ed

In the present study, most popular instant messaging applications i.e. WhatsApp, Facebook Messenger, QQi and Telegram were used for sharing the sample video file. Filmed short Video file from Source phone was sent to various Android based phone via different instant messaging applications and then this video file was forwarded to other Mobile phones. After multiple forwarding, we have picked one mobile phone on which the same video was received via different instant messaging applications. Video files received through different applications on mobile phone were saved or downloaded as per applications instruction, so that these received video files can be analyzed for further comparison with original video file. The metadata properties, Hash Value and Audio Amplitude Statistics of all video files on receiving mobile phone via popular instant messaging applications were extracted and results are tabulated in Table.2, Table.3 and Table.4 respectively.

On comparing the result obtained for these video files with original file properties, we found some interesting observations which should be considered while analyzing results, investigating and developing an opinion about the real life cases on viral video messages.

The observations are listed below:

a) Hash value: In Table.2 Hash values generated for original and all files received via different instant messaging applications is tabulated. Hash value obtained for video file received via QQi is same as of original video file (see Table. 2) this indicate that QQi preserves originality of transferred file. Whereas, for other applications hash value of video file get changed.

b) Exposure Date & File Name: date of receiving and date of downloading of the video files on these apps can differ and the name of the saved video file mostly depends on the date and time of downloading of these video files, as can be seen from Table.3.

TABLE 3
Metadata Properties of video files received through various instant messaging apps and for original Source file

Properties ∨	**Metadata Properties at receiving end 02**				**Metadata Properties at Source**
Application Name >	**WhatsApp**	**Telegram**	**Facebook Messenger**	**QQi**	
Exposure Date • **Receiving** • **Downloading**	**04/10/2018** **09/10/2018**	**15/10/2018** **15/10/2018**	**05/10/2018** **09/10/2018**	**04/10/18** **05/10/18**	Creation: **04/10/2018** Sending: **04/10/2018**
General Properties:					
File Name	VID-20181009-WA0000	5_6172214724176904214	received_275455243091901	20181004_150603	20181004_150603
Format	MPEG-4	MPEG-4	MPEG-4	MPEG-4	MPEG-4
Codec ID	mp42 (isom/mp42)	isom (isom/iso2/avc1/mp41)	isom (isom/iso2/avc1/mp41)	mp42 (isom/mp42)	mp42 (isom/mp42)
File Size	7.27 MiB	6.63 MiB	534 KiB	7.27 MiB	7.27 MiB
Duration	18 s 176 ms	18 s 178 ms	18 s 234 ms	18 s 176 ms	18 s 176 ms
Overall bit rate	3 356 kb/s	3 062 kb/s	240 kb/s	3 356 kb/s	3 356 kb/s
Video Properties:					
Bit rate	3 096 kb/s	2 797 kb/s	167 kb/s	3 096 kb/s	3 096 kb/s
Width	640 pixels	480 pixels	480 pixels	640 pixels	640 pixels
Height	480 pixels	640 pixels	640 pixels	480 pixels	480 pixels
Resolution	640x480	640x480	640x480	640x480	640x480
Display Aspect ratio	4:3	0.750	0.750	4:3	4:3
Frame Rate	30.041 FPS	30.041 FPS	30.000 FPS	30.041 FPS	30.041 FPS
Bits/ (pixel*frame)	0.335	0.303	0.018	0.335	0.335
Audio properties:					
Bit rate	256 kb/s	256 kb/s	64.0 kb/s	256 kb/s	256 kb/s
Sampling rate	48.0 kHz	48.0 kHz	48.0 kHz	48.0 kHz	48.0 kHz
Frame rate	46.875 FPS (1024 SPF)	46.875 FPS (1024 SPF)	46.875 FPS (1024 SPF)	46.875FPS(1024 SPF)	46.875FPS(1024 SPF)

c) Table.3 shows that source or digital cameras of mobile phone have captured the video in Quick time-based container formats MPEG-4 with selected compression codec's i.e. in mp42 (isom/mp42). While sending or receiving a particular video file via different instant messaging applications, some change or compression occurs in codecs of video files. These variations in codec String is clearly visible in Table.3 for different types of instant messaging applications. As we have used short video of a few seconds and of low quality for present study, variation is visible only in video files of Telegram and face book messenger clearly. Not much difference is observed in video files forwarded using WhatsApp and QQi applications.

d) Due to individual compression codec of particular application and their maximum file

quality criteria restrictions, while processing any video message; File size, Audio and video bit rate, Frame rate and Display aspect ratio etc. also get affected as seen in Table.3.

e) Bitrate generally determines the size and quality of video and audio files: the higher the bitrate, the better the quality and the larger the file size because

File size = bitrate (kilobits per second) x duration.

here, 1 byte per second (1 B/s) corresponds to 8 bit/s.

