International Journal of Cyber-Security and Digital Forensics (IJCSDF) 11(2): 34-39
The Society of Digital Information and Wireless Communications (SDIWC), 2022 ISSN: 2305

Analysis of Digital Document Engineering Forensic with NIJ

[1*]Arizona Firdonsyah and [2]Danur Wijayanto
[1,2]Department of Information Technology, Universitas 'Aisyiyah Yogyakarta
Jalan Siliwangi 63, 55133, Yogyakarta, Indonesia
[1*]arizona@unisayogya.ac.id, [2]danurwijayanto@unisayogya.ac.id

ABSTRACT

Digital forensics can assist in digitally collecting evidence to be presented in court in accordance with applicable law. One example of digital forensic science is image forensics, which aims to collect and look for evidentiary facts in determining the authenticity of an image. Various criminal and pornographic cases involving image files often occur, therefore image forensics is an important key item to assist the court in making decisions. This research examines the authenticity of digital documents using the National Institute of Justice (NIJ) method by applying the forensic ELA (Error Level Analysis) method. Several previous studies have proven that the forensic ELA method can detect modifications that have been made to images. Differences with previous studies, in this study the authors also checked the metadata of the images before performing the ELA examination using photoforensic software. The results of the analysis show a high level of inconsistency in images and writing because there are many white dots in several places such as the letterhead logo, letterhead writing, text content, footnotes, and initials below the right.

KEYWORDS

Forensics, Documents, Image, NIST (National Institute of Standard and Technology), ELA (Error Level Analysis), Fotoforensics

1 INTRODUCTION

The development of advanced digital image manipulation technology makes it easy to change or modify photos so that image forgery is increasingly prevalent [1]. Improved image manipulation techniques make it difficult for viewers to distinguish between real photos and manipulations [2]. Image manipulation activities are often carried out before the image is published. Image manipulation has a purpose such as fixing the background and manipulating certain parts [3]. Besides that, it can also be used for negative things such as insinuating or dropping other people influence other people, and spreading hoax news [4].

Technological advances in the fields of information, communication and media have changed people's mindset and behavior. This causes significant cultural, economic and social changes. Today's information technology can be said to be a double-edged sword, because apart from being able to have a negative impact, it can also have a positive impact. Various crimes that use information technology and the internet as a medium are called cybercrime.

Digital forensics can assist in digitally collecting evidence to be presented in a trial in accordance with applicable law. One example of the field of digital forensics is image forensics which aims to collect and look for evidentiary facts in determining the authenticity of an image [5]. Various criminal and pornographic cases involving image files are still common, therefore forensics on images as evidence is an important key to assist the court in making decisions..

This research will test the authenticity of digital letters documents using the National Institute of Justice (NIJ) method by applying the forensic ELA (Error Level Analysis) method. Several previous studies have proven that the forensic ELA method can detect modifications that have been made to images. Differences with previous research, our research also checked the metadata of the images before performing the ELA examination using photoforensics software.

2 RELATED WORKS

Research conducted by [6] discusses image manipulation software which allows inexperienced users to modify digital images in an easy way. The researcher also concludes that techniques in image forgery are getting more sophisticated so we need used sophisticated and complicated methods to detect image forgery. Based on research conducted by Hasan et al.,

Román et al., and Firdonsyah, it shows that in conducting computer forensics investigations such as image falsification, several software and hardware tools can be used [7]–[9].

Another study related to images was carried out by Harahap and Sulistyo et al.. Harahap researched Fotoforensics and concluded that the features of www.fotoforensics.com can be used as an accurate detection of the authenticity of images. The facilities provided from fotoforensics.com can be used and are very efficient in detecting the authenticity of photos, especially in the ELA (Error Level Analysis) feature. This study only shows the part of the photo that has been manipulated by displaying differences and comparing the color gradients in the original and manipulated photos [10].

