

Analysis Forensic Video in Storage Data Using Tampering Method

By Imam Riadi

Analysis of Forensic Video in Storage Data Using Tampering Method

Amirul Putra Justicia¹, Imam Riadi²

¹ Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

² Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
(amirul1400018033@webmail.uad.ac.id, imam.riadi@js.uad.ac.id)

ABSTRACT

In the legal world, a evidence of video recording has a high level of confidence and is often the evidence. This raises the issue of ensuring an original video or engineering result in digital evidence in the form of forensic video on storage data. One form of engineering that can be done on the video is tampering. The technique used is zooming, Laplacian sharpening, contrast brightness, optical deblurring, turbulence deblurring, exposure, temperature tint, Wiener filter, bilateral filter, unsharp masking and homomorphic filter. The result shows that the accuracy of the assessment in case of CCTV video case analysis (CCTV) about car bumping and car tire fitting according to DI Yogyakarta Police investigators who identified in the field of INAFIS said that 70% of identification of CCTV video footage and face of the perpetrator or suspect or attacker already can be processed investigation of evidence.

Keywords: *Video, Forensic, Tampering, Storage, Data*

1 INTRODUCTION

Technological and industrial progress is the result of the human culture in addition to bringing and having positive and negative impacts. On the positives impact that is on the developing human. While the negative impact is to make people act evil in the form of other things in technology. One of the crimes in techonological information related to the system the crime that makes IT systems and facilities (e.g. computer hardware) within the police force is video manipulation when identifying the perpetrator.

During the year 2017, criminal cases in the jurisdiction of Yogyakarta Regional Police of the Republic of Indonesia decreased compared to the previous year. Similarly, the number of cases that have been resolved, increased compared to the year 2016. That the total cases handled by police officers DIY reached 4795 criminal acts. The number decreased by 23.79% compared to last year which reached 6292 criminal cases. As for the number of

cases completed this year amounted to 2632 criminal acts, the number of settlement cases increased from last year. In 2016, out of 6292 criminal cases successfully completed 3066 cases, if presented 48.73% complete. For this year's clearance rate increased, from 4795 cases we successfully completed 2632 cases and if the percentage of successful completion reached 54.89% this year.

So, compared to last year increased 6.06% for cases that were resolved. Of the thousands of cases handled by DIY Police officers this year, some cases have increased or decreased. As the case of narcotics has decreased compared to last year, from 496 to 371 cases. Similarly, the case of theft with the weight (curat) also decreased from 721 to 577 cases. For cases of domestic violence also decreased 13.86 percent, of which last year there were to solve the problem, the method associated with the forensic video is by the Tampering method. Many ways are made to detect whether a content can be manipulated or not. Forensic multimedia research develops in many cases of image and video files.[1] Whereas the level of public confidence in the video is higher than the picture.

In the legal world, for example, a evidence of video recording has a high level of confidence and is often a key evidence to reveal the case because the process of data manipulation such as video recording is considered more difficult than the process of image manipulation. But now the process of video manipulation facilitated by the availability of video editing applications, both open source or paid. These applications make it easy for someone to manipulate the video and the manipulations can look so real that they can be trusted. Although in time, the process of video manipulation takes longer than the process of manipulating images.

So, thereby demanding the existence of an authenticated or original video. This needs to be proved by research that focuses on finding solutions on how to detect them.

2 LITERATURE REVIEW

2.1 Related Works

Figure 1 shows the workflow to relate the works in the research. The process in the works has

three important things such as research sources, methodology and the results of the research.

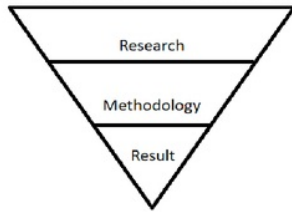


Figure 1. Related Works

According to the earlier inspected other researcher by [1] and [2], forensic video analysis is using tampering data as the methods to manifest the video to be an evidence. The result showed by [1] and [2] to compare the tampering video and original video to check on the texture and sharpness of the video display.

