Image Forensics to Detect Image Authenticity using Error Level Analysis and Noise Analysis Methods

Ocha Maulidya
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
Digital development is so rapid that it is easy to change the image, especially the image on the image. It can be made and changed as desired if taking the definition of a digital image itself is evidence of information technology presenting an object in a computer device. Processing images like this is easy, even without leaving a trace of its use. The rapid development of editing tools makes manipulating image images easier for technology users. There are examples of three image manipulation techniques: splicing imagery, copy-move image, and retouching imagery. Image manipulation can also be dangerous because there are many cases of spreading unsubstantiated hoax news, including the spread of fake photos. If left unchecked, this will impact thinking and visualization, where people cannot distinguish between real and fake news. This is the basis for conducting this research, detecting changes in an image using the Error Level Analysis and Noise Analysis methods. This research is expected to produce and provide good results in detecting these image objects to help users and increase knowledge.

Keywords
Digital Forensics, Image Forensics, Digital Imagery, Error Level Analysis, Noise Analysis, Twitter, ForensicallyBeta

1. INTRODUCTION
Digital image is one of the pieces of evidence of information technology that presents an object in a computer device. Digital images can be obtained on digital cameras that will be processed directly into the computer [1]. One is image processing on images, which can be created and manipulated easily, leaving no visible traces to its users. The ease of creating and changing images can damage the image's credibility on various sides. As a result, prone to being used for bad things because of changes in the image of the image, and all the information conveyed will be different [2]. Photos that have been manipulated develop very quickly and sophisticatedly, making it impossible for someone to distinguish just from casual observation whether the image is original or has been manipulated [3].

The rapid development of editing software makes manipulating images easier for technology users. There are three image manipulation techniques: image splicing, image retouching, and copy-move image manipulation [4]. Currently, image manipulation is often misused by most people to be used as a medium for creating fake images or hoaxes. A type of image manipulation that is very common and often used by someone is to perform copy-move image manipulation techniques. The copy-move method is often used because it is easy and efficient [5]. Image manipulation through copy-move means covering some subjects in a view through others with a similar idea. Identifying copy-move in an image can be attempted in the spatial region by working within each pixel or in the frequency region through shape-shifting [6].

The internet world is filled with information about hoaxes, provocations, slander, and even intolerant attitudes toward religion. Therefore, information that has yet to be declared the truth spreads rapidly through the internet as an online tool. Since the presidential election will be held in 2024, fake news, including manipulated photos, will be easy to find. Even people who have yet to have time to understand the meaning of the news will react to the information that was circulated first [7].

Digital forensics is a field that intends to obtain data and detect digital evidence to be accounted for in a legal assembly. Digital evidence results from objects from electronic goods such as PCs, cellphones, notebooks, servers, or other communication equipment. Categorized as a storage tool and can be analyzed as evidence [8]. One of the applications of forensics is image forensics. Image forensics itself is divided into two types, namely active authentication and passive authentication. Active authentication is a procedure used to ensure the view by requiring bonus data about the image's authenticity; this matter is used to embed a watermark on the purity of the image itself. On the other hand, passive authentication acts as a blind detection method or does not require extra data on the image [9]. To perform detection on the image, several methods can be used, such as Error Level Analysis (ELA), Hue Saturation Value (HSV), Clone Detection, Principal Component Analysis (PCA), Metadata, Noise Analysis, and JPEG Analysis.

In this research, the forensic field methods used are Error Level Analysis (ELA) and Noise Analysis, a way to understand the percentage of analyzing images in the filter results. Noise Analysis is said to be able to see or recognize the detection of image cloning in the image to be used with different points of light contrast. Then the image format for research is Joint Photographic Experts Group or JPEG. This format was chosen because it is highly supported on all devices and various applications, one of which is with tools in the form of Forensicallybeta.

From the background that has been described, the two methods that will be used function to detect the level of authenticity in an image, and the final results will be compared as learning and knowledge. Using the Forensicallybeta tool is hoped to facilitate the equation between the original image and the image that has been falsified. As a result, it can be used by many people to determine the purity of the image in an image and as a guide to determine the authenticity of the image and make it easier to analyze the spread of information that can cause misunderstanding.

