Characteristics of WeChat formation images for forensic applications

Xiulian Qiu[a], Jinhua Zeng[*b,c,d,e]
[a]Forensic Science Center, East China University of Political Science and Law, Shanghai 201620, China; [b]Academy of Forensic Science, Shanghai 200063, China; [c]School of Software Engineering, Chengdu University of Information Technology, Chengdu 610225, China; [d]Shanghai Forensic Service Platform, Shanghai 200063, China; [e]Key Laboratory of Forensic Science, Ministry of Justice, Shanghai 200063, China

ABSTRACT

Images formed by WeChat are widely used as a type of evidence in courts. The research on their image characteristics is of great significance to forensic science application. In this paper, we study the characteristics of the WeChat formed images and videos. Their file attributes, metadata, and digital data change features are systematically studied under the different operating system environments, different program versions, different formation methods, different transmission methods, etc. The forensic examination on the WeChat formed images is further discussed, involving image formation time identification, image source identification, image authenticity identification, and so on. Our results show that the images and videos formed by the WeChat program have their own unique image characteristics, which can be effectively applied for forensic examination of the WeChat formed images.

Keywords: Forensic science, WeChat program, WeChat formed images and videos, forensic authenticity identification, forensic formation time identification

1. INTRODUCTION

WeChat was born in 2011 and has become a truly popular application program in China with over 1.2 billion users by 2022. The record forms in the WeChat include text, voice, image, video, and other types of data. WeChat users inevitably interact with audio-visual materials in a various way when they use the program. Moreover, audio-visual materials are an important type of legal evidence in China. Experts have to verify the authenticity of the submitted evidence, which maybe claimed to be generated, transmitted, or downloaded by the WeChat program.

In the research of passive forensic techniques for forensic image authentication, there are lots of outcomes in the forensic science[1,2]. Image tampering usually goes through the following steps, that are original image acquisition, image editing, post-editing processing and "Save As" operation. Tampering artifact detection in each step has become an important breakthrough in the domain research. For example, in the original image acquisition stage, the source of the image can be effectively estimated by detecting the device pattern noises, so as to determine whether the suspected image is originated from the claimed shooting device[3,4]. The "Save As" operation during image editing usually involves the image recompression process. Based on the above fact, the recompression detection of JPEG images is proposed to detect tampering[5]. In the post-editing stage, the tampering artifact detection methods include blurring operation detection, contrast adjustment detection[6], etc. In terms of image editing detection, regional image copy detection methods[7,8] is common way for image forgery detection. With regard to the video tampering detection research, the corresponding methods mainly focus on video coding artifact detection[9,10], video content tampering detection, etc.

In practice of forensic image authentication, the key techniques consist of storage media inspection, recording system inspection, file attribute/metadata inspection, single-frame picture inspection, audio inspection, video inspection, recording equipment inspection, digital watermark analysis, and so on. This paper focuses on the study of the file attributes and metadata characteristics of images and videos formed by WeChat program, which are analyzed under the different operating system environments, different program versions, different formation methods, different transmission methods, etc. The application of the above results in the field of forensic science is further discussed in the paper.

*zengjh@ssfjd.cn; phone 86 021 52369723

International Conference on Optics, Electronics, and Communication Engineering (OECE 2024), edited by Yang Yue, Proc. of SPIE Vol. 13395, 133954C · © 2024 SPIE · 0277-786X · Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.3048363

2. EXPERIMENTAL DATA

In the experiments, three different mobile phone operating systems are studied. The selected mobile phones including HUAWEI P30 Pro, OnePlus 9 and iPhone 11, and the detailed information is shown in Table 1.

Table 1. The studied mobile phone information.

No.	Cell phone brand and model	System version	WeChat version
1	HUAWEI P30 Pro	HarmonyOS 3.0.0.168	8.0.41
2	OnePlus 9	ColorOS 12.1, Android 12	8.0.33
3	iPhone 11	iOS 16.6.1	8.0.41

For the acquisition of experimental data, three images and two videos were taken by using the shooting function in the WeChat of the studied cell phones, and then were saved to the cell phones by using the download function in the WeChat. In addition, the computer version of WeChat (WeChat 3.9.6.24) was installed in a 64-bit educational version of Windows 10 system, and the above images and videos were downloaded by using this WeChat version for further study.

