

Multimedia Forensic Analysis of TikTok Application Using National Institute of Justice (NIJ) Method

Rachmad Nur Fauzi, Nuril Anwar

Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Kragilan, Tamanan, Daerah Istimewa Yogyakarta, 55191, Indonesia

ARTICLE INFO

Article history:

Received September 28, 2023
Revised October 11, 2023
Published October 24, 2023

Keywords:

Digital forensics,
Error level analysis,
Mobile forensics
Multimedia forensics,
TikTok

ABSTRACT

The advancement of technology, especially in mobile devices like smartphones, has had a significant impact on human life, particularly during the COVID-19 pandemic, leading to the growth of online activities, especially on social media platforms like TikTok. TikTok is a highly popular social media platform, primarily known for its focus on short videos and images often accompanied by music. However, this has also opened up opportunities for misuse, including the spread of false information and defamation. To address this issue, this research utilizes mobile forensic analysis with Error Level Analysis (ELA) to collect digital evidence related to crimes on TikTok. This research contributes by applying digital forensic techniques, specifically Error Level Analysis (ELA), to detect image manipulation on TikTok. By using forensic methods, this research helps uncover digital crimes occurring on TikTok and provides essential insights to combat misuse and criminal activities on this social media platform. The research aims to collect digital evidence from TikTok on mobile devices using MOBILedit Forensic Express Pro and authenticate it with ELA through tools like FotoForensics and Forensically, as well as manual examination. This research follows the National Institute of Justice (NIJ) methodology with ten stages of mobile forensic investigation, including scenario creation, identification, collection, investigation, and analysis. The research yields manipulated digital evidence from TikTok, primarily concerning upload times. Error Level Analysis (ELA) is used to assess the authenticity of images, revealing signs of manipulation in digital evidence. The research's contribution is to produce or collect manipulated digital evidence from TikTok, primarily concerning upload times, and to apply the Error Level Analysis (ELA) approach or technique to assess the authenticity of images, uncovering signs of manipulation in digital evidence.

This work is licensed under a [Creative Commons Attribution-Share Alike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



Corresponding Author:

Nuril Anwar, Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Kragilan, Tamanan, Daerah Istimewa Yogyakarta, 55191, Indonesia
Email: nuril.anwar@tif.uad.ac.id

1. INTRODUCTION

The rapid development of technology, especially in mobile devices like mobile phones [1], has brought both positive and negative impacts on human life. One of the side effects is that mobile phones collect a lot of crucial user data [2]. The widespread use of mobile phones [3], especially during the COVID-19 pandemic that has driven online activities, has spurred communication development, particularly through social media [4]. One highly popular social media platform is the TikTok [5] application. The concept of TikTok [6] is simple, revolving around short video and image [7] combinations, ranging from 15 to 60 seconds, featuring various types of content often accompanied by music. Apart from video sharing, TikTok [8] features social networking elements, such as follower or friend concepts, the ability to comment on content, exchange messages, conduct live broadcasts, and give virtual TikTok [9] currency gifts. Throughout the 2010s, TikTok managed to secure

a place among the top 10 most downloaded mobile apps [10]. In 2019, it even reached the 2nd rank in terms of downloads [11] and had around 800 million active users [12].

According to Sensor Tower's report for the first quarter of 2021, the TikTok [13] app was downloaded 385.6 million times. Sensor Tower reported that TikTok [14] users spent over 920 million US dollars on the app in the first quarter of 2021, marking a 74 percent increase compared to the previous year [15].

TikTok [16] has established regulations regarding uploaded content. If uploaded content contains adult, vulgar, or violent material, TikTok will automatically remove it. Despite these content upload regulations, TikTok [17] still provides users with ease in creating content on the platform.

However, the use of TikTok also carries the potential for content misuse in criminal activities, such as spreading misinformation (hoaxes) and defamation. Analysis [18] and forensic methods are required to address such misuse, especially in identifying digital crimes occurring on the TikTok application.

One of the TikTok contents related to the spread of false information (hoax) often involves images. In today's era, digital images have evolved into essential data carriers with the advancement of the internet and rapid progress in image processing tools and software. This development has made it exceedingly easy to alter images without leaving any traces. Almost every digital image we encounter in our daily lives may have undergone multiple processing stages to enhance its quality [18]. With the availability of various software, it has become easier to forge images without leaving any traces [19]. One of the most significant developments in editing tools like Adobe Photoshop, Paintshop Pro, or GIMP [20] and others includes automatic methods for editing without leaving any traces. Consequently, image tampering detection, a scheme that identifies the integrity and primitiveness of digital images, has garnered significant attention over the last decade [21], one of which is the Error Level Analysis (ELA) approach.

In this journal, the researchers employ mobile forensics [22] analysis [23] using the National Institute of Justice (NIJ) [24] methodology to gather digital evidence [25] of crimes occurring on an Android [26] smartphone, specifically the Xiaomi Redmi 6a, with TikTok installed. The analysis will involve the Error Level Analysis (ELA) [27] approach and the search for timestamps [28] of the content. Image forensics [29] is a field where Error Level Analysis, often abbreviated as ELA, is employed to identify different parts of an image that have undergone varying compression levels. This process can be employed to detect manipulated images that have been altered using editing tools. This approach can prove to be an effective preprocessing step before moving forward with modeling [30]. It is hoped that the results of this research will contribute to addressing the issue of misuse and criminal activities on this social media platform. The research's contribution is to produce or collect manipulated digital evidence from TikTok, primarily concerning upload times, and to apply the Error Level Analysis (ELA) approach or technique to assess the authenticity of images, uncovering signs of manipulation in digital evidence.

2. METHODS

Fig. 1 is a flowchart used in the mobile forensics case research [40] investigations, covering ten stages starting from Research Objectives, Scenario Creation, Experimentation, National Institute of Justice (NIJ), Recommendations, and Conclusion.

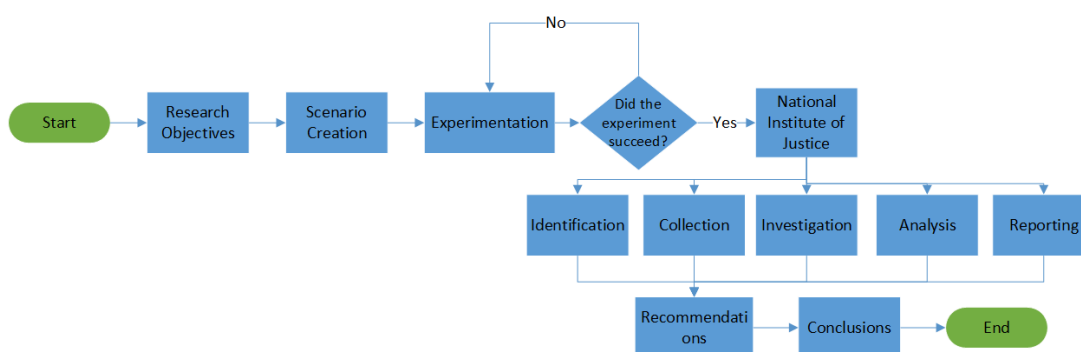


Fig. 1. Research Stages

The primary objective of this research is [31] to gather digital evidence [25] from the TikTok application installed on mobile phones as and the mobile phone devices themselves. The acquired evidence will subsequently be subjected to authentication through the [32] Error Level Analysis [33] approach using forensic tools, [34] namely FotoForensics [35] and Forensically, along with manual examination. The overarching