2.2 Digital Forensics

Handling of case related to the use of information technology often requires forensics. Forensic is an activity to conduct investigations and establish facts relating to criminal events and other legal issues. Digital forensics is part of forensic science encompassing the discovery and investigation of the material (data) could be seen figure 2.[3][4]



Figure 2. Application of Digital Forensics

2.3 Storage Data

The data stored on a storage device is mostly confidential or private, so the data must be secured from a third party shown in Figure 3.[5][6]

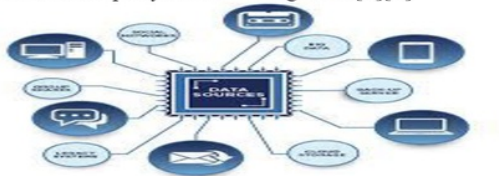


Figure 3. Storage Data

Data Storage in Figure 3 is anything that can be stored in memory according to a certain format. Basically, can be interpreted as Storage is a place to store program instructions and data usage with the computer. Data Storage is one of the most important

tools in a series of tools that reside in a computer. [7][8][9].

2.4 Tampering Method

It can be seen in Figure 4 there are two types of tampering manipulation.

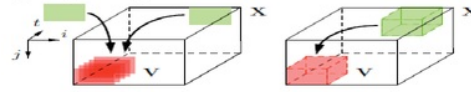


Figure 4. Tampering Video Illustration

The first picture to the left is a tampering process by inserting images into several frames in the video. In the second picture to the right is a tampering process by inserting multiple frame pieces from one video to several different frames in the same video. Many methods have been built to detect tampering with the video. Research conducted on [10] can even detect with two types of tampering. The first way is to detect the presence of spatial copy move or it can be duplicated to a similar object in the same scene or scene using Histogram of Gradients (HOG) matching or lumped. The second way is to detect the existence of temporal copy-move or can by inserting an object from frame to frame by using exploitation.

Research conducted by [11] that detects the presence of tampering on video using noise characteristics. The characteristic of noise possessed by the original frame with the inserted frame pieces has a difference and is very sensitive to the compression process. In the research [12] developed an algorithm to detect the tampering video manipulation, is inserting pieces of certain frames on a number of other frames. The algorithm developed works by forming 3D block on the video and cross-correlation process is done on the 3D block with all parts of the video is non-overlapped.

2.5 Video

Movies or moving images are digital data consisting of multiple images. The term video usually refers to some mobile image storage format. Divided into two, namely analog video, for example, VHS and Betamax, and digital video, for example, DVD, QuickTime, and MPEG-4. Videos can be recorded and transmitted in various physical media in Figure 5.[13][12]



Figure 5. Case Video

3 METHODOLOGY

3.1 Development Stage

It is the stage of doing case simulations to try to implement VideoCleaner in detecting such video footage being manipulated or not. The case simulation aims to perform testing with VideoCleaner in detecting the video recording that will be changed or manipulated the data, so the video recording looks original. Stages of research can be seen in Figure 6. [14]



Figure 6. Research Stages

Tampering video that changes from its original form is a picture and video. Such changes may be classified as intentional or unintentional acts. Accidental Tampering has a malicious purpose by modifying content removing the copyright. In addition, accidental tampering is a consequence of digital operational processes, such as improving brightness, formatting changes, size reduction, etc. In video signals, tampering technique can be classified as spatial and temporal changes. Spatial tampering techniques are tailored to changes made based on pixels on the frame [15].

3.2 Video Simulation Process

The simulation stage starts with preparing the video as a medium for tampering analysis. The Attacker can eliminate evidence by manipulating video it aims to eliminate evidence of Figure 7. [16]

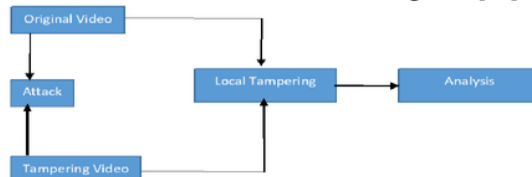


Figure 7. Video Simulation Process

Figure 7 is a tampering video simulation process using attack cropping, zooming, rotation, and grayscale. In the original video made the attack into a video tampering by cropping, zooming, rotation, and grayscale. After the video tampering, it will be analyzed by local tampering method between the original video and video tampering. [15]