2. STUDY LITERATURE
2.1 Forensics Digital
Forensics (derived from the Latin forensis) can be interpreted

as "from the outside," which is a scientific process based on science in collecting, analyzing, and revealing useful evidence to be brought to trial related to legal cases. Forensic techniques for examining image files are called forensic photography techniques [9].

There are two digital forensics methods: static forensics and live forensics. The static forensic method uses conventional procedures and approaches, such as electronic evidence in a bit-by-bit image forensic process. This process is carried out when the system is not turned on. At the same time, the live forensic method is run when the machine must be in a state of power.

2.2 Digital Imagery

Digital image studies how an image is formed, processed, and analyzed to produce information humans can understand. For the discussion on images according to the preparation, there are two types: analog and digital. Digital image represents the light intensity function in discrete form in a two-dimensional plane. This image is organized based on a collection of pixels with coordinates (x, y) and amplitude f(x, y). Meanwhile, analog images result from analog image acquisition tools, such as the human eye and analog cameras [17].

2.3 Twitter

Twitter is a social media that is very widely used by the world. Twitter has different characteristics than other social media, one of which is a reasonably simple appearance and use that can attract much interest. Twitter is also used for political communication as a channel [18]. Using Twitter is believed to be a place that has higher news content than other social media.

2.4 Metadata

Metadata is structured information that describes, explains, locates, or at least makes information easy to rediscover, use or manage. Metadata is often called data about data or information about information [24].

2.5 Error Level Analysis (ELA)

Error level analysis (ELA) method is a technique to detect image manipulation by restoring the image at a certain quality level and then computing the difference between the compressed image and the previous image. When the image has no changes, the 8x8 pixel grid is potentially unchanged and remains the same. However, if the image has changed, the part that has been manipulated will have a higher error potential than the rest of the image. ELA works by resaving the image to determine the average error value [6].

In this analysis, several things need to be considered, such as the need to consider several things about the error rate experienced. Patterns belong to a collection of pixels whose image shape will be identical to the original image with the same features and colors. If the image has been modified, it will form a different edge pattern (less detail), and some colors may become lighter. A surface is an area or has the same area color. If the image is manipulated, the character will emit rainbow colors [13].

2.6 Noise Analysis

Noise Analysis is a method to detect photos against noise or detect image damage in photos. In the image engineering article, noise is generally a statistical variation of measurements made by random processes. In imaging, noise appears as an artifact in the grainy structure that covers the image [19].

2.7 Digital Evidence

According to one expert Eoghan Casey, digital evidence is data obtained from storage or sent directly by a computer to support theoretical evidence when an offense requires concrete or factual evidence. The data is a combination of numbers that present comprehensive information from file types such as text, images, video, or audio [20][21].

2.8 Forensics Tools

Forensic tools assist investigators in handling and collecting data related to the case to be investigated. Forensic tools must follow the need to accumulate facts and confirm if the digital facts are genuine to be accepted and also protect the honesty of information and avoid changing information or documents that make digital evidence unacceptable, the comparison of the use of forensic tools will also affect the digital facts obtained [22]. The tool used in this research is Forensicallybeta. Foresicallybeta is a tool that can detect web-based images, accessed via the link https://29a.ch/photo-forensics/#forensic-magnifier. In this tool, the user himself can detect photos starting from the Clone method, ELA, Noise, CPA, Metadata, and so on [3].

3. METHOD

The scenario created in this case is where the perpetrator has a motive for revenge against the victim by spreading hoax news using an image owned by the perpetrator and manipulating the picture, as simulated in Figure 1.

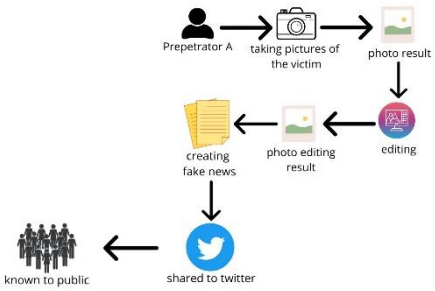


Figure 1. Case Scenario

After the perpetrator manipulates the image, the perpetrator creates fake news that makes the opinion even more, then spreads it via Twitter and spreads it until it is known to many people. The victim knew this information and reported this incident to the authorities until an investigation was carried out against the perpetrator.