framework for this research is anchored within the National Institute of Justice (NIJ) paradigm [36]. Error Level Analysis (ELA) [37] is an advanced digital forensic technique that aids in identifying disturbances or image manipulations [38]. Error Level Analysis (ELA) is a technique used to detect image manipulation by restoring the image at a specific quality level and calculating the compression level ratio. Generally, this technique is applied to images in a lossy format (lossy compression). The image format used in data mining is JPEG. In JPEG images, compression is carried out independently for every 8×8 pixels in the image. If an image is not manipulated, every 8×8 pixels in the image should have the same error rate. This article examines three different levels of image compression: 10%, 50%, and 90% [39].

2.1. Scenario Creation

The research commences by constructing a forensic scenario [41] that simulates the stages involved in mobile forensics [42]. In this instance, the scenario centers on a Xiaomi Redmi 6a mobile phone, serving as pivotal evidence in a case concerning the dissemination of hoax content.

Fig. 2 the research scenario begins with the Suspect uploading hoax content about the appearance of a tiger in the Nature Reserve. This content goes viral and causes concerns among the community and visitors, leading to a decrease in the number of visitors. The Nature Reserve management reports the incident to the police and identifies the Suspect. The Suspect is apprehended with the smartphone used to upload the hoax content. The researcher conducts forensic analysis [43] using the NIJ method on the smartphone to gather and analyze images within the hoax content. Error Level Analysis (ELA) is utilized to determine the authenticity of the images and detect manipulations. The research report presents findings from the forensic process, image analysis, and conclusions regarding the authenticity of the content and the Suspect's role in disseminating the hoax content. Furthermore, an experiment is conducted by uploading hoax content on TikTok and executing the National Institute Of Justice (NIJ) method steps by the research scenario.

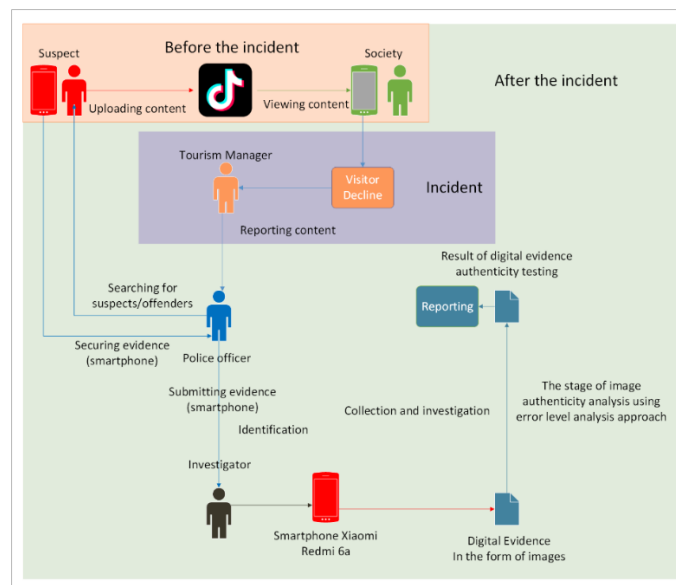


Fig. 2. Research Scenario

2.2. Identification

This phase involves data collection and preliminary preparations for the forensic investigation. Tools and resources are assembled, including an Acer Nitro 5 laptop, forensic tools, a mobile phone, the TikTok application, MD5 and SHA Checksum Utility version 2.1, Adobe Photoshop, ROOT Check version 4.5.0, and USB cables.

2.3. Collection

In this stage, the researcher will collect physical evidence related to the investigation process. The gathered physical evidence will be documented. In the context of this research case, the collected evidence includes a mobile phone with the TikTok application version 25.0.41 installed, which was used by the perpetrator to spread false information or hoaxes. The evidence has been secured by the police and will subsequently be handed over to the investigator or researcher for further analysis.

2.4. Investigation

In this stage, the examination process of the evidence collected during the collection phase will take place using "unfurl," a method aimed at determining when this content was uploaded by the TikTok user. Additionally, in this stage, the evidence will be examined through a data extraction process using the prepared forensic tools. The forensic tool utilized for this purpose is MOBILedit Forensic Express Pro [44].

Fig. 3 represents the outcome of a search conducted using Unfurl based on the TikTok link, revealing that the content's timestamps [45] indicate it was uploaded on June 15, 2023, at 07:58:33 by the account name @ahmadf75664851946.

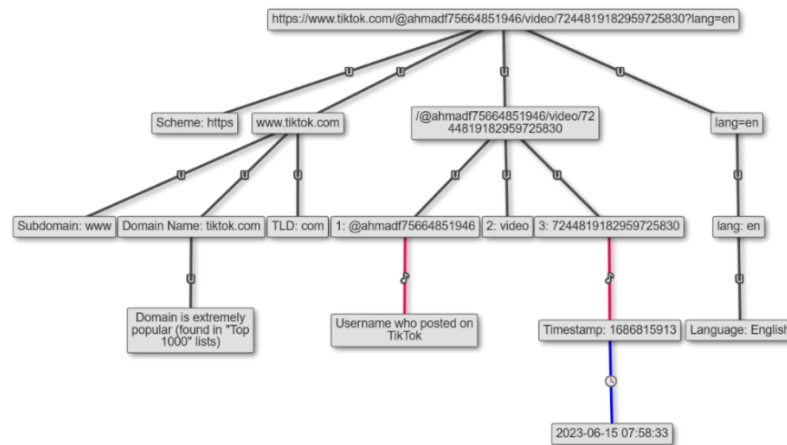


Fig. 3. Search Results

This phase entails a meticulous examination of the collected evidence. It involves employing the "unfurl" method to establish when the content was uploaded on TikTok and conducting a data extraction process using MOBILedit Forensic Express Pro [46]. During acquisition, multiple copies of the evidence are generated: a master copy reserved for trial, a second copy for further analysis, and a third backup copy. Pertinent information about the mobile phone, TikTok application, user accounts, and digital evidence, including images, is extracted and cross-referenced between the two acquisitions to verify its validity by examining file directories and checking hash values using the MD5 and SHA Checksum Utility tools for image-based digital evidence.

Table 1 is the result of acquiring evidence from a Xiaomi Redmi 6A smartphone with the TikTok application installed, using the MOBILedit Forensic Express Pro tool. Two digital evidence items were discovered, and then cross-referenced based on the digital evidence hash values from both acquisitions as a form of digital evidence validation.

