



# Techniques for Video Authenticity Analysis Using the Localization Tampering Method to Support Forensic CCTV Investigations

Ririn Anggraini <sup>a,1,\*</sup>; Yudi Prayudi <sup>a,2</sup>

<sup>a</sup> Islamic University of Indonesia Yogyakarta, Jl. Kaliurang No.Km. 14.5, Krawitan, Umbulmartani, Ngemplak District, Sleman Regency, Indonesia

<sup>1</sup> 22917017@students.uii.ac.id; <sup>2</sup> prayudi@uii.ac.id

\* Corresponding author

**Article history:** Received September 09, 2024; Revised September 24, 2024; Accepted December 03, 2024; Available online December 29, 2024.

## Abstract

Closed Circuit Television (CCTV) is frequently utilized as legal evidence in judicial proceedings. However, the authenticity of CCTV footage is often contested, requiring forensic analysis to verify its reliability as digital evidence. This study aimed to assess the authenticity of video footage using the Localization Tampering method. To simulate manipulation, various manipulation techniques, such as zooming, cropping, converting to grayscale, deleting frames, and rotating video sections, were applied. The Localization Tampering method was then used to detect manipulated areas by analyzing individual frames, calculating their histograms, and interpreting the histogram graph result. The findings demonstrated the method's ability to accurately identify the location and duration of manipulated frames. This offered a valuable tool to support forensic investigations of CCTV footage. Furthermore, this study highlights the challenges in detecting manipulation in low-quality videos, which required more sophisticated remediation techniques. Despite these challenges, the Localization Tampering method demonstrated consistent reliability in preserving the integrity of video footage, making it a practical solution for verifying digital evidence in a legal context. Overall, this study provides an effective approach to ensure that manipulated videos can be identified and corrected, contributing to a more robust CCTV forensics process and maintaining the credibility as evidence in a crime case.

**Keywords:** CCTV; Digital Forensics; Evidence; Histogram; *Localization Tampering*.

## Introduction

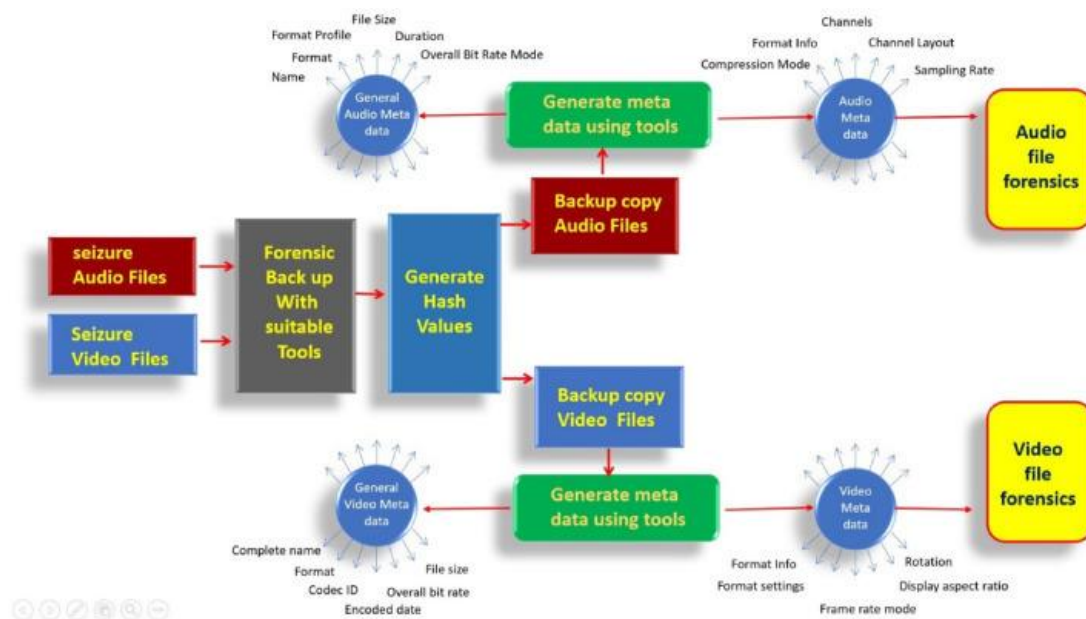
CCTV (Closed Circuit Television) is a surveillance tool commonly used to monitor properties such as homes, offices, warehouses, and even on highway premises. In addition, CCTV also serves as an alternative to reduce theft cases because criminals tend to think twice when they know that there is a CCTV that can record their face [1]. CCTV has developed into a crucial technology in modern surveillance systems [2]. CCTV footage can be used as evidence or reference for a variety of interests, including security, investigation, or evaluation.

The role of CCTV cameras is needed as a security system in daily life. The use of CCTV cameras, which is currently high in demand, is considered very efficient as a security mechanism because of its ability to anticipate misconducts [2]. The CCTV camera can recognize all the detected objects and usually records data continuously based on time as part of its security monitoring function [3]. Video footage is usually considered as more powerful and accurate pieces of evidence compared to photographs [4].

Video recording can be used as evidence in the context of forensic digital analysis. Digital forensics includes the ability to find digital evidence stored in a variety of media, such as computer storage, USB devices, CDs, network traffic, etc [5], [6]. The purpose of digital forensics is to obtain relevant digital records and can be used as a legal evidence [7], [8]. Video footage from CCTV can be important digital evidence in uncovering a case in the court, as it provides a clear visual picture of an incident, which can support the investigation process and strengthen legal arguments [9]. However, when a video is used as evidence in the court, then initial authentication steps must be taken. The video authentication process is essential to ensure that the footage is not subject to manipulation or falsification that could harm the integrity of the information [10]. One of the video authentication processes carried out is to analyze and detect the footage to obtain authenticity information [11].