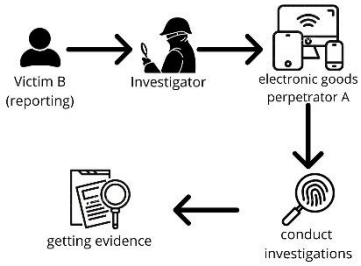


Figure 2. Case Investigation

Figure 2 explains the flow of the evidence retrieval process. Where investigators confiscate electronic items used by the perpetrator and data recovery is carried out. From the results of this recovery, evidence was found in the form of original photos in it and the results of images that had been manipulated. Furthermore, the research stage is carried out for further identification. These stages can be seen in Figure 3.

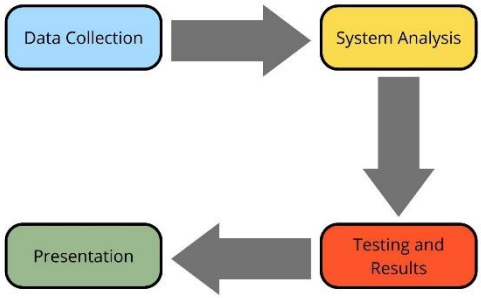


Figure 3. Schematic of Method

The stage carried out is data collection by collecting JPEG files by taking 4 sample images. Files in the form of two original photos and two that have been manipulated. The second is system analysis to determine what methods/tools will be used in this research. The tools used are Forensicallybeta and include the methods applied, namely Error Level Analysis and Noise Analysis. Next is the testing stage of the images selected into the tools/methods used. The last is the analysis and presentation of the results, where the results that have been obtained will be analyzed and compared, and the evidence that has been found.

4. RESULTS AND DISCUSSION

The next is Results and Discussion. This process reviews the results of analyzing the necessary information. Includes a data collection session, where the information on the data is collected in the form of images owned by the perpetrator. After that, testing and analysis will be conducted to find comparisons of original and manipulated photos until they are finally presented.

4.1 Data Collection

The first thing to do is to collect data. The data obtained is in the form of image files in JPEG format, which should take 4 photo illustrations of different types. Files in the form of 2 original photos and two manipulated photos come from the computer device owned by the perpetrator. The photo is tried to be manipulated into a splicing image and a copy-move image.

Table 1. Scenario Image

Original Image  a	Copy-move Image  b
Original Image  c	Splicing Image  d

Original Image  e	Copy-move Image  f
Original Image  g	Retouching Image  h

4.2 System Analysis

This stage is a process of planning the software that will be used in the research. This system analysis is needed for the smooth running of the research process, including identifying tools used to obtain valid results. Table 2 lists the tools used in this research, along with a description of each tool.

Table 2. Tools and Usability

Tools	Usability
ForensicallyBeta	Detect photos by checking techniques with ELA, Noise Analysis, and Metadata methods.

4.3 Testing and Results

This is the stage where the evidence that has been collected will be tested on the system that has been determined. Steps will be taken through a unique identification process of digital evidence and identification of data sources. This research also uses digital evidence in the form of available images, which are then processed with Forensicallybeta tools. Then see, the difference in the image will be compared.

4.3.1 Metadata

The first analysis stage is to analyze the findings by checking the metadata. Metadata is information about data. Metadata contains various information about the data from a data file need to realize. The original image uploaded to the Forensicallybeta tool will use the Metadata Analysis method. This process is used to identify differences in the file so that it can get between the original photo and the manipulated photo. In the modified results, Figure 4 is the finding of the results of Forensicallybeta.

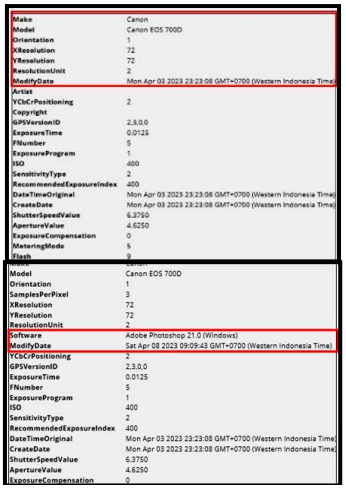


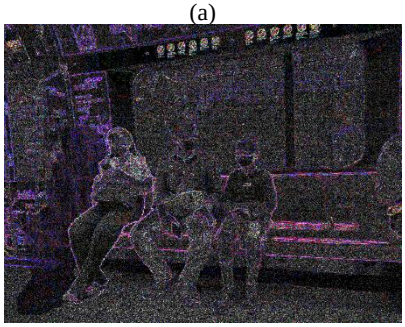
Figure 4. Metadata (1)

Figure 4 displays the Metadata of the original and manipulated photos. The manipulated photo below shows changes in Metadata, especially the appearance of the line "Software", "Adobe Photoshop 21.0 (Windows)" as in the red box, therefore it can be confirmed that both photos are manipulated. While the original photo does not show the line, therefore both photos are original photos.