Table 2 represents the results of acquiring evidence found on the Xiaomi Redmi 6A smartphone using the MOBILedit Forensic Express Pro tool. Two digital evidence items were discovered, and then cross-referenced based on the hash values from both acquisitions as a form of digital evidence validation.

Table 3 represents the metadata of digital evidence discovered in device files, where there are four files consisting of two modified files and two original files. In the case of the modified files, it is known that these files were modified on November 27, 2022, and November 28, 2022, while the original files were captured on November 4, 2019, and November 25, 2022.

Table 1. Evidence Found on Tiktok

	First Acquisition	Second Acquisition
<i>Digital Evidence</i>		
Format	cnt	cnt
Directory	phone/applications0/com.ss.android.ugc.trill/live_external/cache/picture/fresco_cache/v2.ols100.1/15/8euMmgJl2WMt	phone/applications0/com.ss.android.ugc.trill/live_external/cache/picture/fresco_cache/v2.ols100.1/15/8euMmgJl2WMt
Nilai HASH	2WMuQbHca3OSEKgfKxY.cnt 4CBFF64C8ADE942B0CF9CD01D3C2BABC	bHca3OSEKgfKxY.cnt 4CBFF64C8ADE942B0CF9CD01D3C2BABC



	First Acquisition	Second Acquisition
Digital Evidence		
Format	cnt	cnt
Direktori	phone/applications0/com.ss.android.ugc.trill/live_extal/cache/picture/fresco_cache/v2.ols100.1/25/9kq3w82OIIOPjwq3Q74ksJ-N0.cnt	phone/applications0/com.ss.android.ugc.trill/live_extal/cache/picture/fresco_cache/v2.ols100.1/25/9kq3w8Qt2OIIOPjwq3Q74ksJ-N0.cnt
HASH value	758B8E350F65CF9515CA8504C5C79327	758B8E350F65CF9515CA8504C5C79327

Table 2. Evidence Found in the Device Files









	First Acquisition	Second Acquisition
Digital Evidence		
Format	jpg	jpg
Directory	phone/raw0/min/media_rw/14C9-2062/Research/Original/IMG_3037.JPG	phone/raw0/min/media_rw/14C9-2062/Research/Original/IMG_3037.JPG
HASH value	FAA6CA0C5A53A578A305B9CB6BA6866B	FAA6CA0C5A53A578A305B9CB6BA6866B
Digital Evidence		
Format	jpg	jpg
Directory	phone/raw0/min/media_rw/14C9-2062/Research/Original/ 20221125_163854.jpg	phone/raw0/min/media_rw/14C9-2062/Research/Original/ 20221125_163854.jpg
HASH value	5941CCDFE5AB767439F426EB69E759E4	5941CCDFE5AB767439F426EB69E759E4
Digital Evidence		
Format	jpg	jpg
Directory	phone/raw0/mnt/media_rw/14C9-2062/Research/IMG_3037.jpg	phone/raw0/mnt/media_rw/14C9-2062/Research/IMG_3037.jpg
HASH value	0A8C4690384363AC4BFA1CFC2F356857	0A8C4690384363AC4BFA1CFC2F356857
Digital Evidence		
Format	jpg	jpg
Directory	phone/raw0/mnt/media_rw/14C9-2062/Research/3.jpg	phone/raw0/mnt/media_rw/14C9-2062/Research/3.jpg
HASH value	15F39EF2E3CBD69B1D8BA87EB985B65A	15F39EF2E3CBD69B1D8BA87EB985B65A

Table 3. Metadata of Digital Evidence
Original File Metadata

Exif Byte Order	: Big-endian (Motorola, MM)	Exif Byte Order	: Little-endian (Intel, II)
Make	: Canon	Make	: samsung
Camera Model Name	: Canon EOS 700D	Camera Model Name	: SM-A725F
Exposure Time	: 1/30	Orientation	: Rotate 90 CW
F Number	: 5.0	X Resolution	: 72
Exposure Program	: Manual	Y Resolution	: 72
ISO	: 200	Resolution Unit	: inches
Exif Version	: 0230	Software	: A725FXXU4BVG2
Date/Time Original	: 2019:11:04 16:52:36	Modify Date	: 2022:11:25 16:38:54
Create Date	: 2019:11:04 16:52:36	Y Cb Cr Positioning	: Centered
Shutter Speed Value	: 1/32	Exposure Time	: 1/176
Aperture Value	: 5.0	F Number	: 1.8
		Exposure Program	: Program AE
		ISO	: 80
		Exif Version	: 0220
		Date/Time Original	: 2022:11:25 16:38:54
		Create Date	: 2022:11:25 16:38:54
		Offset Time	: +07:00

Modified File Metadata

File Size	: 544 kB	File Size	: 6.7 MB
File Modification Date/Time	: 2022:11:27 17:12:14+07:00	File Modification Date/Time	: 2022:11:28 08:19:46+07:00
File Access Date/Time	: 2023:08:10 09:54:24+07:00	File Access Date/Time	: 2023:08:10 09:56:51+07:00
File Creation Date/Time	: 2023:07:15 19:47:24+07:00	File Creation Date/Time	: 2023:07:15 19:47:23+07:00
File Permissions	: -rw-rw-rw-	File Permissions	: -rw-rw-rw-
File Type	: JPEG	File Type	: JPEG
File Type Extension	: jpg	File Type Extension	: jpg
MIME Type	: image/jpeg	MIME Type	: image/jpeg
Exif Byte Order	: Big-endian (Motorola, MM)	Exif Byte Order	: Little-endian (Intel, II)
Software	: Picasa	Photometric Interpretation	: RGB
XMP Toolkit	: Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22	Make	: samsung
Creator Tool	: Picasa	Camera Model Name	: SM-A725F
MPIC Digest	: d41d8cd98f00b284e9880998ecf8427e	Orientation	: Horizontal (normal)
		Samples Per Pixel	: 3
		X Resolution	: 72
		Y Resolution	: 72
		Resolution Unit	: inches
		Software	: Adobe Photoshop 21.1 (Windows)
		Modify Date	: 2022:11:28 08:16:08
		Y Cb Cr Positioning	: Centered

2.5. Analysis

The acquired digital evidence, primarily images, is scrutinized in detail. Authentication using the Error Level Analysis (ELA) approach is carried out using two forensic tools: FotoForensics and Forensically. This involves converting RGB values to YCrCb and calculating ELA values for each image. The authenticity of the images is determined by examining their contrast and coloration patterns.

A. Analysis of TikTok Digital Evidence Using FotoForensics:

FotoForensics is one of the tools used to analyze the authenticity of an image. In this case, the researcher employs the Error Level Analysis (ELA) method to establish the authenticity of the digital evidence in the form of images. The obtained digital evidence will be uploaded to FotoForensics for analysis. The following presents the results of the digital evidence analysis using the Error Level Analysis (ELA) method.