While the research conducted by Sulistyo et al. detect the authenticity of the image using the ELA method and Principal Component Analysis (PCA) using the Forensicallybeta tool. By using the method used, the author succeeded in detecting the authenticity of the image based on its color components. The manipulated image has a much sharper color contrast when compared to the original image which applies to the ELA and PCA methods [11].

Subsequent research was conducted by Irwansyah & Yudiastuti [12] who used the ELA method as well as Forensically Beta tools for Image splicing, Copy-Move and Retouching Images, which showed that they could detect differences in the two image objects studied. In addition, forensic image analysis using the JPEGSnoop application displays clear results on the differences between the original image and the manipulatd image.

Research conducted by Arizona [9] and Roni Anggara [13], examined mobile forensics using the NIJ method. This research shows that using the NIJ method, can help analyze and obtain information from digital evidence

3 METHODOLOGY, TOOLS, AND PARAMETERS

3.1 Research Methodology

The method used in this research is a framework National Institute of Justice (NIJ).The stages of the NIJmethod can be seen in Figure 1.

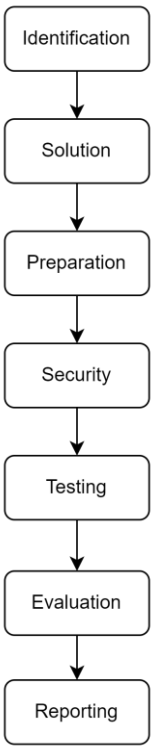


Figure 1. NIJ Scheme

The explanation of the stages of the NIJ method is as follows:

1. **Identification**, problem identification by collecting information on physical evidence and identifying the problems encountered.
2. **Solution**, is a solution to the problems faced and related to the selection of forensic software to obtain digital evidence.
3. **Preparation**, the process of preparing the physical evidence, equipment and software needed for forensic analysis.
4. **Security**, it is the process of maintaining the integrity of physical evidence by making replicas of physical evidence.
5. **Testing**, testing of physical evidence and forensic software is carried out. Testing can be done by logical extraction (digital proof extraction from physical image proof file) and physical extraction (digital proof extraction from direct physical evidence)
6. **Evaluation**, evaluation of the process and test results. Evaluation is done by

comparing the extraction results from each forensic software

7. **Reporting**, presenting the final results of the forensic process.

3.2 Research Tools and Parameters

We are used Forensic Tools for this research as described on Table 1. Our research using three tools : Foxit PDF for PDF Reader, Metadata2Go for metadata reader, and FotoForensics for ELA analysis .

Table 1. Forensics Tools

No	Forensic Tools	Description
1	Foxit PDF	PDR Reader that can be used to physical observation on PDF Files.
2	Metadata2Go	free online tool that allows access the hidden exif & meta data of files
3	FotoForensics	Tools for digital picture analysis, including error level analysis

conducting the examination. In the research conducted, analyzes such as [14]:

i. Checks the metadata of the file to be authenticated. This metadata analysis was carried out at the beginning to find out the details of the source file. The points observed are MAC (Modification Time, Access Time, and Creation Time).
ii. Conduct physical observations and conduct an initial assessment of findings of irregularities in the letter section.
iii. Performs an ELA to see if there is any digital manipulation in the file.

Table 2. Possible Solutions

No	Possible Solution
1	Installing forensic softwares
2	Creating cloning of file wich used for physical evidence to preserve contained digital evidences
3	Conducting metadata extraction of digital evidences. Analisa metadata ini dilakukan di awal untuk mengetahui detail sumber file. Poin yang diamati adalah MAC (Modification Time, Access Time, and Creation Time)
4	Manual examination untuk penilaian awal temuan kejanggalan pada bagian surat
5	Analyse using Error Level Analysis untuk mengetahui apakah ada manipulasi digital di dalam file
6	Make report based on Solution

4 RESULT and DISCUSSION

4.1 Identification

Identification stage is the process of searching and documenting physical evidence and identifying the encountered problems so that forensic investigator is able to determine which solution that can be done [9].