Bitrate for full video and individually for video and its audio have also been calculated and compared which clearly shows variation as per Table.3 and ratio for video i.e. Bits/ (pixel*frame) also shows variation and this is clearly shown in Figure.2

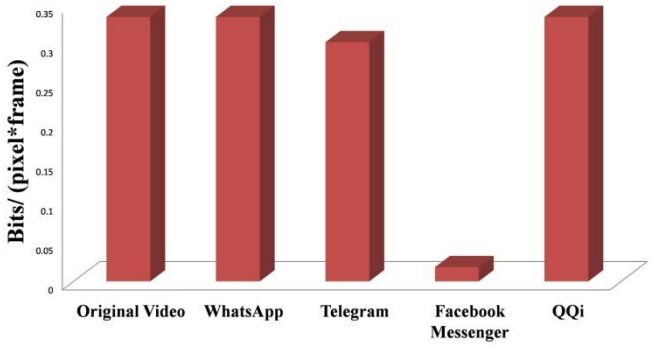

Figure2. Comparison of video properties i.e. ratio Bits/ (pixel*frame) with the all instant massaging app and original video as in Table.3.

TABLE 4.

Amplitude Statistics of all video files received through various instant messaging apps and for original Source file.

Properties ∨	Metadata Properties at receiving end 02				Metadata Properties at Source
Application Name >	WhatsApp	Telegram	Facebook Messenger	QQi	
Amplitude statistics of Audio:					
Peak amplitude: Left Right	 -0.509 dB -0.509 dB	 -0.509 dB -0.509 dB	 -0.027dB -0.027dB	 -0.509 dB -0.509 dB	 -0.509 dB -0.509 dB
Peak amplitude value: Left Right	 0.943103 0.943103	 0.943103 0.943103	 0.996924 0.996924	 0.943103 0.943103	 0.943103 0.943103
DC offset: Left Right	 -0.000602 -0.000602	 -0.000602 -0.000602	 -0.000577 -0.000577	 -0.000602 -0.000602	 -0.000602 -0.000602
Possibly clipped	0	0	0	0	0
Loudness: Left Right	 -18.55 LUFS -18.55 LUFS	 -18.55 LUFS -18.55 LUFS	 -18.57 LUFS -18.57 LUFS	 -18.55 LUFS -18.55 LUFS	 -18.55 LUFS -18.55 LUFS
Mean Loudness:	-15.54 LUFS	-15.54 LUFS	-15.56 LUFS	-15.54 LUFS	-15.54 LUFS
Loudness range: Left Right	 19.92 LU 19.92 LU	 19.92 LU 19.92 LU	 19.30 LU 19.30 LU	 19.92 LU 19.92 LU	 19.92 LU 19.92 LU
Mean Loudness range:	19.92 LU	19.92 LU	19.30 LU	19.92 LU	19.92 LU

This study of metadata of video files gives many important points to consider while examining the Video cases and how the properties of these video files change when forwarded by users of different applications of Smartphones. These metadata properties of video files also lead to many crucial information about video files which can be applied as a tool in identifying the authenticity of any video and can be used to find out, if any manipulation or tampering was done in between forwarding of any video messages. Moreover, audio of any video file also plays a very important role as a forensic evidence because voice quality and its spectrograph can be utilized as forensic investigation tools for voice identification and authentication. Therefore, it is also important to know how the properties of Voice or Audio files gets changed while transmitting/sending through instant messaging applications. For this, we have also analyzed and compared the Amplitude Statistics of all these files using Gold Wave Software. Gold Wave is a commercial digital audio editing software. Amplitude statistics of video file at source end and of all video files received through various instant messaging apps are shown in Table.3. On comparing, it was found that for the particular video file, audio properties like sampling rate (see Table.3.), Peak amplitude and loudness does not get affected generally but for Facebook messenger, variation in peak amplitude up to -0.027 dB from -0.509 dB of original file and in loudness was observed.