Fig. 4 shows the results of the analysis using the Error Level Analysis (ELA) method. The analysis revealed that both pieces of digital evidence indicate signs of manipulation, as there are areas within the images with higher or lower contrast compared to other areas. If the images were genuine, they should exhibit uniform coloration across regions, without objects displaying significantly pronounced contrasts.



Fig. 4. Tiktok Digital Evidence ELA Results

B. Analysis Stage of Original Unmodified File Using FotoForensics

FotoForensics is one of the tools used to analyze the authenticity of an image. In this case, the researcher employs the Error Level Analysis (ELA) method to establish the authenticity of the digital evidence in the form of images. The obtained digital evidence will be uploaded to FotoForensics for analysis. The following presents the results of the digital evidence analysis using the Error Level Analysis (ELA) method.

Fig. 5 the ELA approach is employed on unmodified original images, revealing consistent coloration patterns across the images and no pronounced contrasts or alterations.



Fig. 5. ELA Result of Original File

C. Analysis Stage of Original Unmodified File Using Forensically

FotoForensics is one of the tools used to analyze the authenticity of an image. In this case, the researcher employs the Error Level Analysis (ELA) method to establish the authenticity of the digital evidence in the form of images. The obtained digital evidence will be uploaded to FotoForensics for analysis. The following presents the results of the digital evidence analysis using the Error Level Analysis (ELA) method.

Fig. 6 displays the analysis outcome using the Error Level Analysis (ELA) method. For the first image, with a JPEG Quality of 90, Error Scale of 15, and Opacity of 0.95, and the second image, with a JPEG Quality of 83, Error Scale of 21, and Opacity of 1.00, both pieces of digital evidence from the original unmodified photo are not identified as manipulated. The analysis reveals that the coloration across the areas in both images remains uniform, and no objects with different or brighter coloration appear.

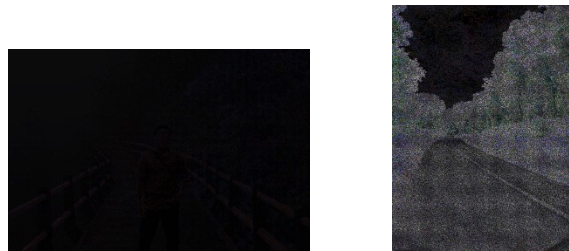


Fig. 6. ELA Result of the Original File

Next, the researcher determines the RGB values of the ELA images using Adobe Photoshop. The process involves converting the RGB values to YCrCb to ascertain the luminance and chrominance values in an 8×8 kernel of the compressed image. The difference between the average luminance and chrominance values (μ) is then calculated to obtain the Error Level Analysis (ELA) value (Q_n) using the following formulas:

The formula for converting RGB values to YCrCb values is as follows:

$$\begin{aligned} Y &= 0.257 \times R + 0.504 \times G + 0.098 \times B + 16 \\ Cb &= -0.257 \times R - 0.291 \times G + 0.439 \times B + 128 \\ Cr &= 0.439 \times R - 0.368 \times G - 0.071 \times B + 128 \end{aligned}$$

The formula to calculate the Error Level Analysis (ELA) value is as follows:

$$\begin{aligned} \mu &= \frac{(Y + Cr + Cb)}{3} \\ \Delta &= |Y - Cr| \times (1.0 - 0.51) + |Y - Cb| \times (1.0 - 0.51) \\ Q_n &= 100 - \mu - \Delta \end{aligned}$$

Table 4 is the first table displaying the results of RGB value searches using Adobe Photoshop tools from the original image within the coordinate range of 1,1 to 8,8. Subsequently, perform additional RGB value searches up to the maximum limit that can be searched, following an 8×8 pattern or coordinates 1,1 to 8,8 repeatedly.

Table 5 is a table presenting the conversion of RGB values to YCrCb values to determine the luminance and chrominance values within an 8×8 kernel of a compressed image. Subsequently, perform additional searches for YCrCb values up to the maximum limit that can be searched based on the RGB values obtained earlier, following an 8×8 pattern or coordinates 1,1 to 8,8 repeatedly.

In Table 6 it can be observed that the Error Level values vary for each coordinate, indicating different levels of Error Level in each coordinate within the 8×8 grid. However, the differences in values are not significantly large. The same calculation process will be performed for the second image, similar to what was done for the first image.

Table 4. Coordinates 8×8

Coordinates	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
R	11	11	11	11	11	11	11	10
G	11	11	11	11	11	11	11	10
B	11	11	11	11	11	11	11	11
Coordinates	2,1	2,2	2,3	2,4	2,5	2,6	2,7	2,8
R	11	11	11	11	11	11	10	10
G	11	11	11	11	11	11	10	10
B	11	11	11	11	11	11	11	10
Coordinates	3,1	3,2	3,3	3,4	3,5	3,6	3,7	3,8
R	10	10	10	10	10	10	9	8
G	10	10	10	10	10	10	9	8
B	11	11	11	11	11	10	9	8
Coordinates	4,1	4,2	4,3	4,4	4,5	4,6	4,7	4,8
R	10	10	10	10	10	10	9	8
G	10	10	10	10	10	10	9	8
B	10	11	10	10	10	10	9	8
Coordinates	5,1	5,2	5,3	5,4	5,5	5,6	5,7	5,8
R	10	10	10	10	10	9	8	8
G	10	10	10	10	10	9	8	8
B	10	10	10	10	10	9	8	8
Coordinates	6,1	6,2	6,3	6,4	6,5	6,6	6,7	6,8
R	9	9	9	9	9	9	8	8
G	9	9	9	9	9	9	8	7
B	10	9	10	9	9	9	8	7
Coordinates	7,1	7,2	7,3	7,4	7,5	7,6	7,7	7,8
R	8	7	8	8	8	8	9	9
G	8	8	8	8	8	7	8	8
B	8	9	8	9	8	8	8	9
Coordinates	8,1	8,2	8,3	8,4	8,5	8,6	8,7	8,8
R	7	7	7	7	7	8	7	9
G	7	7	7	7	7	7	7	8
B	8	7	7	7	8	8	8	9