3. FILE NAMING AND STORAGE PATH FEATURES

3.1 Original storage path

The default storage path for taken images and downloaded images on the No.1 cell phone is "\Internal Storage\images\WeiXin". For taken and downloaded videos, the default storage path is "\Internal Storage\DCIM\WeiXin". For the No. 2 cell phone, the default storage path for taken and downloaded videos is "Internal Shared Storage \images\WeiXin", and the storage path for videos is same to the images. With regard to the No. 3 cell phone, the default storage path for typical taken and downloaded examples of images and videos both are "Internal Storage\DCIM\202309", where "202309" folder is the information of the year and month when the images or videos were taken.

3.2 File naming conventions

The typical name of a sample image taken by the No. 1 cell phone is shown as "wx_camera_1695025042129.jpg", which contains the fixed "wx_camera" prefix and the ".jpg" suffix. The middle number "1695025042129" indicate the Unix timestamp information of the modification time, which can be converted to China standard time "2023-09-18 16:17:22" in "Year/Month/Day Hour:Minute:Second" format. The file name of a sample image downloaded from WeChat in No. 1 cell phone is named as "mmexport1695025100052.jpg", which contains the fixed prefix "mmexport" and ".jpg" suffix. The middle number "1695025100052" is the Unix timestamp information of the image modification time, that is "2023-09-18 16:18:20" in China standard time. With regard to the formed videos in the No. 1 cell phone, the typical sample names are "wx_camera_1695103775816.mp4" and "mmexport1695103798728.mp4" respectively for the recorded video and the downloaded one. The middle numbers are the Unix timestamp information of the last modification times of the videos. The file names of the images and videos taken or downloaded in the WeChat of the No. 2 cell phone are basically the same as those in the No. 1 cell phone.

In the No. 3 cell phone, the typical sample images taken in the WeChat is shown as "IMG_8538.JPG", which contains the fixed "IMG" prefix and ".JPG" suffix. The number "8538" in the middle of the file name is the production order number of the image. For the downloaded image, the typical sample name is shown as "DEYH8777.JPG", which contains a four-uppercase letter prefix plus a four-digit number and a ".JPG" suffix. The meanings of the letters and digits in the file name are not known yet. The sample filenames of the video recorded and downloaded in the WeChat are named as "APOX6276.MP4" and "QRCH7388.MP4" respectively, which contain a four-uppercase letter prefix plus four digits and a ".MP4" suffix.

In computer version of the WeChat program, the naming pattern of the image file sent by the No. 1 to No. 3 cell phones is consistent, and the typical file name is "WeChat Picture_20230919155626.jpg", which contains the fixed "WeChat Picture" prefix and ".jpg" suffix. The number in the middle indicates the time when the image was received in the WeChat program. With regard to formed videos, the naming methods of the videos sent by the No.1 and No.2 cell phone are the same. The typical sample file name is "ddaf6d643e99357cda753c76e47d6f9f.mp4", in which the 32 characters

should be the MD5 hash value. A typical file name for a video sent from the No.3 cell phone is "WeChat_20230915132723.mp4", which contains a fixed "WeChat_" prefix and ".mp4" suffix, and the middle numbers indicate the time when the video was received in the WeChat program.

4. FILE ATTRIBUTE AND METADATA FEATURES

By directly linking the experimental cell phones to the computer, the digital data in the internal storage are studied. It is found that the file attributes and metadata characteristics of the formed images and videos in No. 1 and No. 2 are basically the same. Here, we use the No. 1 cell phone data as an example to analyze the file attributes/metadata features in the No. 1 and No. 2 cell phones.

The file attributes of the images and videos taken or downloaded from the WeChat of the No. 1 cell phone consist of the information of file modification time, file size, original file name, etc. There is no data in the "creation time" column. In terms of metadata information, the typical metadata of the images and videos in No. 1 cell phone are shown in Figures 1 and 2. The metadata of the taken images and recorded videos are exactly the same with the downloaded ones.

	---- JFIF ----
JFIFVersion	1.01
ResolutionUnit	None
XResolution	1
YResolution	1
	---- ICC_Profile ----
ProfileCMMType	
ProfileVersion	2.1.0
ProfileClass	Display Device Profile
ColorSpaceData	RGB
ProfileConnectionSpace	XYZ
ProfileDateTime	0000:00:00 00:00:00
ProfileFileSignature	acsp
PrimaryPlatform	Unknown ()
CMMFlags	Not Embedded, Independent
DeviceManufacturer	
DeviceModel	
DeviceAttributes	Reflective, Glossy, Positive, Color
RenderingIntent	Media-Relative Colorimetric
ConnectionSpaceIlluminant	0.9642 1 0.82491
ProfileCreator	
ProfileID	0
ProfileDescription	sRGB
RedMatrixColumn	0.43607 0.22249 0.01392
GreenMatrixColumn	0.38515 0.71687 0.09708
BlueMatrixColumn	0.14307 0.06061 0.7141
RedTRC	(Binary data 40 bytes, use -b option to extract)
GreenTRC	(Binary data 40 bytes, use -b option to extract)
BlueTRC	(Binary data 40 bytes, use -b option to extract)
MediaWhitePoint	0.9642 1 0.82491
ProfileCopyright	Google Inc. 2016

Figure 1. Metadata of an image taken by the WeChat in the No. 1 cell phone.