3.3 Flowchart Video Tampering Detection

Stages of the flowchart for detecting Video Tampering there are 9 stages. Here's the detecting step with Video Tampering in Figure 8. [16]

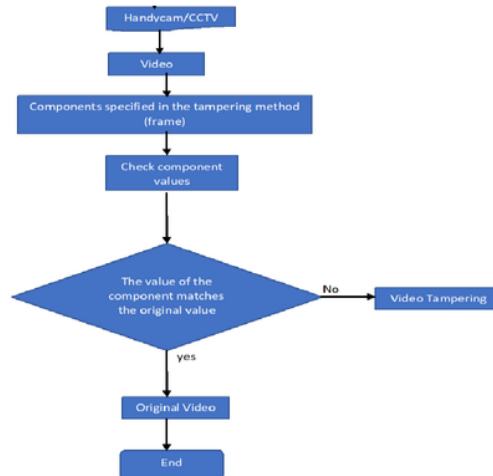


Figure 8. Flowchart Video Tampering Detection

Figure 8 is a process or analytical step for video authenticity detection. The first process is to find a video on the Close-Circuit Television (CCTV) camera for example. Then from the video is done checking the value on the frame. After that from the results of checking, if there is a difference in value then the video is tampering. If the component values are the same, then the video is the original video. The results of the analysis will be known where the differences in frames that have experienced tampering. The similarities of the basic theory were tampering method and differences of the other researchers to prove this study uses of the techniques. Some techniques are used for zooming, Laplacian sharpening, contrast brightness, optical deblurring, turbulence deblurring, exposure, temperature tint, Wiener filter, bilateral filter, unsharp masking and homomorphic filter.

4 RESULTS AND DISCUSSION

4.1 Scenario of Research Plan

The simulation process of finding evidence from CCTV recordings is an early stage done by Yogyakarta Regional Police of the Republic of Indonesia, IT Police investigators in the field of INAFIS (Indonesia Automatic Fingerprint Identification System) to test the CCTV video recording is original or engineering. The simulation

begins with the way when a suspect/attacker or an attacker looks like he did when the incident started through the CCTV camera at the scene of the crime scene. Figure 9 shows the experimental scenario of analyzing CCTV recording data residing in hardware in the form of DVR Decoder (Digital Video Recorder) where the device is neatly mounted on the right side of the scene.

The results of a crime scene, Yogyakarta Regional Police of the Republic of Indonesia police investigators then brought the CCTV video recordings to the lab INAFIS Yogyakarta Regional Police of the Republic of Indonesia workspace to be followed up and identified with Tensor PLC computer in Regional Police of the Republic of Indonesia. Then DIY Police investigators analyzed the video with AMPED FIVE Ultimate 9010 application for analysis. After that investigator, Yogyakarta Regional Police of the Republic of Indonesia will do face matching or face matching. If the video recording is less obvious it will be fixed again in analyzing the video recording with AMPED FIVE Ultimate 9010 application until visible.

If indeed the identification results of the video recording cannot be obtained, it will be forwarded by other DIY Police investigators to be taken to the Police Headquarters conducted investigation of pieces of evidence process. [8][17][18]

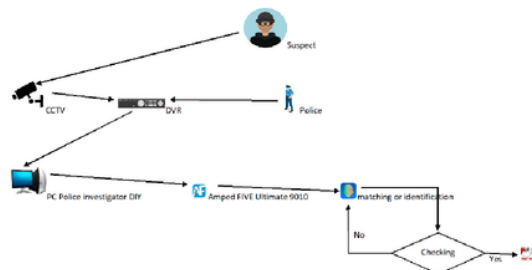


Figure 9. A scenario of Research Plan

Computer Investigator Tensor with IP address 43.249.141.51 serves as a tool to identify the incident of CCTV video recordings in Yogyakarta Regional Police of the Republic of Indonesia. First of all, CCTV video recordings are inserted into the DIY computer Investigator Tensor to be identified for clarity. In Yogyakarta Regional Police of the Republic of Indonesia itself uses digital forensic science to be used as data tensor. The tensor data function itself is to take a picture of CCTV and to clarify the image. The CCTV video footage is from a crime scene (TKP) via DVR (Digital Video Record) on the CCTV camera itself.