Table 5. Converting RGB values to YCrCb values

Coordinates	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
Y	25.449	25.449	25.449	25.449	25.449	25.449	25.449	24.688
CB	128	128	128	128	128	128	128	128.439
CR	128	128	128	128	128	128	128	127.929
Coordinates	2,1	2,2	2,3	2,4	2,5	2,6	2,7	2,8
Y	25.449	25.449	25.449	25.449	25.449	25.449	24.688	24.59
CB	128	128	128	128	128	128	128.439	128
CR	128	128	128	128	128	128	127.929	128
Coordinates	3,1	3,2	3,3	3,4	3,5	3,6	3,7	3,8
Y	24.688	24.688	24.688	24.688	24.688	24.59	23.731	22.872
CB	128.439	128.439	128.439	128.439	128.439	128	128	128
CR	127.929	127.929	127.929	127.929	127.929	128	128	128
Coordinates	4,1	4,2	4,3	4,4	4,5	4,6	4,7	4,8
Y	24.59	24.688	24.59	24.59	24.59	24.59	23.731	22.872
CB	128	128.439	128	128	128	128	128	128
CR	128	127.929	128	128	128	128	128	128
Coordinates	5,1	5,2	5,3	5,4	5,5	5,6	5,7	5,8
Y	24.59	24.59	24.59	24.59	24.59	23.731	22.872	22.872
CB	128	128	128	128	128	128	128	128
CR	128	128	128	128	128	128	128	128
Coordinates	6,1	6,2	6,3	6,4	6,5	6,6	6,7	6,8
Y	23.829	23.731	23.829	23.731	23.731	23.731	22.872	22.27
CB	128.439	128	128.439	128	128	128	128	127.852
CR	127.929	128	127.929	128	128	128	128	128.439
Coordinates	7,1	7,2	7,3	7,4	7,5	7,6	7,7	7,8
Y	22.872	22.713	22.872	22.97	22.872	22.368	23.129	23.227
CB	128	128.587	128	128.439	128	128.291	127.852	128.291
CR	128	127.49	128	127.929	128	128.368	128.439	128.368
Coordinates	8,1	8,2	8,3	8,4	8,5	8,6	8,7	8,8
Y	22.111	22.013	22.013	22.013	22.111	22.368	22.111	23.227
CB	128.439	128	128	128	128.439	128.291	128.439	128.291
CR	127.929	128	128	128	127.929	128.368	127.929	128.368

Table 6. Error Level Analysis values

Coordinates	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
μ	94	94	94	94	94	94	94	94
Δ	-100	-100	-100	-100	-100	-100	-100	-101
Qn	107	107	107	107	107	107	107	108
Coordinates	2	2	2	2	3	3	3	3
μ	94	94	94	94	94	94	94	94
Δ	-100	-100	-100	-100	-100	-100	-101	-101
Qn	107	107	107	107	107	107	108	108
Coordinates	3	3	3	3	4	4	4	4
μ	94	94	94	94	94	94	94	93
Δ	-101	-101	-101	-101	-101	-101	-102	-103
Qn	108	108	108	108	108	108	109	110
Coordinates	4	4	4	4	5	5	5	5
μ	94	94	94	94	94	94	93	93
Δ	-101	-101	-101	-101	-101	-101	-102	-103
Qn	108	108	108	108	108	108	109	110
Coordinates	5	5	5	5	6	6	6	6
μ	94	94	94	94	94	93	93	93
Δ	-101	-101	-101	-101	-101	-102	-103	-103
Qn	108	108	108	108	108	109	110	110
Coordinates	6	6	6	6	7	7	7	7
μ	93	93	93	93	93	93	93	93
Δ	-102	-102	-102	-102	-102	-102	-103	-104
Qn	109	109	109	109	109	109	110	111
Coordinates	7	7	7	7	8	8	8	8
μ	93	93	93	93	93	93	93	93
Δ	-103	-103	-103	-103	-103	-104	-103	-103
Qn	110	110	110	110	110	111	110	110
Coordinates	8	8	8	8	9	9	9	9
μ	93	93	93	93	93	93	93	93
Δ	-104	-104	-104	-104	-104	-104	-104	-103
Qn	111	111	111	111	111	111	111	110

D. Digital Evidence Using Forensically

Forensically is one of the tools used to analyze the authenticity of an image. In this case, the researcher employs the Error Level Analysis (ELA) method to establish the authenticity of the digital evidence in the form of images. The obtained digital evidence will be uploaded to Forensically for analysis. The following presents the results of the digital evidence analysis using the Error Level Analysis (ELA) method.

Fig. 7 displays the analysis outcome using the Error Level Analysis (ELA) method. For the first image, with JPEG Quality of 90, an Error Scale of 15, and an Opacity of 0.95, the first piece of digital evidence is identified as manipulated. In this image, certain areas exhibit higher contrast or brightness compared to other areas. Similarly, for the second image, with JPEG Quality 83, Error Scale 21, and Opacity 1.00, the second piece of digital evidence is also identified as manipulated. In this image, areas with purplish hues contrast with the brighter dominant areas. In an authentic image, coloration should remain consistent across regions.



Fig. 7. ELA Result of TikTok File

Next, the researcher will proceed to determine the YCrCb values and the Error Level Analysis (ELA) (Qn) values by performing calculations similar to those conducted in the analysis stage of the original unmodified file.

2.6. Reporting

The acquired evidence, including the mobile phone with the TikTok application (version 25.0.41), serves as the cornerstone of the investigation. Data extracted from the mobile phone provides crucial information about the suspect, user accounts, and digital evidence. Metadata from the hoax content, including timestamps, is extracted using the Unfurl tool.

2.7. Recommendations

In this stage, the researcher provides recommendations for tools to analyze the authenticity of images using the Error Level Analysis (ELA) method based on the previous research stages. FotoForensics is a free image analysis tool with an intuitive user interface that is easy to use. However, it's only accessible in Indonesia through a VPN, and its features are limited to compression analysis and automated manipulation detection.

On the other hand, Forensically offers more comprehensive features in forensic image analysis without requiring a VPN. This tool provides a wide range of analysis features and offers in-depth analysis of compression levels, colors, and signs of manipulation in images. However, its complex interface and lack of explanations about its features might pose challenges.

When selecting a tool for image analysis, it's important to consider the pros and cons of each tool. If ease of use and a focus on manipulation detection are the primary factors, FotoForensics might be the preferred choice. However, if more features and flexibility in image compression settings are required, Forensically could be a good alternative.

3. RESULTS AND DISCUSSION

The research stages encompassed the acquisition of timestamps from Unfurl searches and metadata, as well as the authenticity analysis of images through the application of the Error Level Analysis (ELA) method using tools like FotoForensics and Forensically.

Table 7 provides a comprehensive overview of timestamps associated with the extracted digital evidence from both the TikTok application and the suspect's mobile phone device. The table delineates the dates of evidence capture, modification, and uploading.

Table 7. Timestamps

Evidence	Capture	Modified	Uploaded
Evidence 1	November 4, 2019	November 27, 2022	June 15, 2023
Evidence 2	November 25, 2022	November 28, 2022	June 15, 2023

After calculating the Error Level Analysis values for the 8x8 pixel grid, the next step is to differentiate the obtained Error Level Analysis values. This process is also performed on an 8x8 pixel grid by selecting values that differ from the common values. These values differing from the common values are considered Error Level Analysis values.

A. Modified Files of TikTok Digital Evidence

1. First Piece of Digital Evidence

In the first digital evidence, after the calculation to find its Error Level Analysis values has been performed, the subsequent step involves sorting the error values to determine which part of the image has varying error values.