4.3.2 Error Level Analysis (ELA)

Next is to analyze the Error Level Analysis method. Where this method is to identify parts of an image with different levels of compression, this technique can determine whether an image has been digitally modified. ELA can show that the image has gone through the editing stage with Photoshop software. The difference can be seen in the image below.

(a)

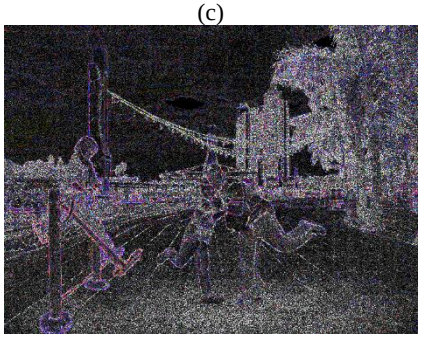


(b)

Figure 5. ELA Comparison 1

It is known that the result in Figure 5 is a comparison image of the original image and the image that has undergone copy-move. The color distribution in image (a) looks even and unified, or there are no suspicious objects because the digital image has not been modified. As for image (b), Error Level Analysis shows significant changes. Where the image turns brighter, there is a mismatch between the image and the color of the original image, there are shadows of objects that are the result of manipulation which indicates that the image has been modified.

(c)



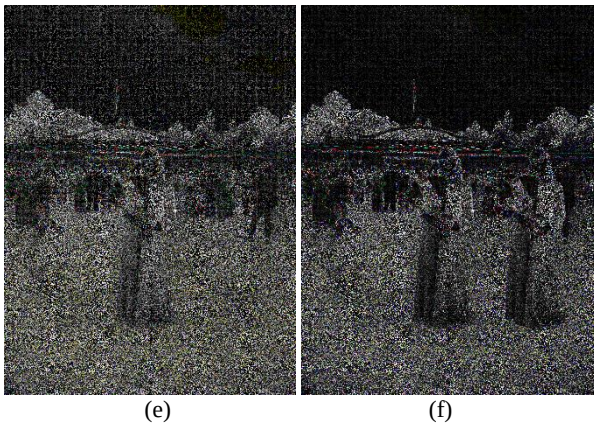
(d)

Figure 6. ELA Comparison 2

Figure 6 is the second ELA comparison. Error Level Analysis gets a difference when the bottom image has a fainter color, and the area where splicing occurs has a color error that is visible compared to its surroundings. So it can be concluded that the image has been compressed.

4.3.3 Noise Analysis

The next step is to analyze the Noise Analysis method. This method is more directed with the term looking for disturbances in the image made. The noise is a point in the image that is not part of the image but is mixed in the picture for some reason [23]. Usually, Noise is used to damage the image in the photo, but in this research, Noise is useful in finding an image error to determine whether the image is modified.



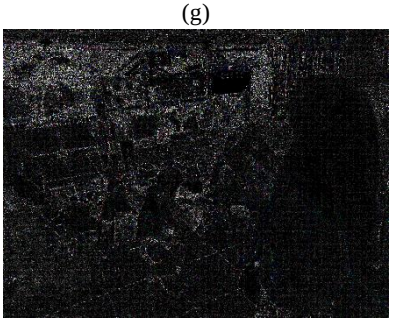
(e) (f)

Figure 7. Noise Comparison 1

It is known that the results in Figure 7 are a comparison image of the original image on the left and the image that has undergone copy-move. the distribution of noise in the original image in the image is still evenly distributed, looks unified or there is no suspicious object because the digital image has not undergone any modification. As for the part of the image that

has been copy-moved, Noise Analysis at first glance does not show any significant changes, but the change in the number of points and colors is getting darker. Noise changes can also be seen where for the manipulation image more visible error lines, which indicates the image has been modified.