Forensic video is a sub-field of digital forensics. In addition to video forensics and computer forensics, there are several other sub-fields of digital forensics such as mobile forensics, cyber forensics, audio forensics, image forensics, malware forensics, and memory forensics. Forensic videos play an important role in understanding the crime situation and supporting the investigation [12]. Analysis of video footage can help identify the perpetrator, clarify the chronology of the incident, and provide visual evidence that can be used in legal proceedings. Therefore, the integrity of the authenticity in the video needs to be considered for authenticity when used as evidence in court [13].

Video is digital data that consists of a series of images. The term video usually refers to a movable moving image storage format. There are two types of video, namely analog video such as VHS and Betamax, as well as digital video such as DVD, QuickTime, and MPEG-4. Videos can be recorded and transmitted through a variety of physical media [14]. Audio-video forensics involves three main principles in forensic science, namely the collection, processing, and interpretation of audio and video recordings [15]. The fundamental process of a video forensic system is to prove whether the given video has been manipulated or not [16].



**Figure 1.** Flowchart of the Analysis Flow of the Forensic Video and Audio Analysis Process

(Source: Srinivasa Murthy Pedapudi, 2023)

Video manipulation techniques are currently improving at an unprecedented speed, the advent of a wide variety of video editing software makes it difficult to distinguish between a manipulated video and an original video [17]. All multimedia-related content is very easy to change using some digital editing software [18]. The development of image and video processing software such as Photoshop, Adobe Premiere, Final Cut Pro, and VN make it easy to manipulate digital visual media without leaving a clear trace [19]. The device provides great support for editing videos easily, and anyone can edit the video as they wish [20]. Anyone can easily use video editing software to change frames, rearrange the sequence of events, or even add fake elements to the video. The purpose of this manipulation varies, including to eliminate evidence of crime, spread false information, or create a narrative in favor of certain parties. Criminals often exploit these vulnerabilities, making the investigation process increasingly difficult to distinguish between original and manipulated videos. Many perpetrators of crimes often cannot be criminalized because the video footage used as crime evidence cannot be used because it has been manipulated [21]. Videos that have been manipulated can make it difficult for the police to solve the problem and are also difficult to use in court decisions [22]. Therefore, it is important to carry out an originality check on the video when used as evidence in a court case [23]. Video manipulation detection aims to ensure authenticity as well as identify potential modifications or counterfeits, in order to verify whether the video is authentic or not [24]. Decisions regarding the authenticity of a video are usually made with the help of certain techniques, which are collectively referred to as counterfeit detection techniques [25].

One type of video manipulation known as tampering, it involves adding specific objects to the video recording. These added objects can be a series of frames from the same or different video, snippets of other frames from the same or different videos, or even images inserted into multiple frames at once [26]. Therefore, multimedia forensics has a role to address this need by providing algorithms and systems that assist investigators to find traces of manipulation

and extract information on multimedia items [27]. To verify the authenticity of a video, there are two main methods that are often used, namely tampering detection and tampering localization. Tampering detection is a method of identifying any manipulation in a video without indicating the specific area that has been manipulated. In contrast, Tampering localization is a method to indicate specific areas in the video that have been manipulated [28].

Research on detecting video tampering has been conducted by some researchers, such as [29] by analyzing the authenticity of video through analyzing frames, histogram calculations, and histogram graphs, from manipulated handycam videos. The research was also conducted by [30] who tested video data using the Generic Computer Forensic Investigation Model (GCFIM) framework to be able to provide structured and valid information to be accepted in the trial as digital evidence. The test results showed significant differences between the original video and the manipulated video, such as differences in file size, video duration, and date. In addition, several other studies have also tried to deal with the problem of video manipulation by developing methods to detect and analyze changes that occur in digital videos. One technique that is often used is metadata analysis, which identifies changes in file size, duration, frame rate, and other technical aspects to detect any manipulation [8]. Another popular method is histogram analysis and frame-by-frame comparison, which takes advantage in color distribution or pixel brightness of differences to identify changes in frames that have been manipulated [15].

Although there have been many studies that offer different approaches to detect video manipulation, there are still challenges in detecting manipulation in low-quality videos or in cases of manipulation involving minor changes that are very difficult to detect. The existing research gap lies in the need for more effective and accurate methods to detect manipulations of various complexity, including in low-resolution video conditions [15]. Therefore, the development of more reliable methods in Localization Tampering becomes more importance.

This study proposed a better Localization Tampering method to detect manipulation in digital video, especially in the context of CCTV footage used as legal evidence. By analyzing the video spatially and temporally, this method was expected to be able to provide more accurate detection of various forms of zooming, cropping, grayscale, deletion, and rotation manipulation. This solution is crucial because it ensures that the video footage used in court reflects authenticity and does not contain alterations that could unfairly influence legal decisions. The success of the Localization Tampering method in detecting manipulation will make a significant contribution to the field of digital forensics and strengthen the justice system by ensuring that video evidence presented in court is credible and valid.

## Method

To improve the structure and effectiveness of the forensic investigation process, a method to assist the investigation is needed. The Localization Tampering method is an approach used to indicate the location of manipulation in a video. The process of this method performs an attack on the original video and the result is compared to the video copy by extracting it into several frames.

By comparing each frame in order, this method can identify the frames that are experiencing differences. In addition, through histogram calculations and histogram graph analysis, the location and duration of tampering can be determined. The values contained in this component are used to create a rule that will then produce an output in the form of video authenticity detection. Thus, this method provides clear information about the location and duration of the manipulation of the video, and the results can be used as a basis for detecting the authenticity of the video.

There were several stages carried out in this study, namely literature study, needs identification, video simulation, analysis, and report. The flow of the methodology can be seen in Figure 2.

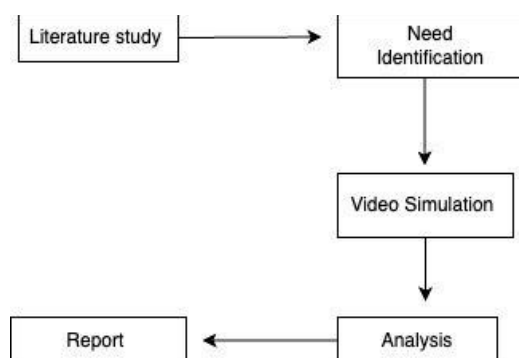


Figure 2. Research Methodology.