IV. CONCLUSION

In the present paper, we have discussed the forensic analysis of the artifacts left by various instant messaging applications on smartphones, and we have shown how these artifacts can provide various information of evidentiary value. Particularly this study was aimed to focus on analyzing and finding the changes occurred in properties of any video files when sent through various instant messaging applications on smartphone.

Results obtained from this study gives an idea of how the properties of video message like its hash value, codec's, audio-video properties, frame rate, bit rate, sampling rate, aspect ratio and audio amplitude statistics etc. get changed when transmitted through different instant messaging applications. It was observed that QQi has transferred video file in its original form without any modification or compression as the Hash value of the received video was same as of the original video. But when the same file gets transferred through Facebook Messenger and Telegram, compression was observed. This degradation in quality and number of frames etc. can lead to loss in valuable information that can be found on these types of short videos of interest in any criminal case examination. In case of WhatsApp, for the sample short video, no variation in parameters was observed and only file name got changed. Moreover, it was found that file transmitted through Facebook messenger suffered maximum compression, even its audio peak amplitude got decreased up to -0.027 dB from -0.509 dB and variation in loudness was also observed. This variation in Audio parameters affect the file authenticity and its usability for probable voice spectrogram analysis with suspected voice for any case.

In the present study, we have taken a short video sample of time duration ~18 sec only. Thus, the results presented is according to it only. If the size or duration of video file is large then the compression behaviour may vary for all four instant messaging applications. Comparison results presented in this paper will help forensic investigators and investigation agencies in examining such video files in any criminal cases by considering behaviour of compression of files on the basis of application used. This work has vast application and can be extended to authentication of fake audio-video messages which get viral through various messaging applications.

V. ACKNOWLEDGEMENT

The authors gratefully acknowledge the support given by, Shri Dr. S.K. Jain, Director cum-CFS, DFSS, MHA,GOI, New Delhi; Shri M. C. Joshi, Director, CFSL Hyderabad.

VI. REFERENCES

[1]. Aditya Mahajan et.al, "Forensic Analysis of Instant Messenger Applications on Android Devices", International Journal of Computer Applications, Volume 68– No.8, April 2013. DOI: 10.5120/11602-6965.

[2]. CosimoAnglano, " Forensic analysis of WhatsApp Messenger on Android smartphones"DigitalInvestigationVolume 11, Issue 3, September 2014, Pages 201-213. DOI: 10.1016/j.diin.2014.04.003

[3]. Thomas Gloe et.al., "Forensic analysis of video file formats" Digital Investigation, Volume 11, Supplement 1, May 2014, Pages S68-S76. DOI: 10.1016/j.diin.2014.03.009.

[4]. Y.-J. Chen et al., "Analysis of Video Quality Variation with Different Bit Rates of H.264 Compression", Journal of Computer and Communications, Vol.4 No.5, May 2016. DOI: 10.4236/jcc.2016.45005.

[5]. D. Calibo, & J. Niguidula "Metadata Extraction Analysis: A Review of Video Data in Effect to Social Media Compression," JOIV : International Journal on Informatics Visualization, vol. 3, no. 1, , pp. 54 - 58, Jan. 2019. DOI: https://doi.org/10.30630/joiv.3.1.216

[6]. J. Randolph Hall,"MPEG--4 Video Authentication Using File Structure And Metadata" MS (Media Forensics) Thesis, University of Colorado, 2015. Available Online at: https://www.ucdenver.edu/ docs/librariesprovider27/ncmf-docs/theses/hall_thesis_fall2015.pdf?sfvrsn=8c4e97b8_2.

[7]. "Most popular global mobile messaging apps 2020", Published by J. Clement, Jul 24, 2020, Available online : https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps

Cite this article as :

Ritika Verma, Anju Pathania, "A Study on Video-Files Sent Through Popular Instant Messaging Applications on Smartphones for Forensics Investigation", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 4, pp. 484-491, July-August 2021. Journal URL : https://ijsrcseit.com/CSEIT2173170