(g)



(h)

Figure 8. Noise Comparison 2

Likewise in the next experiment with the second material. Where in Figure 8 it can be seen that the distribution of the Noise Analysis image is still evenly distributed and appears to be unified on all objects in the image because there has been no image modification. There is no sign of suspicious objects in the image. When switching to the bottom image at first glance there is no significant change, but if we zoom in and count all the pixels in the image then there is a change between the two. If the one that has been manipulated is a little dimmer and the noise is a little faint compared to the original image. The photo has certainly undergone image retouching modification.

4.4 Presentation

Next is the Validation of Results in image authenticity detection research using the Error Level Analysis and Noise Analysis methods in Table 6 below.

Table 6. Validation of Results

Image Detect	**ELA**	**Image Detect**	**Noise**
Original Image	- Original image with Forensicallybeta - Set JPEG Quality 90 - Error Scale 40 (the higher the level of authenticity, the clearer it is). - Opacity 0.95 (To make the image transparent, if the opacity is low then the error scale cannot be seen)	**Original Image**	- Setting on Noise Amplitude 40 (using the middle amplitude value because if it is too small, you cannot see the error, if it is too big, there will be more noise and it is difficult to detect the error) - Turn off the Equalize Histogram checkbox to reduce image noise. - Opacity 0.78 (the higher the opacity)
Fake Image	- Settings in the Forensicallybeta tool are the same as in the original image - The results of the image are detected to be manipulated, namely, the image looks darker and the error in the color is getting clearer.	**Fake Image**	- The settings in the Forensicallybeta tool are the same as in the original image. - The results of the manipulated image can be seen with clear colorful lines around the noise, and the image will be dimmer.

The analysis stage shows that the features of the Forensicallybeta tool can detect the difference between the original photo and the manipulated photo with image combination image disturbance and compression differences in the image. This is proven by detection using the ELA and Noise Analysis methods. The following are the results of image authenticity detection research using the Error Level Analysis and Noise Analysis methods in Table 4.7 as follows:

Table 7. ELA and Noise Results

Image Detection	ELA	Noise
Image (a) and (b)	Detected	Detected
Image (c) and (d)	Detected	Detected
Image (e) and (f)	Detected	Detected
Image (g) and (h)	Detected	Detected

5. CONCLUSIONS

Error Level Analysis and Noise Analysis method techniques can be used to detect image authenticity using the ForensicallyBeta tool. Together with other methods such as Metadata and RGB Histogram to see the difference between the original image and the manipulated image. The comparison of methods can produce an analysis that proves the difference between the original photo and the manipulated photo with perfect detection accuracy. The more changes occur in the image, the more ELA will bring up color errors and Noise will further reduce the spots in the photo. It is expected that the results of further research can be developed using other forensic tools and other forensic methods. It is also possible to develop systems/tools and application of other techniques, where the image detection and calculation are much more accurate. With this research, it can also support the detection of image authenticity to determine the original image and the image that has been modified.

6. REFERENCES

[1] A. Apriliani, K. Hijjayanti, and Suhairoh, "Image Authenticity Analysis Using Exif Metadata," vol. 5, no. 1, pp. 84-85, 2020, doi: 10.24114/ cess.v5i1.15600.

[2] W.Y. Sulistyo, I. Riadi, and A. Yudhana, "Analysis of Image Authenticity Detection Using Error Level Analysis with Forensicallybeta," vol. 1, no. 1, pp. 154, 2018.

[3] T.R. Hidayat, "Web-based Photo Forensics Application", 1st ed, STIMIK AKAKOM, Yogyakarta, 2017.

[4] Irwansyah, H. Yudiastuti, "Digital Forensic Analysis of Engineering Images Using JPEGSNOOP and Forensicallybeta", vol. 21, no. 1, pp. 55-59, 2019, doi:10.33557/jurnalmatrik.v21i1.518.

[5] A.Y. Wijaya, " Development of Block Matching Method for Copy Move Detection in Image Forgery," JUTI: Jurnal Ilmiah Teknologi Informasi, vol.15, no. 1, pp. 84-94, 2017, doi: 10.12962/j24068535.v15i1.a638.

[6] B. Darmawan, A. Sasmitha, and P.W. Buana, "Development of Image Modification Detection Method Using Error Level Analysis Method," vol. 7, no. 1, pp. 29-35, 2019, doi:10.24843/JIM.2019.v07.i01.p04.