Fig. 8 represents the outcome of Error Level Analysis, where, in the first box, there is a diverse range of values, spanning from 83 to 98 and 100 to 111. In Error Level Analysis, pixels with higher error values appear relatively darker in color. The error value range between 83 and 98 likely indicates alterations or manipulations in those pixels. This suggests that changes or manipulations have occurred in only a relatively small part of the entire photograph.

103	104	103	104	104	100	101	103
104	104	104	104	103	100	106	106
104	105	104	102	101	101	101	103
104	104	103	103	105	111	83	102
103	104	104	104	106	104	97	105
103	104	105	106	104	104	98	102
103	106	106	106	106	103	103	96
106	107	108	107	104	105	101	102

103	103	103	102	105	102	101	93
104	105	104	102	105	104	99	98
104	103	103	102	103	104	101	102
102	102	103	103	105	103	98	99
102	100	100	103	104	105	98	94
102	102	101	97	99	97	95	97
100	101	99	100	100	97	96	88
100	101	101	100	99	99	93	88

Fig. 8. Sorting of Error Level Analysis Values for The First Piece of Digital Evidence

In the second box, a range of values varying from 88 to 100 and 101 to 105 can be seen. However, the values within coordinates 1,1 to 8,8 are more uniform, indicating no significant changes. In Error Level Analysis, pixels with higher error values will appear relatively darker.

B. Second Piece of Digital Evidence

In the second digital evidence, after the calculation to find its Error Level Analysis values has been performed, the subsequent step involves sorting the error values to determine which part of the image has varying error values.

Fig. 9 depicts the sorting of Error Level Analysis values for the second piece of digital evidence. Similar to the first piece, diverse values between 1 to 29 and 34 to 95 indicate potential changes. Notably, the range between 29 and 26 in coordinates 8,7 to 8,8 implies alterations in these areas.

36	91	89	93	94	95	75	28
15	90	94	92	90	82	8	3
20	88	89	89	86	55	7	9
10	34	88	85	85	33	10	12
4	46	81	89	58	5	9	12
8	13	15	20	8	17	15	19
6	11	11	24	15	12	5	3
5	6	26	29	9	1	29	26

Fig. 9. Sorting of Error Level Analysis Values for The Second Piece of Digital Evidence

C. Original Files

1. First Original File

In the first digital evidence, after the calculation to find its Error Level Analysis values has been performed, the subsequent step involves sorting the error values to determine which part of the image has varying error values.

Fig. 10 represents the outcome of Error Level Analysis, where, in the first box, a diverse range of values can be observed, ranging from 107 to 111. However, the values within coordinates 1,1 to 8,8 are more uniform, indicating no significant changes. In Error Level Analysis, pixels with higher error values will appear relatively darker.

107	107	107	107	107	107	107	108
107	107	107	107	107	107	108	108
108	108	108	108	108	108	109	110
108	108	108	108	108	108	109	110
108	108	108	108	108	109	110	110
109	109	109	109	109	109	110	111
110	110	110	110	110	111	110	110
111	111	111	111	111	111	111	110

109	110	111	111	112	111	111	112
110	111	111	112	110	110	110	111
110	111	111	110	110	111	111	112
111	111	110	110	111	111	111	112
111	110	110	110	111	110	109	111
111	111	112	110	110	111	111	112
110	111	111	110	110	111	110	112
110	112	114	113	111	111	111	111

Fig. 10. Sorting of Error Level Analysis Values for The First Original File

In the second box, a range of values varying from 109 to 114 can be seen. However, the values within coordinates 1,1 to 8,8 are more uniform, indicating no significant changes. In Error Level Analysis, pixels with higher error values will appear relatively darker.

2. Second Original File

In the second digital evidence, after the calculation to find its Error Level Analysis values has been performed, the subsequent step involves sorting the error values to determine which part of the image has varying error values.

Fig. 11 showcases the sorting of Error Level Analysis values for the second original file. A broad value range between 30 and 109 is observed, while values within coordinates 1,1 to 8,8 maintain uniformity.

Table 8 elucidates the comparison of analysis results derived from both FotoForensics and Forensically tools. All images demonstrate positive indications for Error Level Analysis under both tools, underscoring their efficacy in processing and analyzing images through this method. Consequently, it can be inferred that the Error Level Analysis method is adept at detecting variations indicative of editing or manipulation processes.

62	101	98	104	108	109	90	53
41	103	105	102	104	95	31	25
41	97	99	96	98	76	27	27
31	51	96	98	97	51	38	40
30	64	94	100	79	30	40	42
38	36	37	47	35	42	41	40
32	40	32	48	40	29	24	24
45	40	59	61	41	30	32	25

Fig. 11. Sorting of Error Level Analysis Values for The Second Original File

Table 8. Comparison of Analysis Results from Both Forensic Tools

Digital Evidence	FotoForensic	Forensically	Error Level Analysis
Photo 1	✓	✓	✓
Photo 2	✓	✓	✓

The results demonstrate the successful application of the Error Level Analysis method to ascertain the authenticity of images within the TikTok context. Timestamps obtained from the Unfurl searches and metadata offer crucial temporal context for the digital evidence. Moreover, the method's ability to identify potential alterations or manipulations in specific areas of the images underscores its value in forensic image analysis.

The uniform Error Level Analysis values within the original files further substantiate their unaltered nature. Similarly, the diverse values within the modified files indicate possible manipulation in localized regions, reaffirming the method's capability in detecting even subtle changes.

The comparative analysis results from FotoForensics and Forensically tools emphasize the reliability of the Error Level Analysis method in flagging variations that could signify tampering. This robust validation process reinforces the suitability of the selected tools and approach for authenticating digital evidence.

In conclusion, the research outcomes substantiate the viability of utilizing the Error Level Analysis method, alongside specialized forensic tools, to determine the authenticity of images within the TikTok environment. The chronological context offered by timestamps enhances the interpretive value of the evidence. The consistency of the Error Level Analysis method's outcomes across different tools bolsters its credibility and positions it as a valuable asset in addressing digital crimes involving image manipulation or editing.

Furthermore, the results of the study titled "Pengembangan Metode Pendeteksi Modifikasi Citra Menggunakan Metode Error Level Analysis" indicate that the Image Processing Application for Detecting Image Modifications Using Android-Based Error Level Analysis Method has two main functions, namely, ELA filter and ELA value analysis. The ELA filter function is influenced by factors such as image contrast and brightness used in image modifications. The results of ELA filter testing show that the Error Level Analysis method has tolerance in detecting modified images, provided that these images have high contrast and brightness values.

Moreover, the ELA value analysis successfully detects modified images that were not detected by the ELA filter. The range of ELA percentage values used to detect modified test images varies from 2.27% to 72.98%, with a threshold value of 8. These test results also note a possible error rate of 35%. These research findings serve as the foundation or reference for the application of the Error Level Analysis (ELA) method in this study.