Yogyakarta Regional Police of the Republic of Indonesia investigators conducted data acquisition or CCTV video record taking via DVR. The CCTV video clip file is copied to the Tensor Investigator's hard disk computer to be compared to the copied video residing on the DVR. Files result of the acquisition of video recording CCTV DIY Police investigator is the master file.

So, when the investigator Regional Police of the Republic of Indonesia wants to analyze it, must be on the acquisition of the CCTV video recording. The use of digital forensic science itself in Regional Police of the Republic of Indonesia is very important and very effective, even with technology owned by Regional Police of the Republic of Indonesia (computer Tensor Investigator) using digital forensics itself has revealed as many as 4 cases that have been successfully removed by Yogyakarta Regional Police of the Republic of Indonesia investigators from 7 cases since 2017.

The very authentic CCTV video recordings are captured directly through the DVR located at the scene of the crime scene (TKP) or around the scene. Regional Police of the Republic of Indonesia itself in analyzing the case of the case by making edits using Video Investigator application owned by Yogyakarta Regional Police of the Republic of Indonesia and coupled with Amped FIVE Ultimate Build 9010 software to be able to clear the level of accuracy 70% and DI Yogyakarta Police investigators said if the CCTV video recording is genuine. [2]

4.2 Flowchart in video analysis

Figure 10 shows the workflow in verifying CCTV video recording and during the video editing process. The process proves the CCTV video recording to need several processes.

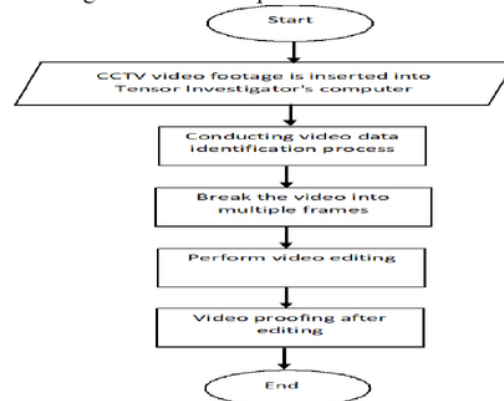


Figure 10. A flowchart in Video Analysis

The stage to prove the video consists of several processes in Figure 10, namely:

1. Evidence of CCTV video recordings from the operator/owner of the DVR CCTV is requested to be directly recorded, then inserted into the Tensor Investigator computer.
2. Police investigators Special DIY INAFIS DIYFIS directly identify the video and search for information contained there in.
3. Yogyakarta Regional Police of the Republic of Indonesia Investigators began to break the CCTV video recordings into frames.
4. After solving the frame, the DIY Police investigator started editing the CCTV video recording.
5. Then the Yogyakarta Regional Police of the Republic of Indonesia investigator proved the result through a video split and Collection of Evidence Remarks at the scene.

4.3 Simulation of CCTV Video Analysis

The process of simulating CCTV video record analysis using video editing with Amped FIVE Ultimate Build 9010 application for clarity and image quality improvement on CCTV video recording found by DIY Police investigators. The simulation begins with the way the CCTV video footage is inserted into the Tensor Investigator computer to be further processed so as to find a bright spot when uncovering the CCTV case.[18]