### A. Literature Studies

At the stage of literature study, an in-depth study of various relevant works to the research topic was carried out. The first step in this process was to collect literature from academic sources, such as scientific journals, books, and related publications. The search was focused on the main theories, basic concepts, methodologies applied, and findings from previous research. This approach was to build a strong theoretical foundation and provide a comprehensive context for the topic under study. This was to support the analysis and development in this research.

### B. Need Identification

This stage of need identification was to set specific goals in analyzing the authenticity of video footage in CCTV forensics. This process involved collecting original videos and manipulated videos to find the location of the changes. Identification of these needs helped determine the focus of the analysis and the method to be used, so that the analysis process became more structured and the results obtained are more significant and relevant to determine the integrity of the video.

### C. Video Simulation

The video simulation stage involved preparing the video for tampering analysis. The original footage of the CCTV video was selected and produced a copy of it, so we had the original video and the video copy for the simulation. In the video copy, various manipulations were performed in different frames [31]. In general, there were two types of video counterfeiting; (1) Falsification through content splicing, where details or frames from different video sources were added; (2) Copy-move counterfeiting, which is another type of counterfeiting, in which the frames and content of the same video were replicated. This created a convincing false impression [32], [33]. In this case, the application of attacks on the original video involved manipulation in certain frames using video editing software such as VN editor. This attack was carried out to create realistic video tampering conditions. The application of attacks such as zooming, cropping, grayscale, deletion, and rotation was applied against the original video.

### D. Analysis

At this stage, the Localization Tampering used to detect parts of the video that have been manipulated, such as zooming, cropping, grayscale, deletion, and rotation of original videos carried out by certain parties with specific purposes. Localization Tampering is a method that is able to detect specific areas in a video that have undergone changes. This detection is done by utilizing pixel coordinates to determine spatial locations, as well as frame sequences to detect temporal changes. The main focus of this method is to identify the frames that have been modified.

In video signals, manipulation techniques can be grouped into two types, spatial and temporal manipulation. Spatial manipulation occurs when changes are made at the pixel level in a single frame. Spatial manipulation is further divided into local and global manipulation. Local manipulation involves making changes to a specific group of pixels, such as changing the color of an area, removing a pixel block, or adding new pixels. Meanwhile, global manipulation involves modifying the entire frame in a video, such as adjusting brightness, changing the format, or zooming. Temporal manipulation occurs when there is a change in the frame order, such as additional of new frames or a change in speed (frame rate) by deleting or duplicating a specific frame [34].

The analysis process consisted of several stages. The first stage was metadata analysis to detect any discrepancies between the original and manipulated videos. After that, the video was broken down into several frames, then each frame was compared one by one. An analysis of the RGB value was performed to determine the distance between the center points of the pixel cluster. In addition, the histogram was calculated to see the color distribution or brightness level of the pixels. In the final stage, the localization tampering applied to identify specific areas in the video that were manipulated.

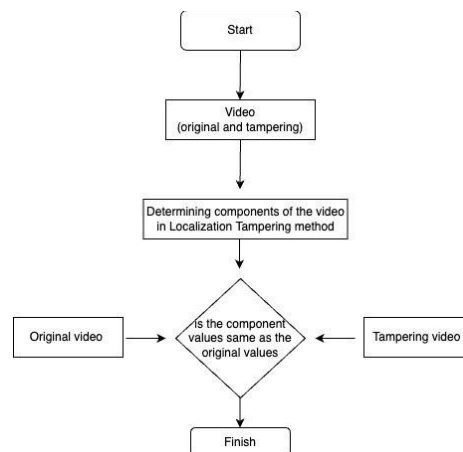


Figure 3. Flowchart of Analysis Flow

In **Figure 3**, the analysis process begins by duplicating the CCTV footage into two versions: the original video and the manipulated video. Manipulation was then applied to the video copy. Localization Tampering method was used to analyze the frames and histograms of the two videos. The frames were compared, while the histogram was used to examine the distribution of color intensity. Significant differences in the distribution indicated manipulation (Tampering), while the similarity of values indicated the authenticity of the video. The results of this analysis revealed the location of the manipulation in the video.

## Results and Discussion

### A. Identification of Research Objects

At the identification stage, two video files were collected as evidence. The first file, named "172128062655263(1)" or the original video. The second file was "VN20240718\_130528" or tampering video that has been manipulated.

The original video file was in MPEG-4 format with isom code (isom/iso2/mp41), 1.09 MiB in size, 13 s 403 ms duration, 680 kb/s bit rate, and 20,072 fps frame rate. Tampering video was in MPEG-4 format with isom code (isom/mp42), 3.37 MiB in size, 13 s 417 ms duration, 2 110 kb/s bit rate, and 24,000 fps frame rate. These two files were collected for analysis to determine the tampering location on the video.

### B. Video Simulation

To obtain digital evidence, a simulation scenario was created using Robit CCTV. The video footage from the CCTV was transferred to a laptop and duplicated into two copies, the original video and the video copy. The video copy was named "VN20240718\_130528" and then manipulated into a video that was tampered through various techniques, such as zooming, cropping, grayscale, deletion, and rotation using VN software. Cropping techniques were used to remove parts of the image in a specific area, zooming was to zoom in on parts of the image and change the visual perception of the recorded event, grayscale was to change the original color to black-and-white to hide color information, and deletion to remove certain parts of the frame to hide specific events. The rotation technique was used to rotate the image 180 degrees, changing the visual orientation in the video. Each of these techniques was applied to different frames to create a video that has been manipulated, which was then further analyzed to identify the tampering technique and its impact on the integrity of the video.