4.2 Solution

After identification phase, we mapping and searching for possible solution. Possible solution described at Table 2 and described as flowchart at Figure 2. This solitions is carried out to examine the results of the examination process using technically and legally justified methods in order to obtain information that can be used to answer questions that are the driving force for

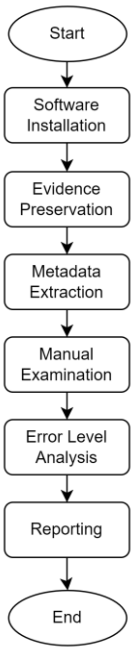


Figure 2. Possible Solutions

4.3 Preparation and Security

The preparation process is the implementation of the planned solution. The preparation stage can be carried out simultaneously or separately with security [7]. The steps taken are:

4.3.1. Installation of Forensic Software

The first process that is carried out is to install forensic software which is used to examine forensic evidence. From the forensics tools shown in Table 1, Foxit PDF was installed which was used for manual examinations.

4.3.2 Securing Physical Evidence's Integrity

Securing physical evidence is necessary to ensure the integrity of digital evidence contained in the physical evidence. This step can be done by isolating physical evidence and making backups in the form of cloning or image files of the physical evidence

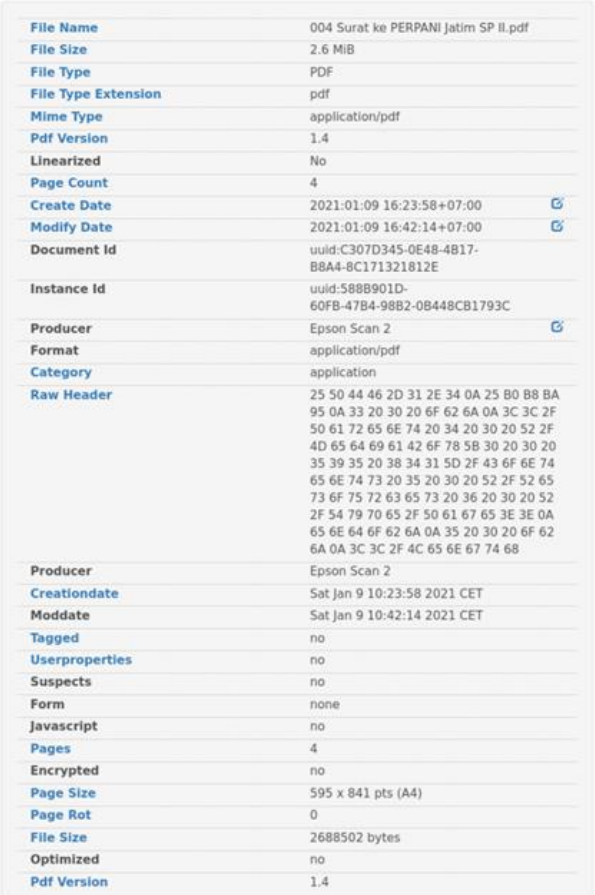
4.4 Testing and Evaluation

Testing process conducted by doing experiment of extracting metadata, manual examination, and Error Level Analysis. Steps of extracting metadata and Error Level Analysis carried out by separating and making soft copies of the evidence in pdf format and the analysis is carried out using soft copies of the evidence so that the integrity of the evidence is maintained and can be reused if needed.

4.4.1. Metadata Extraction

Metadata analysis was carried out to find out the details of the source file, especially MAC (Modification Time, Access Time, and Creation Time). metadata check results is shown in Figure 3.

From the results of the metadata examination shown in Figure 3, there are parts that need to be observed which are shown in Table 3.