In table 1 shows that the frame detection scenario on the CCTV video recording in the case of car bundling can be used as evidence for the editing process using the tampering method to the perpetrator who did the car trucking located on Jl. Karel Sasuit Tubun No. 43, Ngampilan, Yogyakarta. In the action 1 (one) person acts to monitor the state of the back of the car (big man wearing a gray shirt, white shorts, black hem no yellow writing behind the hem and white hat), 1 (one) while wearing a black hat, sweater suit, jeans, wearing a wristwatch, wearing a mask (face cover) and shoes), 1 (one) peer as car razor and watching the situation (wearing a gray sweater, a cream-colored trousers, swallow slippers and short-haired crosswords), 1 (one) suspect doing surveillance (wearing a T-shirt (on the back read "REPRESENT YOGYA PARTNER SULTAN"), wearing black shorts and wearing a black hat) and 1) another suspect waited for the other four friends who were stunting the car (wearing a yellow black hem behind the hem, blue shorts, and black hat). [19] [20]



Figure 11. Wheel blocking and car bundling

Figure 11 CCTV video recording shows that the incident of car bleaching started last Sunday on the 11th of March 2018. It is clear from the CCTV video footage showed at 13:06:42 than 2 (two) actors doing the incident (1 (one) fellow suspect carboy and tire car seal from the left side of the car (wearing a black hat, sweater suit, jeans, wearing a wristwatch, wearing masks and shoes), 1 (one) peer as car razor and watched the situation (wearing a gray sweater, beige trousers, swallow slippers and crew-cut hair) began to car the left-handed car wheel and car trucking.[21]

Table 1 Frame detection on video





Attack	Analysis	
	Original Video	Video Tampering
Cropping		
	Frame 40	Frame 40
Conclusion: Zooming and Cropping occurs in frame 40		

Figure 12 is the front-end AMPED FIVE Ultimate 9010 application used to identify and analyze CCTV video case. Tools that exist in the filter in this application include sharpening menu, denoise, deblurring etc. In the sharpen menu itself there are 2 (two) features namely Laplacian sharpening and unsharp masking. Then on the menu denoise, there are 6 (six) features namely Averaging, Filter, Gaussian Filter, Wiener Filter, Bilateral Filter, Median Filter and Deblocking. In the deblurring menu, there are 5 (five) features of Motion Deblurring, Optical Deblurring, Nonlinear Deblurring, Blind Deconvolution and Turbulence Deblurring.[19] It shows the main attacker to be can appear in CCTV.



Figure 12. After the Tempering Method is done by Zooming and Cropping or Cutting on the Frame Perpetrators

Table 2 Frame detection on video

Attack	Analysis	
	Original Video	Video Tampering
Laplacian Sharpening		
	Frame 1	Frame 1

Conclusion: A Sharpening Laplacian occurs in frame 1

Table 2 shows that the frame detection scenario on the CCTV video recording in the case of car bundling uses the Laplacian Sharpening to process to sharpen the image of deblurring results. In the case of car wrecking and tire car seizure, clearly visible CCTV video footage shows that the car is right beside the shop (shop house). In frame 1 of the table is Original video in case of car bundling and tire car tire on Laplacian Sharpening feature. In the Tampering Video table shown on the CCTV record evidence, the picture is clarified using the tampering method to provide an incident in the case shown in frame 1 of the Sharpening Laplacian feature. By doing the tampering method, Yogyakarta Regional Police of the Republic of Indonesia investigators can identify the scene or crime scene clearly.

Process the stages of the method are done by sharpening the image or image location of the incident with the image of the results of purification with AMPED FIVE Ultimate 9010 tools with techniques to sharpen the image or image.

By setting the image using AMPED FIVE software it is known from the position sought or the invention of the frame image to -0 at the second (00: 00: 00: 000) [P] seconds. [P] indicates the position of frame taking and time (00: 00: 00: 000) indicating the time 2018-03-11 13:06:00. Figures 2018 indicate the incident in 2018, month 03 shows the incidence in the

3rd month of March and the 11th appeared the beginning of the incident case in the case of plundering and tire car seal in front of the shop on Jl. Karel Sasuit Tubun No. 43 in Ngampilan area, Yogyakarta. At the time of the incident started seen on the CCTV record of the DVR, can be shown in Figure 13. [5][22]