[7] M. Subli, M.M. Efendi, "Comparison of Hoax Photo Analysis Results Using the Exif/Metadata Method," 1st ed, Widina Bhakti Persada Bandung, 2021, Bab 1, pp. 1-3.

[8] M.R. Al-Fajri, Carudin, and D. Yusup, "Forensic Image Analysis in Detecting Image File Engineering with the NIST Method", vol. 6, no. 2, pp.84-90, 2021, doi: 10.32528/justindo.v6i2.5120.

[9] D.A. Faroek, R. Umar and I. Riadi, "Image Authenticity Detection Using Error Level Analysis (ELA) and Principal Component Analysis (CPA)," vol. 8, no. 2, pp. 132-137, 2019, doi: 10.22441/format.2019.v8.i2.006.

[10] Y.M. Djaksana, A.K. Rivai, and D. Supriyadi, "Analysis of Image Manipulation (ImageForgery) Using the Integration of Error Level Analysis and Block Matching Methods," vol. 12, no. 1, pp. 79-84, 2018.

[11] F. Harahap, "Photo Manipulation Detection with Forensicallybeta and Imageforensic.org Tools with Error Level Analysis (ELA) Method," vol. 2, no. 3, pp. 159-164, 2021.

[12] C. Juditha, "Hoax Communication Interactivity in Social Media and Anticipation", vol. 3, no. 1, pp. 31-44, 2018, doi: 10.30818/jpkm.2018.2030104.

[13] A.S. Primastuti, "Developing of Image Detection System with JPG Format using Error Level Analysis Technique," vol. 184, no. 2, pp. 41-47, 2022, doi: 10.5120/ijca2022921977.

[14] A.Wicaksono, N. Mardiyantoro, and H. Sibyan, "Application of Error Level Analysis Method to Detect Digital Image Modification," vol. 1, no. 1, pp. 62-69, 2022.

[15] RN. Pambayun, "Analysis of Trim Features on Solid State Drives for Digital Forensics Cases," 1st ed, Muhammadiyah Purwokerto University, 2018.

[16] X. Zhao, J. Li, S. Li, and S. Wang, "Detecting digital citra splicing in chroma spaces," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6526 LNCS, pp. 12-22, 2011.

[17] P. N. Andono, T. Sutojo and Muljono, "Digital Image Processing", Yogyakarta: Penerbit Andi, 2017.

[18] F. Z. Emeraldien, R. J. Sunarsono and R. Alit, "Twitter as a Political Communication Platform in Indonesia," SCAN Jurnal Teknologi Informasi dan Komunikasi, vol. 14, no. 1, pp. 21-30, 2019.

[19] "Image Engineering," [Online]. Available: https://www.image-engineering.de/library/image-quality/factors/1080-noise. [Accessed 2022].

[20] "LMS SPADA INDONESIA," Kemendikbud, 2021. [Online]. Available: https://lmsspada.kemdikbud.go.id/mod/page/view.php?id=57362. [Accessed 2022].

[21] "National Institute of Justice (NIJ)," U.S Department of Justice, [Online]. Available: https://nij.ojp.gov/digital-evidence-and-forensics. [Accessed 2022].

[22] Sunardi, I. Riadi and I. M. Nasrulloh, " Solid State Drive (SSD) Forensic Analysis Using the GRR Rapid Response Framework," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 6, no. 5, pp. 509-518, 2019.

[23] W. T. Handoko, E. Ardhianto and E. Safriliyanto, "Analisis Dan Implementasi Image Denoising dengan Metode Normal Shrink sebagai Wavelet Thresholding Analysis," Jurnal Teknologi Informasi DINAMIK, vol. 16, no. 1, pp. 56-63, 2011.

[24] G. H. A. Kusuma and I. N. Prawiranegara, "Digital Forensic Analysis of CCTV Video Recordings Using Metadata and Hash," Prosiding Seminar Nasional Sisfotek (Sistem Informasi dan Teknologi Informasi), vol. 3, no. 1, pp. 223-227, 2019

[25] S. Ratna, " Digital Image Processing and Histogram with Phyton and Text Editor Phycharm," Jurnal Ilmiah "Technologia," vol. 11, no. 3, pp. 181-186, 2020.