### C. Analysis

At this stage, the Localization Tampering method was used to analyze the video, the goal was to detect parts that have been changed, added, or deleted. This method focused on identifying frames that have been manipulated. The analysis steps with Localization Tampering are outlined as follows:

#### 1) Metadata Analysis

At this stage, metadata analysis was used to verify the format, duration, size, and frame of the video. The difference in metadata between the original video and the manipulated video indicated manipulation. In this study, Mediainfo tools were used to identify the metadata of the two videos.

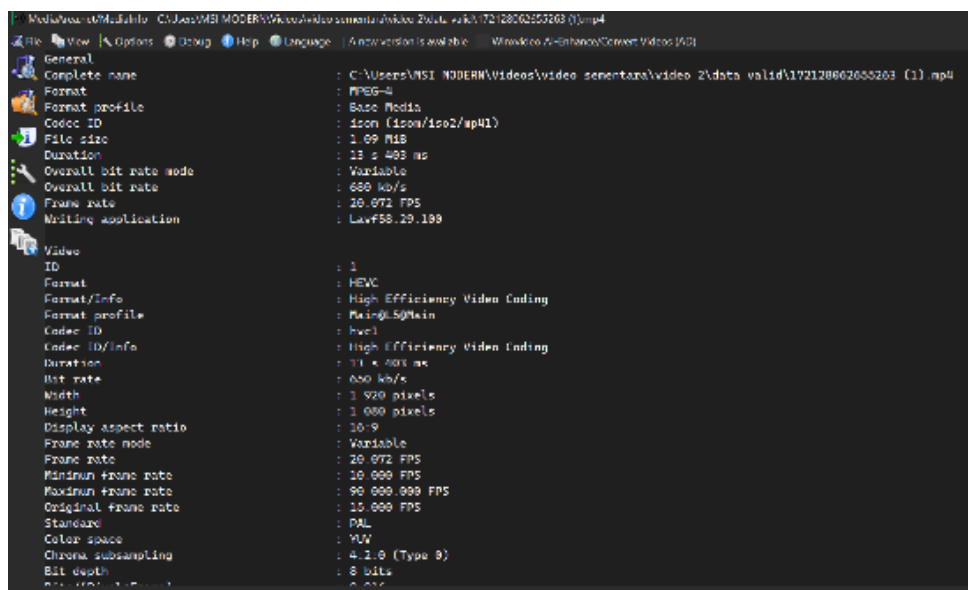
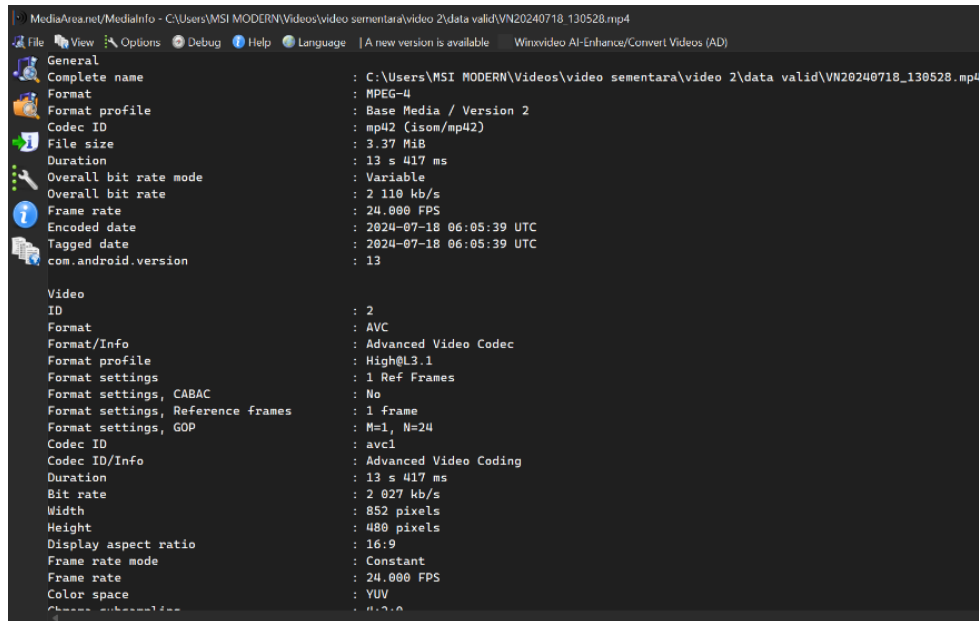


Figure 4. Original video digital proof metadata.



**Figure 5.** Metadata digital proof of tampering video

In [Figure 4](#) and [Figure 5](#), it can be seen that the metadata of the original video file and the tampering video showed a difference in values. This was an indication of tampering in one of the files. After metadata analysis was carried out, then frame by frame analysis was carried out by extracting the video into a JPG image file using the tools on the Esgif website. The extraction results were obtained with the number of frames each being 135 frames.

After the original video and the tampering video were extracted into JPG images, then visual analysis was carried out to compare the images from the two files. The comparison showed changes in the size, color, and objects in the frame. The detected images underwent changes and were then further analyzed. In addition, the RGB value of each frame was analyzed using the JPEGsnoop tool to display the RGB value of the image from the average brightness pixels in a single frame. [Table 1](#) shows the results obtained from the evaluation of the RGB Frame value between the Original Video and the Video that has been tampered.