4. CONCLUSION

The findings of this research underscore the critical role that image authenticity analysis holds in the context of digital forensics. The evidence gleaned from the study strongly suggests that the digital evidence, particularly images extracted from the TikTok application and the mobile phone device, has undergone manipulation or editing that could impede their authenticity and integrity. This revelation necessitates the deployment of sophisticated analysis techniques to ensure the accuracy and reliability of digital evidence.

The Error Level Analysis (ELA) method, coupled with the strategic application of the National Institute of Justice (NIJ) framework, has proven to be a potent arsenal for detecting potential instances of image manipulation. Through meticulous investigation and the establishment of rigorous standards, this study has demonstrated the utility of these tools in not only identifying manipulated images but also in illuminating the stages of tampering.

In essence, the study has illuminated the indispensable nature of image authenticity analysis, particularly within dynamic digital environments like TikTok. This research not only contributes to the growing body of knowledge in digital forensics but also underscores the significance of methodological precision and advanced tools in safeguarding the integrity of digital evidence.

As digital platforms continue to evolve and expand, the lessons learned from this research will be instrumental in refining investigative methodologies, enhancing legal proceedings, and ultimately strengthening the foundations of justice in the digital realm. By providing an effective means to scrutinize and assess the authenticity of images, the Error Level Analysis technique, in conjunction with the NIJ framework, emerges as a powerful tool in the hands of investigators striving to ensure the veracity of digital evidence.

Future studies could delve deeper into the nuances of image manipulation techniques and their detection, further refining the methodologies outlined in this research. Furthermore, the implications of this research extend beyond the field of digital forensics, resonating in the broader realms of cybersecurity, media integrity, and the increasingly interconnected digital landscape.

In conclusion, the study not only sheds light on the necessity of upholding digital evidence integrity but also highlights the transformative potential of forensic methodologies and tools in a digital world where the authenticity of visual information is paramount.

REFERENCES

- [1] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty, *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices*. Packt Publishing Ltd, 2014, https://books.google.co.id/books?hl=id&lr=&id=TU_cDwAAQBAJ.
- [2] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, "Post-mortem digital forensic artifacts of TikTok Android App," *ACM Int. Conf. Proceeding Ser.*, pp. 1-8, 2020, <https://doi.org/10.1145/3407023.3409203>.
- [3] A. Leonardo and R. Indrayani, "The Comparison Performance of Digital Forensic Tools Using Additional Root Access Options," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 7, no. 3, p. 512, 2022, <https://doi.org/10.26555/jiteki.v7i3.22381>.
- [4] C. Hargreaves, "Digital Forensics Education: A New Source of Forensic Evidence," *Forensic Science Education and Training: A Tool-kit for Lecturers and Practitioner Trainers*, pp. 73-85. 2017, <https://doi.org/10.1002/9781118689196.ch6>.
- [5] N. H. Khoa, P. T. Duy, H. D. Hoang, D. T. Thu Hien, and V. H. Pham, "Forensic analysis of TikTok application to seek digital artifacts on Android smartphone," *Proc. RIVF Int. Conf. Comput. Commun. Technol. RIVF*, 2020, <https://doi.org/10.1109/RIVF48685.2020.9140739>.
- [6] R. N. Ria and T. Setiawan, "Forensic Linguistic Analysis of Netizens' Hate Speech Acts in Tik-Tok Comment Section," *BloLAE*, vol. 5, no. 2, pp. 141-152, 2021, <https://doi.org/10.33258/biolae.v5i2.894>.
- [7] A. Nakamura *et al.*, "Independent component analysis of hyperspectral data measured from overlapping latent fingerprints: Forensic potential of independent component images," *Forensic Sci. Int.*, vol. 343, p. 111549, 2023, <https://doi.org/10.1016/j.forciint.2022.111549>.
- [8] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," *Int. J. Comput. Appl.*, vol. 175, no. 34, pp. 47-52, 2020, <https://doi.org/10.5120/ijca2020920897>.
- [9] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, "Analyzing tiktok from a digital forensics perspective," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 12, no. 3, pp. 87-115, 2021. <https://doi.org/10.22667/JOWUA.2021.09.30.087>.
- [10] "Facebook owns the four most downloaded apps of the decade - BBC News." <https://www.bbc.com/news/technology-50838013> (accessed Jul. 25, 2023).
- [11] "TikTok and WhatsApp top the app downloads for 2019 - BBC Newsround." <https://www.bbc.co.uk/newsround/51117970> (accessed Jul. 25, 2023).
- [12] "TikTok: What is the app and how much data does it collect? - BBC News." <https://www.bbc.com/news/technology-53476117> (accessed Jul. 25, 2023).
- [13] D. B. V. Kaye, X. Chen, and J. Zeng, "The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok," *Mob. Media Commun.*, vol. 9, no. 2, pp. 229-253, 2021, <https://doi.org/10.1177/2050157920952120>.
- [14] J. C. Medina Serrano, O. Papakyriakopoulos, and S. Hegelich, "Dancing to the Partisan Beat: A First Analysis of Political Communication on TikTok," *WebSci - Proc. 12th ACM Conf. Web Sci.*, pp. 157-166, 2020, <https://doi.org/10.1145/3394231.3397916>.
- [15] "Global App Spending Approached \$65 Billion in the First Half of 2021, Up More Than 24% Year-Over-Year." <https://sensortower.com/blog/app-revenue-and-downloads-1h-2021> (accessed May 05, 2022).
- [16] Y. Keim, S. Hutchinson, A. Shrivastava, and U. Karabiyik, "Forensic Analysis of TikTok Alternatives on Android and iOS Devices: Byte, Dubsplash, and Triller," *Electron.*, vol. 11, no. 18, 2022, <https://doi.org/10.3390/electronics11182972>.
- [17] A. Neyaz, A. Kumar, S. Krishnan, J. Placker, and Q. Liu, "Security, Privacy and Steganographic Analysis of FaceApp and TikTok," *Int. J. Comput. Sci. Secur.*, vol. 14, no. 2, pp. 38-59, 2020, <https://www.csejournals.org/manuscript/Journals/IJCSS/Volume14/Issue2/IJCSS-1552.pdf>.
- [18] R. Montasari and R. Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," *Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3*, pp. 205-212, 2019, <https://doi.org/10.1109/ICGS3.2019.8688020>.
- [19] O. M. Al-Qershi and B. E. Khoo, "Enhanced block-based copy-move forgery detection using k-means clustering," *Multidimens. Syst. Signal Process.*, vol. 30, no. 4, pp. 1671-1695, 2019, <https://doi.org/10.1007/S11045-018-0624->

Y/METRICS.