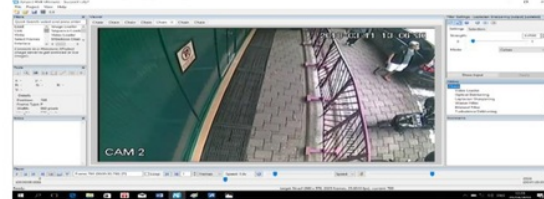
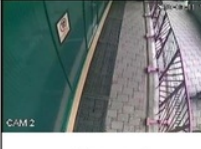



Figure 13. Laplacian Sharpening



Table 3 Frame detection on video

Attack	Analysis	
	Original Video	Video Tampering
Unsharp Masking		
	Frame 1	Frame 1

Conclusion: Unsharp Masking occurs on frame 1

Table 3 shows that the frame detection scenario on the CCTV video recording in the case of car bundling. It uses the Unsharp Masking to detect the location when occurs tampering.

Table 4 Frame detection on video

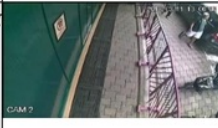

Attack	Analysis	
	Original Video	Video Tampering
Contrast Brightness		
	Frame 40	Frame 40

Conclusion: Unsharp Masking occurs on frame Zooming and Contrast Brightness occurred on frame 40

Table 4 shows that the frame detection scenario on the CCTV video recording in the case of car bundling. Contrast Brightness is the process of improving the opaque contrast of images or images. In the case of car wrecking and tire car seizure, it is clear that CCTV video footage shows that the main perpetrator is beside the left side of the car and the location of the car is on the right side of the shop (shop house). At frame 40 on the table is Original

video in case of car drag and tire car tire on Contrast rightness feature.[15]



Table 5 Frame detection on video

Attack	Analysis	
	Original Video	Video Tampering
Zooming		
	Frame 40	Frame 40

Conclusion: There was zooming on frame 40

Table 5 shows that the frame detection scenario on the CCTV video recording in the case of car bundling. Zooming is the process of increasing the view images sharper.


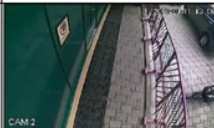
Table 6 Frame detection on video

Attack	Analysis	
	Original Video	Video Tampering
Optical Deblurring		
	Frame 1	Frame 1

Conclusion: Optical Deblurring occurs in frame 1

Table 6 shows that the frame detection scenario on the CCTV video recording in the case of car bundling. Optical Deblurring is the ultimate blend of form and function when using the tampering methods.

Table 7 Frame detection on video



Attack	Analysis	
	Original Video	Video Tampering
Exposure		
	Frame 1	Frame 1

Conclusion: Exposure occurs on frame 1

Table 7 shows that the frame detection scenario on the CCTV video recording in the case of car bundling. Exposure is much the receive the light in camera sensor to take a picture when using the tampering methods.

4.4 Validation of Evidences

Table 8 Validates the Results of the Investigation by Yogyakarta Regional Police of the Republic of Indonesia

Attack	Analysis	
	Original Video	Video Tampering
Turbulence Deblurring		
	Frame 72	Frame 72

Conclusion: There was a Turbulence Deblurring on frame 72

Table 8 shows that the frame detection scenario on the CCTV video recording ⁷ the case of car bundling. Turbulence Deblurring affects the imaging system at a long distance, which causes time-varying blur when using the tampering methods.

Table 9 Validation Video Evidence



Original Video	Videos of Tampering results
 Frame target 40 dan timeline 13:06:30 Position seek 765 Frame 765 (00:00:30:598)	 Frame target 40 dan timeline 13:06:30 Position seek 765 Frame 765 (00:00:30:598)

Table 10 Validation Video Evidence



Original Video	Videos of Tampering results
 Frame target 54 and timeline 13:06:42 Position seek 1077 Frame 1077 (00:00:43:078)	 Frame target 54 and timeline 13:06:42 Position seek 1077 Frame 1077 (00:00:43:078)