**Table 1.** RGB Frame Values

No.	Frame	Original Video			Video Tampering		
		R	G	B	R	G	B
1.	Frame 00016	255	249	249	255	253	253
2.	Frame 00017	255	249	249	255	253	253
3.	Frame 00018	255	249	249	255	253	253
4.	Frame 00019	255	249	249	255	253	253
5.	Frame 00020	255	249	249	255	253	253
6.	Frame 00021	255	249	249	255	253	253
7.	Frame 00048	255	249	255	255	254	251
8.	Frame 00049	255	249	255	255	254	251
9.	Frame 00050	255	249	255	255	254	251
10.	Frame 00051	255	249	255	255	253	251
11.	Frame 00052	255	249	255	255	253	251
12.	Frame 00053	255	249	255	255	253	251
13.	Frame 00075	255	248	251	255	252	255
14.	Frame 00076	255	248	251	255	252	255
14.	Frame 00078	255	248	251	255	252	255
16.	Frame 00079	255	248	251	255	252	255
17.	Frame 00080	255	248	251	255	252	255
18.	Frame 00114	255	249	255	236	233	236

No.	Frame	Original Video			Video Tampering		
		R	G	B	R	G	B
19.	Frame 00115	255	249	255	236	233	236
20.	Frame 00116	255	249	255	234	234	234
21.	Frame 00117	255	242	240	234	234	234
22.	Frame 00118	255	249	255	234	234	234
23.	Frame 00119	255	249	255	234	234	234
24.	Frame 00120	255	242	221	255	254	255
25.	Frame 00121	255	243	224	255	254	255
26.	Frame 00122	255	244	223	255	254	255
27.	Frame 00123	255	249	255	255	254	255
28.	Frame 00124	255	249	255	255	255	255
29.	Frame 00125	255	249	255	255	255	255

After obtaining the RGB value of each frame, then an analysis was carried out using the K-means algorithm to group the RGB data. The analysis was carried out in stages frame by frame to determine the middle value (centroid).

To determine the centroid of each frame, the RGB value was divided by half and then the center value of each pixel was calculated. Furthermore, calculating the distance of cluster members was conducted by subtracting the pixel value of the data on the R color attribute by the value of the initial centroid of the cluster on the R color attribute, then the result was magnified by 2. This was also done for the G and B color attributes.

$$F116A = \sqrt{(255 - 127.5)^2 + (249 - 124.5)^2 + (255 - 127.5)^2} = 219.2$$











$$F117A = \sqrt{(255 - 127.5)^2 + (242 - 121)^2 + (240 - 127.5)^2} = 208.6$$

$$F116T = \sqrt{(234 - 117)^2 + (234 - 117)^2 + (234 - 117)^2} = 202.6$$

$$F117T = \sqrt{(234 - 117)^2 + (234 - 117)^2 + (234 - 117)^2} = 202.6$$

From the results obtained, it can be seen that there was a significant difference between the pixel value in the original video and the tampering video. In frames 16 and 17 of the original video the RGB pixel values produced were different, while the RGB pixel values in frames 16 and 17 of the tampering video had the same value, so it can be said that in the frames with the same value there was manipulation in the grayscale.

**Table 2.** Frame detection on video

Manipulation	Analysis		Conclusion
	Original Video	Video Tampering	
Cropping	 Frame 00016	 Frame 00016	Tampering occurred due to different frame sizes
Zooming	 Frame00048	 Frame00048	Zooming occurred in the frame due to video tampering
Deletion	 Frame00075	 Frame00075	There was a reduction in frames due to a missing part of the frame
Greyscale	 Frame00116	 Frame00116	Greyscale occurred in the frame, as seen from the color in the changing frame
Rotation	 Frame00120	 Frame00120	Rotation occurred in the frame due to a 180-degree rotation

## 2) Histogram Analysis

This stage of analysis was carried out by calculating a value matrix to compare the histogram between the original video and the manipulated video based on the pixel value of each frame. This analysis was also used to make a graphical comparison between the two videos. The histogram values of the image were obtained by the following formula:

$$h_i = \frac{n_i}{n} \quad i = 0, 1, 2, \dots, L - 1 \tag{1}$$

In fact, to obtain the image histogram from the original video and the manipulated video, the first step was to calculate the occurrence frequency of each gray level,  $n_i$ , where  $i$  was the value of the gray level. This calculation was carried out using the help of MATLAB tools. The result of the histogram matrix calculation of the original video frame was compared to the manipulated video frame. This was done to detect differences that can indicate manipulation. This analysis was important to ensure the authenticity and integrity of the video, especially in digital forensics and data security.

From the data presented in **Table 3** and **Table 4**, it can be seen that the larger  $n_i$  value, the greater the  $h_i$  value. The histogram calculation shows the difference between the original video frame and the manipulated video frame. It turned out that the manipulation activities changed the distribution of histogram values and created a different pattern than the original video. In this case, histogram analysis helped identify frames that were subject to manipulation.

**Table 3.** Histogram values on the original video

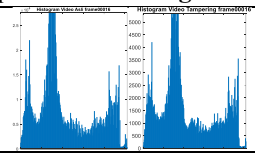
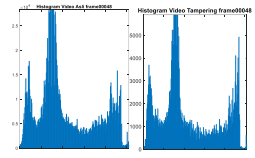
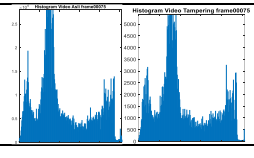
$i$	$H_i$	$i$	$H_i$
0	0.000099	6	0.001845
1	0.000611	7	0.003105
2	0.001113	8	0.003260
3	0.001187	9	0.003506
4	0.001371	10	0.003707
5	0.001378	11	0.002979

**Table 4.** Histogram values on tampering videos

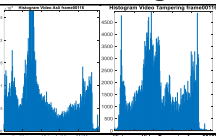
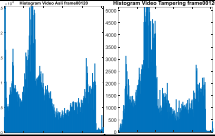
$i$	$H_i$	$i$	$H_i$
0	0.000042	6	0.002489
1	0.000281	7	0.003281
2	0.000604	8	0.003484
3	0.000844	9	0.004260
4	0.001849	10	0.005338
5	0.001555	11	0.004252

The display of the comparison histogram graph image on the digital evidence frame from the results of the original video frame and the tampering video frame can be seen in **Table 5**.