File Name	004 Surat ke PERPANI Jatim SP II.pdf
File Size	2.6 MiB
File Type	PDF
File Type Extension	pdf
Mime Type	application/pdf
Pdf Version	1.4
Linearized	No
Page Count	4
Create Date	2021:01:09 16:23:58+07:00
Modify Date	2021:01:09 16:42:14+07:00
Document Id	uuid:C307D345-0E48-4B17-B8A4-8C171321812E
Instance Id	uuid:588B901D-60FB-47B4-98B2-0B448CB1793C
Producer	Epson Scan 2
Format	application/pdf
Category	application
Raw Header	25 50 44 46 2D 31 2E 34 0A 25 B0 B8 BA 95 0A 33 20 30 20 6F 62 6A 0A 3C 3C 2F 50 61 72 65 6E 74 20 34 20 30 20 52 2F 4D 65 64 69 61 42 6F 78 5B 30 20 30 20 35 39 35 20 38 34 31 5D 2F 43 6F 6E 74 65 6E 74 73 20 35 20 30 20 52 2F 52 65 73 6F 75 72 63 65 73 20 36 20 30 20 52 2F 54 79 70 65 2F 50 61 67 65 3E 3E 0A 65 6E 64 6F 62 6A 0A 35 20 30 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68
Producer	Epson Scan 2
Creationdate	Sat Jan 9 10:23:58 2021 CET
Moddate	Sat Jan 9 10:42:14 2021 CET
Tagged	no
Userproperties	no
Suspects	no
Form	none
Javascript	no
Pages	4
Encrypted	no
Page Size	595 x 841 pts (A4)
Page Rot	0
File Size	2688502 bytes
Optimized	no
Pdf Version	1.4

Figure 3. Metadata

Table 3. Important Metadata

Create Date	9 Januari 2021 16:23:58+07:00
Modify Date	9 Januari 2021 16:42:14+07:00
Producer	Epson Scan

Based on the metadata in Figure 3 and Table 3, the corresponding file was created on January 9, 2021 at 16:23:58 GMT (Greenwich Mean Time) and the last edit was on January 9, 2021 at 16:23:58 GMT and can be assumed to be the result scans from Epson printers.

4.4.2.Physical Observation

This process is carried out an initial assessment if irregularities are found. The results of physical observations are shown in Table 4. at this stage there are anomalies in the signature where the owner of the signature is not known and there is an oddity in the stamp that is not interrupted by the color of the signature

Table 4. Physical Observation Result

Early Findings	Finding Object
There is a signature on the letter that is not known to the owner of the signature and it is possible for the signature to be the result of electronic duplication instead of a direct signature.	Signature
There is an affixing of a signature on a letter that is not known to the owner of the signature, there are signatures and signatures that are made possible by electronic duplicating results not from direct signatures. The stamp color is blue or a bright color, but on the display it can be seen that the stamp color overlaps and is not interrupted by the black and darker signature color. signature	Signature

Figure 4. First Page

4.3.3. Error Level Analysis

The analyzed file has 3 pages which are all analyzed to find out if there is any digital manipulation within the pages. The first page is shown in Figure 4, the second page is shown in Figure 5 and the third page is shown in Figure 6.
The first page shows a high level of inconsistency in images and text. We can see a lot of accumulation of white dots in the following places: the writing on the letterhead, the letterhead logo on the right, the text of the letter, the writing and stamp on the signature, the initials on the bottom right, and the writing below the letter. This buildup of white dots indicates digital manipulation was performed on the file.
The same thing is seen on the second and third pages which show a high level of inconsistency in images and writing. You can see a lot of white dots piled up in the following places: all letterhead logos, letterhead writings, text contents, letterheads, and initials below right. This buildup of white dots indicates digital manipulation was performed on the file.

Figure 5. Second Page

Figure 6. Third Page

4.5 Reporting

Based on the forensic analysis that has been carried out in the study, the letters are suspected to have been manipulated based on processes and techniques, including physical examinations and observations carried out using Foxit PDF software, metadata examination and observation with metadata2go software and Error Level Analysis examination using photoforensics software.