	---- QuickTime ----		
MajorBrand	MP4 Base Media v1 [IS0 14496-12:2003]		
MinorVersion	0.2.0	MediaTimeScale	90000
CompatibleBrands	isom*iso2*avc1*mp41	MediaDuration	8.22 s
Version	0	MediaLanguageCode	und
CreateDate	1900:01:00 00:00:00	HandlerType	Video Track
ModifyDate	1900:01:00 00:00:00	HandlerDescription	VideoHandler
TimeScale	1000	GraphicsMode	srcCopy
Duration	8.22 s	OpColor	0 0 0
PreferredRate	1	CompressorID	avc1
PreferredVolume	100.00%	SourceImageWidth	720
MatrixStructure	1 0 0 0 1 0 0 0 1	SourceImageHeight	1280
PreviewTime	0 s	XResolution	72
PreviewDuration	0 s	YResolution	72
PosterTime	0 s	BitDepth	24
SelectionTime	0 s	VideoFrameRate	24.70
SelectionDuration	0 s	TrackVersion	0
CurrentTime	0 s	TrackCreateDate	1900:01:00 00:00:00
NextTrackID	3	TrackModifyDate	1900:01:00 00:00:00
TrackVersion	0	TrackID	2
TrackCreateDate	1900:01:00 00:00:00	TrackDuration	8.18 s
TrackModifyDate	1900:01:00 00:00:00	TrackLayer	0
TrackID	1	TrackVolume	100.00%
TrackDuration	8.22 s	MatrixStructure	1 0 0 0 1 0 0 0 1
TrackLayer	0	MediaHeaderVersion	0
TrackVolume	0.00%	MediaCreateDate	1900:01:00 00:00:00
MatrixStructure	1 0 0 0 1 0 0 0 1	MediaModifyDate	1900:01:00 00:00:00
ImageWidth	720	MediaTimeScale	44100
ImageHeight	1280	MediaDuration	8.17 s
MediaHeaderVersion	0	MediaLanguageCode	und
MediaCreateDate	1900:01:00 00:00:00	HandlerType	Audio Track
MediaModifyDate	1900:01:00 00:00:00		

Figure 2. Metadata of a video captured by the WeChat in the No. 1 cell phone.

In Figure 1, the creation time of image in metadata is the default “0000:00:00 00:00:00”. In Figure 2, it can be seen that the creation time and modification time of the video file in the metadata is the default “1900:01:00 00:00:00”. There is little valid information in metadata, but the structure of metadata is an important forensic feature.

In the No. 3 cell phone, we can see the “creation time”, “modification time”, “file size” information of the WeChat formed images and videos. Among them, the “creation time” is the time when the file is completely saved. The initial “modification time” is the time when the writing of the file in the storage is completed, but in the existing Apple iOS, the “modification time” of the image file may change automatically with the use of the cell phone. In terms of metadata, the typical metadata of the images and video are shown in Figures 3 and 4. The metadata of the recorded video are exactly the same with the downloaded one.

	---- JFIF ----
JFIFVersion	1.01
ResolutionUnit	None
XResolution	72
YResolution	72
	---- EXIF ----
Orientation	Horizontal (normal)
XResolution	72
YResolution	72
ResolutionUnit	inches
YCbCrPositioning	Centered
ExifVersion	0221
ComponentsConfiguration	Y, Cb, Cr, -
FlashpixVersion	0100
ColorSpace	sRGB
ExifImageWidth	1080
ExifImageHeight	1920
SceneCaptureType	Standard
Compression	JPEG (old-style)
XResolution	72
YResolution	72
ResolutionUnit	inches
ThumbnailOffset	316
ThumbnailLength	3200
	---- Photoshop ----
IPTCDigest	d41d8cd98f00b204e9800998ecf8427e

Figure 3. Metadata of an image taken by the WeChat in the No. 3 cell phone.