**Table 5.** Frame comparison histogram chart

Frame	Comparison of Histogram Charts	Duration	Information
Frame 00016		0.797	With the same frame tampering can be identified with the image size change or crooping manipulation
Frame 00048		2.39	With the same frame, tampering can be identified with a change in the image looked closer or zooming manipulation
Frame 00075		3.74	With the same frame, Tampering can be identified with the presence of missing frames or deletions



Frame	Comparison of Histogram Charts	Duration	Information
Frame 00116		5.78	With the same frame, a color change was identified or grayscale
Frame 00120		5.98	With the same frame rotation can be detected

Based on the data in [Table 5](#), it was found that from frames 1 to 135 (the 1st to 5th seconds), manipulations such as cropping, zooming, deletion, grayscale, and rotation were detected. This manipulation aimed to hide an authentic event or evidence. The detection showed cropping manipulation in frames 16-21, zooming in frames 48-53, deletion in frames 75-80, grayscale in frames 114-119, and rotation in frames 120-125. Overall the video was tampered in the first 5 seconds.

Overall, the detection of manipulation on CCTV footage in this study was carried out using the Localization Tampering method. This method aimed to identify specific parts of the video that have undergone changes, both spatially and temporally. This technique was very effective in detecting various forms of tampering, such as cropping, zooming, grayscale, deletion, and rotation, by performing frame-by-frame analysis and comparing changes in pixel intensity between frames. Localization Tampering relies on frame-to-frame comparisons to detect changes that occur in spatial dimensions. This technique compares the distribution of colors and pixels between frames, where significant differences indicate manipulation.

In the simulations carried out, this technique was able to detect cropping manipulation, where a part of the image has been removed from the frame. In the cropping case, the manipulated frame showed a noticeable difference in color histogram and pixel intensity compared to the original frame. The frame affected by cropping had a histogram value indicating the loss of a specific area in the pixel intensity distribution, so this technique can instantly identify the manipulated area. In addition, this method also successfully detected changes in frames caused by grayscale manipulation, where the loss of color detail significantly affects the distribution of RGB values between frames.

In addition to detecting spatial changes, Localization Tampering method also analyzed temporal aspects of the video, including the time sequence between frames. Temporal manipulation, such as frame deletion, can be detected by analyzing the frame sequence. In this study, this method successfully detected temporal gaps in video recordings, where frame deletion caused discrepancies in the recording time sequence. This technique allowed the detection of frame deletion by comparing the timestamps between frames and checking for any discrepancies in their sequence. Frame deletion detected in the simulation indicated the existence of time manipulation aimed at hiding important parts of the footage. Metadata analysis also reinforced these findings by showing differences in the video length, which should have been consistent with the original video.

One of the advantages of the Localization Tampering technique was its integration with the K-Means algorithm, which was used to group pixels based on similar color intensities. This algorithm helped to clarify the detection of small changes in the frame, especially in manipulations such as zooming or rotation, which changed the structure of the image without losing much detail. In this study, the K-Means algorithm was used to identify groups of pixels that underwent significant changes in the frames that had been manipulated. For example, in a zoomed frame, there was a change in the distribution of pixels that caused some groups of pixels to change significantly compared to the original frame. The K-Means algorithm allowed the detection of this manipulation by differentiating between groups of pixels that remained stable and those with drastic changes.

The object of this research was two CCTV video recordings with 13 seconds 403 milliseconds and 13 seconds 417 milliseconds, respectively, consisting of 135 frames. The results of the analysis showed that at frames 16 to 125 there was a significant difference in values based on the K-Means algorithm and histogram graphs, which indicated a manipulation in the video. In this study, several tools were used, including Ezgif for separating frames, MediaInfo for metadata analysis, JPEGsnoop for calculating RGB pixel values, and MATLAB for displaying histogram graphs. The use of the Localization Tampering method supported by these tools has proven to be effective in detecting and analyzing tampering in CCTV videos.

However, this study also identified several challenges in the application of the Localization Tampering method on CCTV video footage with varying qualities. Key challenges included poor video quality or low resolution, which can complicate the process of detecting manipulation. The complexity of the manipulation techniques used, such as the combination of multiple tampering methods, can also complicate the analysis process. In addition, the limitations of the analysis tool as well as the difference in frame rate and bit rate between the original video and the manipulated video can affect the results of the analysis.

#### **D. Discussion**

The study also faced limitations when performing video extraction, where a difference in RGB value was detected in the first frame, even though the frame has not been manipulated. To address these shortcomings, more in-depth analysis is needed in the future so that tampering site detection can be carried out more accurately and reliably. Further development of the methods and tools used will help improve the accuracy of manipulation detection, especially on low-resolution or poor-quality videos.

In this study, there were several limitations that need to be considered to understand the limitations of the analysis results. One of the main limitations was the varying quality of CCTV video footage, especially low-resolution or poor-quality videos. This can complicate the process of detecting manipulation because small changes in the distribution of pixels often cannot be detected with the expected accuracy. In addition, the complexity of the manipulation techniques used, such as a combination of zooming, cropping, grayscale, deletion, and rotation, also presents its own challenges in the analysis, especially when several of these techniques are applied simultaneously.

Another limitation in this study was the difference in frame rate and bit rate between the original video and the manipulated video. The rates can affect the results of manipulation analysis and detection. The use of tools in analysis, such as Ezgif, MediaInfo, JPEGsnoop, and MATLAB, also has limitations in accuracy, especially in low-quality videos. In addition, at the video extraction stage, a difference in RGB values was detected in the first frame, although no manipulation has been performed on that frame, indicating a potential bias in the analysis results.

To overcome these limitations, further development of the Localization Tampering method and the use of more advanced analysis tools were needed. Future research is expected to optimize detection techniques to handle videos of varying quality, as well as improve accuracy in detecting minor manipulations.

This study showed that the Localization Tampering method was effective in detecting manipulation in CCTV videos, especially in identifying spatial and temporal changes. The results of this study were in line with other studies that also use similar methods to detect video manipulation. For example, a study by [29] using the Localization Tampering method to detect manipulation in handycam videos found that this method was effective in detecting pixel changes between frames, both in color and brightness intensity.

However, there were differences in accuracy level in detecting manipulation in low-quality videos. Several previous studies, such as the one conducted by [30], indicating that the Generic Computer Forensics Investigation Model (*GCFIM*) method was more effective in dealing with low-resolution videos and more complex levels of manipulation. This method offered a more comprehensive structure in metadata and visual analysis. It allowed for more in-depth detection of manipulation, especially in the case of minor tampering.