5 CONCLUSION and FUTURE WORK

The results show that using the National Institute of Justice (NIJ) and Error Level Analysis (ELA) methods can be used to prove the authenticity of images or images. The results of the analysis show a high level of inconsistency in the images and writings due to the accumulation of white dots in several places such as letterhead logos, letterhead writings, text contents, footnotes, and initials below the right. Further research can be developed by making comparisons with other forensics tools like exiftool, or PDFMtEd

REFERENCES

[1] F. Mahardika, A. D. Khatulistian, and A. P. Kuncoro, “Review Foto Forensic.com dengan Teknik Error Level Analysis dan JPEG untuk mengetahui Citra Asli,” *J. Inform.*, p. 5, 2018.

[2] A. Y. Wijaya, S. A. Musayyab, and H. Studiawan, “PENGEMBANGAN METODE BLOCK MATCHING UNTUK DETEKSI COPY-MOVE PADA PEMALSUAN CITRA,” *JUTI J. Ilm. Teknol. Inf.*, vol. 15, no. 1, p. 84, Jan. 2017, doi: 10.12962/j24068535.v15i1.a638.

[3] I. Riadi, A. Fadlil, and T. Sari, “Image Forensic for detecting Splicing Image with Distance Function,” *Int. J. Comput. Appl.*, vol. 169, no. 5, pp. 6–10, Jul. 2017, doi: 10.5120/ijca2017914729.

[4] C. Iakovidou, M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, “Content-aware detection of JPEG grid inconsistencies for intuitive image forensics,” *J. Vis. Commun. Image Represent.*, vol. 54, pp. 155–170, Jul. 2018, doi: 10.1016/j.jvcir.2018.05.011.

[5] R. Umar, A. Fadlil, and A. I. Putra, “Analisis Forensics Untuk Mendeteksi Pemalsuan Video,” *J-SAKTI J. Sains Komput. Dan Inform.*, vol. 3, no. 2, p. 193, Sep. 2019, doi: 10.30645/j-sakti.v3i2.140.

[6] V. P. Nampoothiri and N. Sugitha, “Digital image forgery — A threaten to digital forensics,” in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, India, Mar. 2016, pp. 1–6. doi: 10.1109/ICCPCT.2016.7530370.

[7] R. Hasan, S. Mahmood, and A. Raghav, “Overview on Computer Forensics tools,” in *Proceedings of 2012 UKACC International Conference on Control*, Cardiff, United Kingdom, Sep. 2012, pp. 400–403. doi: 10.1109/CONTROL.2012.6334663.

[8] R. F. M. Román, N. M. L. Mora, J. P. N. Vicuña, and J. I. P. Orozco, “Digital Forensics Tools,” *Int. J. Appl. Eng. Res.*, vol. 11, no. 19, 2016.

[9] A. Firdonsyah, “Comparative Analysis of Forensic Softwares for Android-based Blackberry Messenger Using NIJ Framework and NIST Measurements,” *Int. J. Cyber-Secur. Digit. Forensics IJCSDF*, vol. 10, no. 2, pp. 78–90, 2021.

[10] F. Harahap, “Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic.org Dengan Metode Error Level Analysis (ELA),” vol. 2, no. 3, p. 6, 2021.

[11] W. Y. Sulistyo, I. Riadi, and A. Yudhana, “Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital,” *JUITA J. Inform.*, vol. 8, no. 2, p. 179, Nov. 2020, doi: 10.30595/juita.v8i2.6602.

[12] I. Irwansyah and H. Yudiastuti, “ANALISIS DIGITAL FORENSIK REKAYASA IMAGE MENGGUNAKAN JPEGSNOOP DAN FORENSICALLY BETA,” *J. Ilm. Matrik*, vol. 21, no. 1, pp. 54–63, Jul. 2019, doi: 10.33557/jurnalmatrik.v21i1.518.

[13] R. Anggara Putra, A. Fadlil, and I. RIadi, “638-1520-1-PB.pdf,” *J. Rekayasa Teknol. Inf. JURTI*, vol. 1, no. 1, 2017.

[14] D. T. Yuwono and S. Juhairiah, “ANALISIS FILE CARVING PADA FILE SYSTEM DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST),” Politeknik Negeri Banjarmasin, 2019, p. 8.