Table 9 and table 10 the analytical simulations obtained in Table 4.2 above, during the identification process of the suspect or the offender or the attacker, it was found that the video recording to reveal the truth in the case of car bickering and tire car discharges are exactly the same and the incident does exist. The evidence found by the Yogyakarta Regional Police of the Republic of Indonesia investigator proved to be valid. The level of accuracy of the assessment in case of CCTV video case analysis of car bombing cases and car tire fitting according to DI Yogyakarta Police investigators who

identified in the field of INAFIS said that 70% of the identification of CCTV video footage and face of the perpetrator or suspect or attacker can already be processed and submitted to Police Headquarter in Jakarta for the LIDIK process.[17][23]

4.5 Test Conclusion

Based on the examination in Yogyakarta Regional Police of the Republic of Indonesia that the original video and tampering video was given by Yogyakarta Regional Police of the Republic of Indonesia investigators in proving the truth is the same. CCTV video recording has been through various tests including Optical Deblurring, Turbulence Deblurring, Contrast Brightness, Exposure, Laplacian *Sharpening*, Unsharp Masking, Wiener Filter, Bilateral Filter, Homomorphic Filter and Temperature Tint with AMPED FIVE Ultimate 9010 application, proving that CCTV video recording on case of carbide and tire car seal at the location.

5 CONCLUSIONS

The results reveal the truth in the case of car plundering and tire fitting car completely - exactly the same and the incident does exist. The evidence found by the DI Yogyakarta Police investigator proved to be valid. The accuracy of the assessment in case of CCTV about car bumping and car tire fitting according to DI Yogyakarta Police investigators who identified in the field of INAFIS said that 70% of identification of CCTV video footage and face of the perpetrator or suspect or attacker already can be processed investigation of evidence.

REFERENCES

- [1] F. Sthevanie, "Journal of Computer Engineering Unikom – Komputika – Volume 3, No. 2 - 2014," vol. 3, pp. 23–28, 2014.
- [2] R. D. Singh and N. Aggarwal, "Video Content Authentication Techniques: A Comprehensive Survey," *Multimed. Syst.*, vol. 0, no. 0, pp. 1–30, 2017.
- [3] A. Novianto, "Understanding and Sample Forensic Case Compiled by Graduate Program Faculty of Industrial Engineering Department Master of Informatics Engineering University of Indonesia Islam Yogyakarta," 2014.
- [4] B. Rahardjo, "Overview of Digital Forensics," *J. Sosioteknologi*, vol. Edisi 29, no. FSRD-ITB, pp. 384–387, 2013.
- [5] A. Amirullah, I. Riadi, and A. Luthfi, "Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System," vol. 143, no. 1, pp. 1–7, 2016.
- [6] T. Gloe, A. Fischer, and M. Kirchner, "Forensic analysis of video file formats," *Digit. Investig.*, vol. 11, no. SUPPL. 1, pp. S68–S76, 2014.
- [7] B. S. Putra and T. J. Pattiasina, "Study of Data Storage Analysis using Nas-Das-San," pp. 47–54, 2012.
- [8] I. Albanna, Faiz, Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," vol. 15, no. 1, pp. 173–178, 2017.
- [9] A. Setyawan and I. Riadi, "Multimedia Application of Memory Learning Using Adobe Flash," vol. 1, pp. 181–190, 2013.
- [10] A. M. Bagiwa, "Passive Video Forgery Detection Using Frame Correlation Statistical Features," 2017.
- [11] V. D'Amiano, L., Cozzolino, D., Poggi, G., "Video Forgery Detection And Localization Based On 3d Patchmatch L. D' Amiano, D. Cozzolino, G. Poggi and L. Verdoliva," *Multimed. Expo. Work. IEEE Int. Conf.*, pp. 1–6, 2015.
- [12] T. Van Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A Survey on Digital Camera Image Forensic Methods," *Multimed. Expo, 2007 IEEE Int. Conf.*, pp. 16–19, 2007.
- [13] J. HASUGIAN, "Electronic Document Storage Media (," pp. 1–6, 2003.
- [14] R. Dynata and I. Lubis, "Digital Forensic Analysis of Abstract Video," no. 70, pp. 1–8.
- [15] D. Y. Sari, Y. Prayudi, and B. Sugiantoro, "Detecting the Authenticity of Video on Handycam with Localization Tampering Method," *Online Inform.*, vol. 2, no. 1, pp. 10–15, 2017.
- [16] M. C. Stamm and K. J. R. Liu, "Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 492–506, 2010.
- [17] R. R. Huizen, N. K. D. A. Jayanti, and D. P. Hostiadi, "Model of Voice Recording Acquisition in Forensic Audio," *Semasteknomedia Online*, vol. 4, no. 1, pp. 2–8–1, 2016.
- [18] I. Riadi and N. B. Listyawan, "Optimalization of Video Storage Using Videocache in Proxy Servers (Case Study on Internet Cafe Net. Yogyakarta)," *Sarj. Tek. Inform.*, vol. 1, pp. 634–646, 2013.
- [19] Luthfi, S. E. Prastya, and I. Riadi, "Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence," vol. 15, no. April, pp. 280–285, 2017.
- [20] Y. D. Rahayu and Y. Prayudi, "Building Integrated Digital Forensics Investigation Frameworks (IDFIF) Using Sequential Logic Method," *Semin. Nas. SENTIKA*, vol. 2014, no. Sentika, 2014.
- [21] A. Sutardja, "Digital Image Manipulation Forensics," 2015.
- [22] W. Wang, "Digital Video Forensics," 2009.
- [23] S. Agarwal and S. Chand, "Digital Image Forensic : A Brief Review," vol. 5, no. 4, pp. 18–19, 2017.