Compared to other studies that used metadata analysis or machine learning algorithms, the method in this study has proven to be superior in detecting more visible manipulations such as cropping and zooming. However, in detecting minor changes some other studies with more advanced approaches such as deep learning proposed by [20] can show more accurate results in detecting very subtle temporal changes.

Although this study has successfully demonstrated the effectiveness of the Localization Tampering method in detecting various forms of video manipulation, a room for further development in dealing with more complex manipulations and on lower-quality videos, as highlighted by previous studies, is

#### **Conclusion**

Based on the results of the analysis conducted by the researcher on the technique of analyzing the authenticity of video recordings to support forensic CCTV investigations, it can be concluded that using the Localization Tampering method has been successfully applied to detect manipulation in CCTV video recordings. Through frame-by-frame analysis, histogram calculations, and histogram graphs, these were able to identify the parts of the video that have been manipulated. The results of the analysis showed a significant difference between the original video and the manipulated video, indicating the success of this method in detecting tampering.

This study also has confirmed the effectiveness and accuracy of the Localization Tampering method in detecting video recording manipulation. Various types of attacks such as cropping, zooming, deletion, grayscale, and rotation were detected at certain frames, which strengthens the ability of this method to identify parts of the video that have been manipulated.

However, the study also identified some challenges and limitations, especially related to the detection of manipulation in low-quality videos, where small differences in the distribution of pixels may not be accurately detected. In addition, the detection of complex manipulations, such as a combination of zooming and rotation, required the development of more sophisticated methods. Overall, the Localization Tampering method used in this study proved to be a reliable solution for detecting video manipulation in the context of digital forensics, specifically to ensure the integrity of CCTV footage used as legal evidence. Further development on aspects of computing efficiency and improved accuracy for low-resolution video scenarios or more complex manipulations is highly recommended.

### Acknowledgement

This research and publication were funded through the PTM Grant provided by the Ministry of Education, Culture, Research, and Technology (Kemdikbudristek) for the year 2024, under contract number 0609.1/LL5-int/AL.04/2024.

### References

- [1] M. Arsyad, E. I. Fitria, M. R. Farhan, and R. Maulana, "Decision Making System for Selecting the Best CCTV Brand Using the Simple Additive Weighting (SAW) Method," *FUSION Journal*, vol. 3, no. 02, 2023, doi: [10.54543/fusion.v3i02.255](https://doi.org/10.54543/fusion.v3i02.255).
- [2] P. Sukanto, Ispandi, A. S. Putra, N. Aisyah, and R. Toufiq, "Forensic Digital Analysis For CCTV Video Recording," *International Journal Of Science*, vol. 3, 2022.
- [3] S. Bahri and H. Kusindaryadi, "Design and Build Student Attendance Monitoring Using Facial Fingerprints Simultaneously Through Classroom CCTV," *RESISTOR (Computer Electrical Power Telecommunication Control Electronics)*, vol. 3, no. 1, 2020.
- [4] W. Wang, X. Jiang, S. Wang, M. Wan, and T. Sun, "Identifying Video Forgery Process Using Optical Flow," In *Lecture Notes in Computer Science (Including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2014, pp. 244–257. doi: [10.1007/978-3-662-43886-2\\_18](https://doi.org/10.1007/978-3-662-43886-2_18).
- [5] I. Riadi, A. Yudhana, and M. C. F. Putra, "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method," *JUTISI (Journal of Informatics and Information Systems Engineering)*, vol. 4, 2018, Accessed: Sep. 24, 2024, doi: [10.28932/jutisi.v4i2.769](https://doi.org/10.28932/jutisi.v4i2.769)
- [6] Herman, A. Yudhana, and F. Anggraini, "Acquisition of Android-Based Tiktok Digital Evidence Using the National Institute of Justice Method," *Journal of Information Technology and Computer Science (JTIK)*, vol. 10, pp. 89–96, 2019, doi: [10.25126/jtiik.2023106416](https://doi.org/10.25126/jtiik.2023106416).
- [7] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, 2017.
- [8] F. Albanna and I. Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, 2017.
- [9] G. H. A. Kusuma and I. N. Prawiranegara, "Digital Forensic Analysis of CCTV Video Footage Using Metadata and Hash," *SISFOTEK (Information Systems and Technology)*, vol. 3, 2019.
- [10] D. Mualfah and R. A. Ramadhan, "Digital Forensic Analysis of CCTV Camera Footage Using the NIST (National Institute of Standards Technology) Method," *IT Journal Research and Development*, vol. 5, no. 2, pp. 171–182, Nov. 2020, doi: [10.25299/itjrd.2021.vol5\(2\).5731](https://doi.org/10.25299/itjrd.2021.vol5(2).5731).
- [11] M. A. S. Nasr, M. F. AlRahmawy, and A. S. Tolba, "Multi-scale structural similarity index for motion detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 3, pp. 399–409, Jul. 2017, doi: [10.1016/j.jksuci.2016.02.004](https://doi.org/10.1016/j.jksuci.2016.02.004).
- [12] P. M. Kulkarni, B. Nautiyal, S. Kumar, R. Medidha, R. R. Savaliya, and M. Eknath, "IOT data Fusion framework for e-commerce," *Measurement: Sensors*, vol. 24, Dec. 2022, doi: [10.1016/j.measen.2022.100507](https://doi.org/10.1016/j.measen.2022.100507).
- [13] D. N. Zhao, R. K. Wang, and Z. M. Lu, "Inter-frame passive-blind forgery detection for video shot based on similarity analysis," *Multimed Tools Appl*, vol. 77, no. 19, pp. 25389–25408, Oct. 2018, doi: [10.1007/s11042-018-5791-1](https://doi.org/10.1007/s11042-018-5791-1).
- [14] T. Van Lanh, K. S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A Survey On Digital Camera Image Forensic Methods," *IEEE International Conference on Multimedia and Expo*, pp. 16–19, 2007.
- [15] S. M. Pedapudi and N. Vadlamani, "Digital Forensics Approach For Handling Audio And Video Files," *Measurement: Sensors*, vol. 29, Oct. 2023, doi: [10.1016/j.measen.2023.100860](https://doi.org/10.1016/j.measen.2023.100860).
- [16] V. Joshi and S. Jain, "Tampering Detection And Localization In Digital Video Using Temporal Difference Between Adjacent Frames Of Actual And Reconstructed Video Clip," *International Journal of Information Technology (Singapore)*, vol. 12, no. 1, pp. 273–282, Mar. 2020, doi: [10.1007/s41870-018-0268-z](https://doi.org/10.1007/s41870-018-0268-z).