- [20] A. Kumar, G. Singh, A. Kansal, and K. Singh, "Digital image forensic approach to counter the JPEG anti-forensic attacks," *IEEE Access*, vol. 9, 2020, <https://doi.org/10.1109/ACCESS.2020.3048246>.
- [21] X. Y. Wang, C. Wang, L. Wang, L. X. Jiao, H. Y. Yang, and P. P. Niu, "A fast and high accurate image copy-move forgery detection approach," *Multidimens. Syst. Signal Process.*, vol. 31, no. 3, pp. 857–883, 2020, <https://doi.org/10.1007/S11045-019-00688-X/METRICS>.
- [22] D. Kim and S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200897, 2020, <https://doi.org/10.1016/j.fsidi.2019.200897>.
- [23] H. Heath, A. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?," *Forensic Sci. Int. Digit. Investig.*, vol. 46, 2023, <https://doi.org/10.1016/j.fsidi.2023.301585>.
- [24] L. Zarwell, "National Institute of Justice Research and Development Programs: Implementation and Impact," *Forensic Sci. Int. Synerg.*, vol. 4, p. 100262, 2022, <https://doi.org/10.1016/j.fsisyn.2022.100262>.
- [25] C. T. Li, "Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions," *Inf. Sci. Ref.*, pp. 470–495, 2010, Accessed: Jun. 25, 2022. [Online]. Available: <http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-60566-836-9.ch020>.
- [26] M. B. Blankesteijn, A. Fukami, and Z. J. M. H. Geradts, "Assessing data remnants in modern smartphones after factory reset," *Forensic Sci. Int. Digit. Investig.*, vol. 46, p. 301587, 2023, <https://doi.org/10.1016/j.fsidi.2023.301587>.
- [27] I. B. K. Sudiatmika, F. Rahman, Trisno, and Suyoto, "Image forgery detection using error level analysis and deep learning," *Telkomnika (Telecommunication Comput. Electron. Control.)*, vol. 17, no. 2, pp. 653–659, 2019, <https://doi.org/10.12928/TELKOMNIKA.V17I2.8976>.
- [28] R. Nordvik and S. Axelsson, "It is about time—Do exFAT implementations handle timestamps correctly?," *Forensic Sci. Int. Digit. Investig.*, vol. 42–43, p. 301476, 2022, <https://doi.org/10.1016/j.fsidi.2022.301476>.
- [29] A. Piva, "An Overview on Image Forensics," *ISRN Signal Process.*, vol. 2013, pp. 1–22, 2013, <https://doi.org/10.1155/2013/496701>.
- [30] A. Gupta, R. Joshi, and R. Laban, "Detection of Tool based Edited Images from Error Level Analysis and Convolutional Neural Network," *arXiv preprint arXiv:2204.09075*, 2022, [Online]. Available: <http://arxiv.org/abs/2204.09075>.
- [31] M. F. Nafiz, D. Kartini, M. R. Faisal, F. Indriani, and T. Hamonangan, "Automated Detection of COVID-19 Cough Sound using Mel- Spectrogram Images and Convolutional Neural Network," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 9, no. 3, pp. 535–548, 2023, <https://doi.org/10.26555/jiteki.v9i3.26374>.
- [32] E. Ramadhani, "Photo splicing detection using error level analysis and laplacian-edge detection plugin on GIMP," *J. Phys. Conf. Ser.*, vol. 1193, no. 1, 2019, <https://doi.org/10.1088/1742-6596/1193/1/012013>.
- [33] N. Kumar, P. Naik, N. Raina, and D. Kayande, "Image Forgery: Detection of Manipulated Images Using Neural Network," *SSRN Electron. J.*, 2020, <https://doi.org/10.2139/ssrn.3682481>.
- [34] D. R. Tobergte and S. Curtis, *Computational Forensics, Digital Crime and Investigation*, vol. 53, no. 9, 2013.
- [35] Z. Khalid and S. Qadir, "An Evaluation Framework For Digital Image Forensics Tools," *J. Digit. Forensics, Secur. Law*, vol. 17, no. 4, pp. 1–13, 2022, <https://commons.erau.edu/jdfsl/vol17/iss2/4/>.
- [36] I. G. N. Guna Wicaksana and I. K. Gede Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 381, 2020, <https://doi.org/10.24843/jlk.2020.v08.i04.p03>.
- [37] C. G. Sri, S. Bano, T. Deepika, N. Kola, and Y. L. Pranathi, "Deep Neural Networks Based Error Level Analysis for Lossless Image Compression Based Forgery Detection," *Int. Conf. Intell. Technol. CONIT*, pp. 1-8, 2021, <https://doi.org/10.1109/CONIT51480.2021.9498357>.
- [38] Ali Dehghantanha, "ELA: Error Level Analysis," *TEHNIKA*, vol. 72, 2023, <https://doi.org/10.5937/tehnika2304445R>.
- [39] W. P. Sari and H. Fahmi, "Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 3, 2021, <https://doi.org/10.22219/kinetik.v6i3.1272>.
- [40] G. Humphries, R. Nordvik, H. Manifavas, P. Cobley, and M. Sorell, "Law enforcement educational challenges for mobile forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301129, 2021, <https://doi.org/10.1016/j.fsidi.2021.301129>.
- [41] T. Fischer *et al.*, "Profiling and imaging of forensic evidence – A pan-European forensic round robin study part 1: Document forgery," *Sci. Justice*, vol. 62, no. 4, pp. 433–447, 2022, <https://doi.org/10.1016/j.scijus.2022.06.001>.
- [42] I. Riadi, S. Sunardi, and P. Widiandana, "Mobile Forensics for Cyberbullying Detection using Term Frequency - Inverse Document Frequency (TF-IDF)," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 5, no. 2, p. 68, 2020, <https://doi.org/10.26555/jiteki.v5i2.14510>.
- [43] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, and J. Kim, "Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data," *Forensic Sci. Int. Digit. Investig.*, vol. 37, p. 301138, 2021, <https://doi.org/10.1016/j.fsidi.2021.301138>.
- [44] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, <https://doi.org/>

[10.5120/ijca2021921076](https://doi.org/10.5120/ijca2021921076).

- [45] J. Han and S. Lee, "A Study on the Processing of Timestamps in the Creation of Multimedia Files on Mobile Devices," *J. Inf. Process. Syst.*, vol. 18, no. 3, pp. 402–410, 2022, [https://doi.org/ 10.3745/JIPS.04.0245](https://doi.org/10.3745/JIPS.04.0245).
- [46] I. Riadi, A. Fadlil, and A. Fauzan, "A study of mobile forensic tools evaluation on android-based LINE messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206, 2018, [https://doi.org/ 10.14569/IJACSA.2018.091024](https://doi.org/10.14569/IJACSA.2018.091024).

BIOGRAPHY OF AUTHORS



Rachmad Nur Fauzi is an undergraduate student in the Department of Informatics at Universitas Ahmad Dahlan. His research interest is centered around Mobile Forensics. Email: rachmad1900018326@webmail.uad.ac.id.



Nuril Anwar, is a lecturer in Departement of Informatics at Universitas Ahmad Dahlan. His research interest is centered on Computer Networks & Security, Digital Forensics. Email: nuril.anwar@tif.uad.ac.id.