Analysis Forensic Video in Storage Data Using Tampering Method

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

- 1 **Ronaldo Rigoni, Pedro Garcia Freitas, Mylene C.Q. Farias. "Tampering Detection of Audio-Visual Content Using Encrypted Watermarks", 2014 27th SIBGRAPI Conference on Graphics, Patterns and Images, 2014** 40 words — 1%
Crossref
- 2 **pdfs.semanticscholar.org** 29 words — 1%
Internet
- 3 **d-nb.info** 26 words — 1%
Internet
- 4 **L. D'Amiano, D. Cozzolino, G. Poggi, L. Verdoliva. "Video forgery detection and localization based on 3D patchmatch", 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2015** 19 words — < 1%
Crossref
- 5 **www.eurasip.org** 19 words — < 1%
Internet
- 6 **Prayudi, Yudi, Ahmad Ashari, and Tri K Priyambodo. "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia", International Journal of Computer Network and Information Security, 2015.** 15 words — < 1%
Crossref
- 7 **Zhang, Hong, Ding Yuan, Changtao Chen, and Mingui Sun. "Deblurring atmospheric turbulence degraded images using an isolate edges prior", 2013 6th** 14 words — < 1%

-
- 8 Kraaijenbrink, P.D.A., J.M. Shea, F. Pellicciotti, S.M. de Jong, and W.W. Immerzeel. "Object-based analysis of unmanned aerial vehicle imagery to map and characterise surface features on a debris-covered glacier", *Remote Sensing of Environment*, 2016. 12 words — < 1%
Crossref
-
- 9 Yee-Yang Teing, Ali Dehghantanha, Kim-Kwang Raymond Choo. "CloudMe forensics: A case of big data forensic investigation", *Concurrency and Computation: Practice and Experience*, 2018. 11 words — < 1%
Crossref
-
- 10 umexpert.um.edu.my 10 words — < 1%
Internet
-
- 11 www.researchgate.net 10 words — < 1%
Internet
-
- 12 Omar Ismael Al-Sanjary, Ahmed Abdullah Ahmed, Adam Amril Bin Jaharadak, Musab A. M Ali, Hwa Majeed Zangana. "Detection clone an object movement using an optical flow approach", *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2018. 10 words — < 1%
Crossref
-
- 13 Raahat Devender Singh, Naveen Aggarwal. "Video content authentication techniques: a comprehensive survey", *Multimedia Systems*, 2017. 7 words — < 1%
Crossref