	---- QuickTime ----
MajorBrand	MP4 v2 [ISO 14496-14]
MinorVersion	0.0.1
CompatibleBrands	isom*mp41*mp42
Version	0
CreateDate	2023:09:19 07:54:25
ModifyDate	2023:09:19 07:54:28
TimeScale	44100
Duration	7.53 s
PreferredRate	1
PreferredVolume	100.00%
MatrixStructure	1 0 0 0 1 0 0 0 1
PreviewTime	0 s
PreviewDuration	0 s
PosterTime	0 s
SelectionTime	0 s
SelectionDuration	0 s
CurrentTime	0 s
NextTrackID	3
TrackVersion	0
TrackCreateDate	2023:09:19 07:54:25
TrackModifyDate	2023:09:19 07:54:28
TrackID	1
TrackDuration	7.53 s
TrackLayer	0
TrackVolume	0.00%
MatrixStructure	1 0 0 0 1 0 0 0 1
ImageWidth	720
ImageHeight	1280
MediaHeaderVersion	0
MediaCreateDate	2023:09:19 07:54:25
MediaModifyDate	2023:09:19 07:54:28

MediaTimeScale	600
MediaDuration	7.53 s
MediaLanguageCode	und
HandlerType	Video Track
HandlerDescription	Core Media Video
GraphicsMode	srcCopy
OpColor	0 0 0
CompressorID	avc1
SourceImageWidth	720
SourceImageHeight	1280
XResolution	72
YResolution	72
BitDepth	24
VideoFrameRate	30.01
TrackVersion	0
TrackCreateDate	2023:09:19 07:54:25
TrackModifyDate	2023:09:19 07:54:28
TrackID	2
TrackDuration	7.50 s
TrackLayer	0
TrackVolume	100.00%
MatrixStructure	1 0 0 0 1 0 0 0 1
MediaHeaderVersion	0
MediaCreateDate	2023:09:19 07:54:25
MediaModifyDate	2023:09:19 07:54:28
MediaTimeScale	44100
MediaDuration	7.55 s
MediaLanguageCode	und
HandlerType	Audio Track

Figure 4. Metadata of a video captured by the WeChat in the No. 3 cell phone.

In Figure 3, there is no time-related information in the metadata, which only contains data such as screen resolution, etc. In Figure 4, it can be seen that the metadata contains rich forensic information, including the creation time, modification

time, duration, screen size and other important information of the video file. The metadata structure is also an important distinguishable feature.

A typical example of metadata for images downloaded from the computer version of the WeChat program is shown in Figure 5. There is less valid information in the metadata. The metadata of the downloaded video is consistent with the metadata of the video captured or downloaded in the No. 3 cell phones.

FileSize	145 kB
FileModifyDate	2023:09:19 15:56:48+08:00
FilePermissions	rw-rw-rw-
FileType	JPEG
MIMEType	image/jpeg
ImageWidth	1080
ImageHeight	1920
EncodingProcess	Baseline DCT, Huffman coding
BitsPerSample	8
ColorComponents	3
YCbCrSubSampling	YCbCr4:2:0 (2 2)
	---- **JFIF** ----
JFIFVersion	1.01
ResolutionUnit	None
XResolution	1
YResolution	1

Figure 5. Metadata of the downloaded images in the computer version of the WeChat program.

5. DIGITAL DATA CHANGING FEATURES

In the No. 1 cell phone, the hash value of the images taken in the WeChat is same to the downloaded images, i.e., the file data are identical. However, there is a big difference between the taken images in the No. 1 cell phone and the downloaded images from the computer version WeChat. By comparing the hexadecimal data of the two files, we find that the latter should be re-encoded, the size of the file becomes smaller, and the structure of the metadata is also changed, as shown in Figure 6.