- 
- [17] P. Johnston, E. Elyan, and C. Jayne, "Video Tampering Localisation Using Features Learned From Authentic Content," *Neural Comput Appl*, vol. 32, no. 16, pp. 12243–12257, Aug. 2020, doi: [10.1007/s00521-019-04272-z](https://doi.org/10.1007/s00521-019-04272-z).
- [18] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal Forensics And Anti-Forensics For Motion Compensated Video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, 2012, doi: [10.1109/TIFS.2012.2205568](https://doi.org/10.1109/TIFS.2012.2205568).
- [19] S. Jia, Z. Xu, H. Wang, C. Feng, and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," *IEEE Access*, vol. 6, pp. 25323–25335, Mar. 2018, doi: [10.1109/ACCESS.2018.2819624](https://doi.org/10.1109/ACCESS.2018.2819624).
- [20] X. H. Nguyen, Y. Hu, M. A. Amin, K. G. Hayat, V. T. Le, and D. T. Truong, "Detecting Video Inter-Frame Forgeries Based on Convolutional Neural Network Model," *International Journal of Image, Graphics and Signal Processing*, vol. 12, no. 3, pp. 1–12, Jun. 2020, doi: [10.5815/ijigsp.2020.03.01](https://doi.org/10.5815/ijigsp.2020.03.01).
- [21] R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive Copy- Move Forgery Detection in Videos," *International Conference on Computer and Communication Technology (ICCT)*, 2014.
- [22] N. Akhtar, M. Hussain, and Z. Habib, "DEEP-STA: Deep Learning-Based Detection and Localization of Various Types of Inter-Frame Video Tampering Using Spatiotemporal Analysis," *Mathematics*, vol. 12, no. 12, Jun. 2024, doi: [10.3390/math12121778](https://doi.org/10.3390/math12121778).
- [23] L. Yu et al., "Exposing Frame Deletion By Detecting Abrupt Changes In Video Streams," *Neurocomputing*, vol. 205, pp. 84–91, Sep. 2016, doi: [10.1016/j.neucom.2016.03.051](https://doi.org/10.1016/j.neucom.2016.03.051).
- [24] N. Akhtar, M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Digital Video Tampering Detection and Localization: Review, Representations, Challenges and Algorithm," Jan. 01, 2022, MDPI. doi: [10.3390/math10020168](https://doi.org/10.3390/math10020168).
- [25] S. Kingra, N. Aggarwal, and R. D. Singh, "Inter-Frame Forgery Detection In H.264 Videos Using Motion And Brightness Gradients," *Multimed Tools Appl*, vol. 76, no. 24, pp. 25767–25786, Dec. 2017, doi: [10.1007/s11042-017-4762-2](https://doi.org/10.1007/s11042-017-4762-2).
- [26] A. P. Justicia and I. Riadi, "Analysis of Forensic Video in Storage Data Using Tampering Method," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, pp. 328–335, 2018, doi: [10.17781/P002471](https://doi.org/10.17781/P002471).
- [27] M. Zampoglou et al., "Detecting Tampered Videos with Multimedia Forensics and Deep Learning," *In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2019, pp. 374–386. doi: [10.1007/978-3-030-05710-7\\_31](https://doi.org/10.1007/978-3-030-05710-7_31).
- [28] P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Local Tampering Detection In Video Sequences," *International workshop on multimedia signal processing (MMSp)*, IEEE, 2013.
- [29] D. Yunita Sari, Y. Prayudi, and B. Sugiantoro, "Detection of Video Authenticity on Handycam Using the Localization Tampering Method," *JOIN*, vol. 2, no. 1, 2017.
- [30] I. Riadi, A. Yudhana, and R. V. A. Saputra, "Video Forensics on CCTV Using the Generic Computer Forensics Investigation Model (GCFIM) Framework," *JURIKOM (Journal of Computer Research)*, vol. 10, no. 2, p. 540, Apr. 2023, doi: [10.30865/jurikom.v10i2.5888](https://doi.org/10.30865/jurikom.v10i2.5888).
- [31] C. Long, A. Basharat, and A. Hoogs, "A Coarse-to-fine Deep Convolutional Neural Network Framework for Frame Duplication Detection and Localization in Forged Videos," *CVPR Workshop*, 2019.
- [32] J. Patel and R. Sheth, "An Optimized Convolution Neural Network Based Inter-Frame Forgery Detection Model-A Multi-Feature Extraction Framework", doi: [10.21917/ijivp.2021.0364](https://doi.org/10.21917/ijivp.2021.0364).
- [33] Y. Liu and T. Huang, "Exposing Video Inter-Frame Forgery By Zernike Opponent Chromaticity Moments And Coarseness Analysis," *Multimed Syst*, vol. 23, no. 2, pp. 223–238, Mar. 2017, doi: [10.1007/s00530-015-0478-1](https://doi.org/10.1007/s00530-015-0478-1).
- [34] R. Rigoni, P. G. Freitas, and M. C. Q. Farias, "Tampering Detection Of Audio-Visual Content Using Encrypted Watermarks," in *Brazilian Symposium of Computer Graphic and Image Processing*, IEEE Computer Society, Oct. 2014, pp. 196–203. doi: [10.1109/SIBGRAP.2014.50](https://doi.org/10.1109/SIBGRAP.2014.50).
-