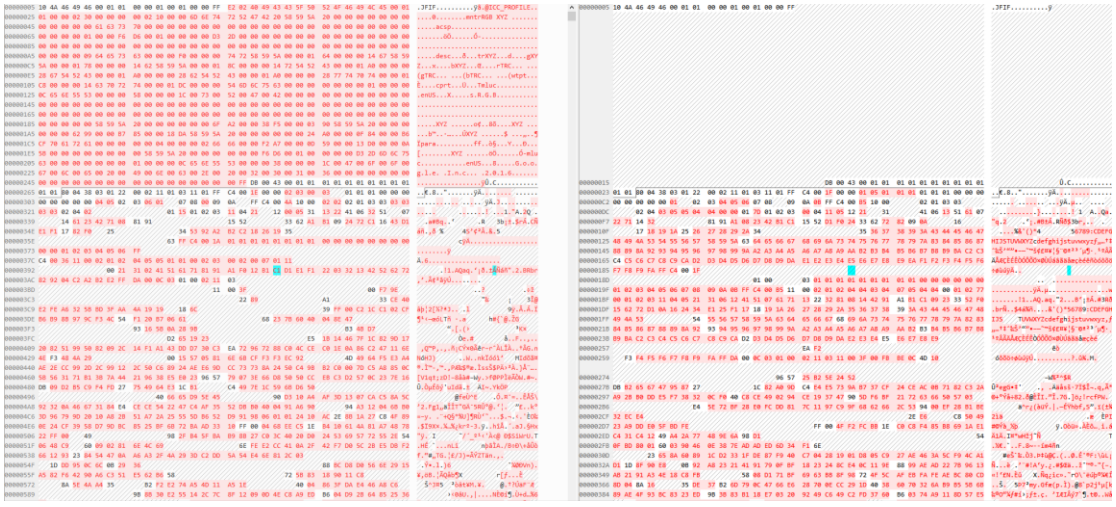

Figure 6. Differences in file header data between the taken image in the No. 1 cell phone and the image downloaded from the computer version of the WeChat.

The hash values of the video downloaded from the No. 1 cell phone and the video downloaded from the computer version WeChat are the same, i.e., the file data are identical. However, the captured video and the downloaded video have slight differences in the meta-data information and also in file sizes. The comparing of the hexadecimal data between the two video files is shown in Figure 7. The digital change feature of files in the No. 2 cell phone is basically the same as in the No. 1 cell phone, and will not be described in detail here.

With regard to the features of the No. 3 cell phone, we find that the hash values of the taken images, the downloaded images and the downloaded images in computer version WeChat are different. There are obvious differences in the

metadata structure. Among them, there is not much difference in the file size between the taken images the downloaded ones, but the size of the downloaded images in computer version WeChat has obviously been reduced. When considering to the formed videos, the recorded video, the downloaded video and the downloaded video in computer version WeChat are identical, that is, their hash values are the same.

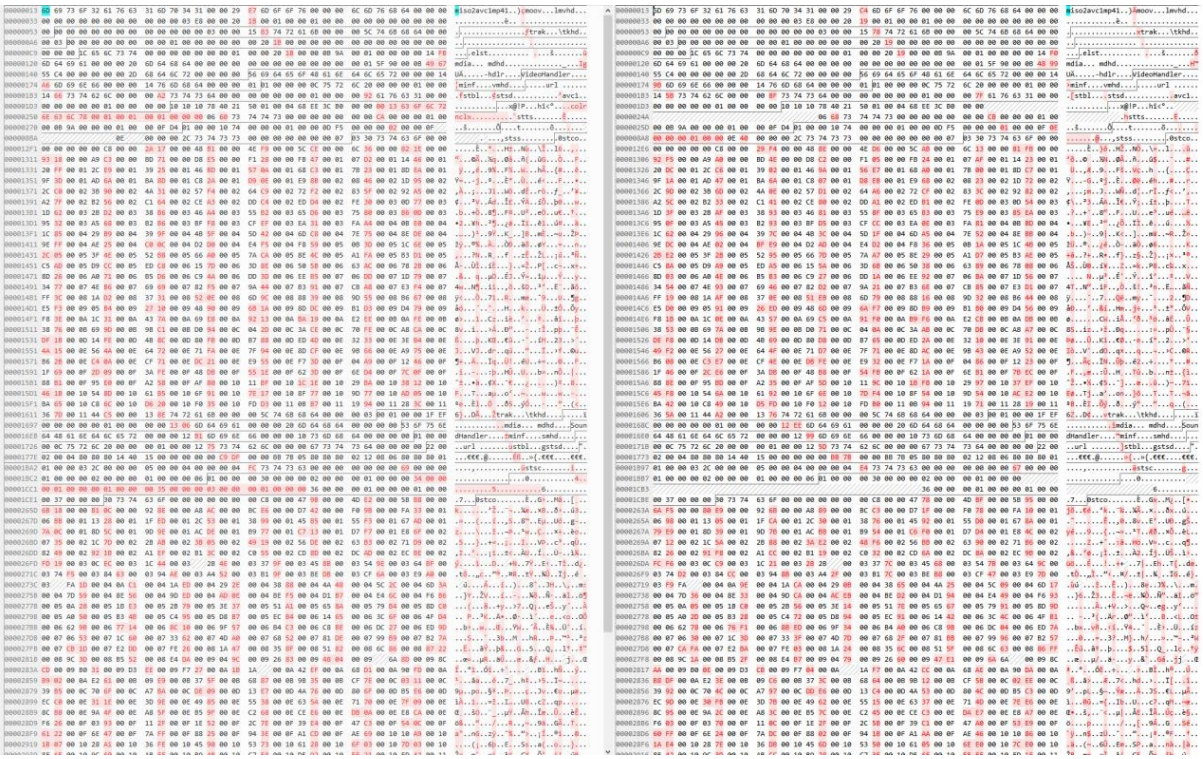

Figure 7. The comparing of the hexadecimal data between the captured video and the downloaded video in the No. 1 cell phone.

6. DISCUSSIONS AND CONCLUSIONS

Forensic examination involving WeChat formed images and videos consists of formation time identification, source identification, image authenticity identification, etc. The WeChat image formation time information mainly involves the image shooting time, sending time and so on. This information can be analyzed by using the image filename and the time-related metadata information. In the forensic shooting time examination of the WeChat formed images, whether the images are original or tampered should be estimated firstly.

With regard to WeChat image source identification, it aims to judge whether the suspected image is formed by WeChat. Source identification is the main inspect angle and content in forensic authenticity identification, we can analyze the file name, file size, encoding mode and metadata structure of the suspected image or video to estimate whether they are formed by WeChat.

To sum up, this paper researches on the characteristics of WeChat formed images and videos. The file attributes, metadata characteristics and digital data changes under different operating system environments, different WeChat versions, different formation methods, different transmission methods and so on, were comprehensively studied. Our results have a good guiding effect on the forensics research related to the formation time identification, image source identification, image authenticity identification of the WeChat formed images and videos.

ACKNOWLEDGMENT

This work was supported by the Shanghai Science and Technology Commission Project (21DZ2200100) and the Ministry of Finance, PR China (GY2024G-6).

REFERENCES

[1] Li, X., Yu, N., Zhang, X., Zhang, W., Li, B., Lu, W., Wang, W. and Liu, X., "Overview of digital media forensics technology," Journal of Image and Graphics 26(06), 1216-1226 (2021).

[2] Zeng, J., Lu, W., Yang, R. and Qiu, X., "Practical tools for digital image forensic authentication," Advanced Multimedia and Ubiquitous Engineering, Lecture Notes in Electrical Engineering 393, (2016).

[3] Lawgaly, A. and Khelifi, F., "Sensor pattern noise estimation based on improved locally adaptive DCT filtering and weighted averaging for source camera identification and verification," IEEE Transactions on Information Forensics and Security 12(2), 392-404 (2017).

[4] Chierchia, G., Cozzolino, D., Poggi, G., Sansone, C. and Verdoliva, L., "Guided filtering for PRNU-based localization of small-size image forgeries," Proceedings of 2014 IEEE International Conference on Acoustics, Speech and Signal Processing, Florence, Italy, 6231-6235 (2014).

[5] Galvan, F., Puglisi, G., Bruna, A. R. and Battiato, S., "First quantization matrix estimation from double compressed JPEG images," IEEE Transactions on Information Forensics and Security 9(8), 1299-1310 (2014).

[6] Cao, G., Zhao, Y., Ni, R. R. and Li, X. L., "Contrast enhancement-based forensics in digital images," IEEE Transactions on Information Forensics and Security 9(3), 515-525 (2014).

[7] Cozzolino, D., Poggi, G. and Verdoliva, L., "Efficient dense-field copymove forgery detection," IEEE Transactions on Information Forensics and Security 10(11), 2284-2297 (2015).

[8] Li, J., Li, X. L., Yang, B. and Sun, X. M., "Segmentation-based image copy-move forgery detection scheme," IEEE Transactions on Information Forensics and Security 10(3), 507-518 (2015).

[9] Liao, D. D., Yang, R., Liu, H. M., Li, J. and Huang, J. W., "Double H.264/AVC compression detection using quantized nonzero AC coefficients," Proceedings of SPIE 7880, Media Watermarking, Security, and Forensics III, San Francisco, USA, 78800Q (2011).

[10] Stamm, M. C., Lin, W. S. and Liu, K. J. R., "Temporal forensics and antiforensics for motion compensated video," IEEE Transactions on Information Forensics and Security 7(4), 1315-1329 (2012).