Infact: Computer International Journal (ICIJ)
Vol.9, No.02, September 2022
p-ISSN : 2527-8363, e-ISSN: 2829-0259
DOI:

Forensic Metadata Analysis in Detecting Digital Image Manipulation

Mario Anugraha[1], Ryan Putranda Kristianto[2], Andre Hartanto[3]
[1, 2,3]Ilmu Informatika, Universitas Katolik Darma Cendika
[1,2,3]Jl. Dr. Ir. H. Soekarno No.201, Klampis Ngasem, Kec. Sukolilo, Surabaya, Jawa Timur
E-mail: mario.anugraha@student.ukdc.ac.id[1], ryan@ukdc.ac.id[2], andre.hartanto@ukdc.ac.id[3]

Submitted: 06/05/2025 , Revision: 06/20/2025, Accepted : 07/31/2025

Abstract

The development of the digital era has brought significant changes to various aspects of life, including the field of photography. Digital photos offer both advantages and disadvantages, one of which is the ease with which they can be modified using image editing software. This makes it increasingly difficult to distinguish between original and manipulated images. Edited photos can spread widely through social media, causing public concern and doubts about the authenticity of information. Individuals often manipulate images for personal gain or interests. The easy access to image editing software further facilitates this manipulation process. In the field of research, digital image forensics has emerged as a scientific method to verify the authenticity of images through accountable evidence. This study aims to detect forgery in digital photos using that approach. The method employed in this research is metadata analysis with the assistance of an offline tool called JPEGsnoop and online tool Forensically Beta. The results show differences in metadata between the original and manipulated images, indicating that modifications have been made to the image.

Keywords:
Digital image forensics;
Metadata;
Digital Photo;

***Corresponding Author: Author's Name**
E-mail: corresponding_email@email.com

1. Introduction

The rapid development of the times has brought many changes in our lives, including in the world of photography. Digital photos have now become an important part of everyday life, with various advantages they offer [1]. However, behind that, there is also another side that needs attention. One of them is the ease of editing or manipulating images using various photo editing applications. The edited results often look very convincing, making it difficult to distinguish them from the original photos. The forms of manipulation vary, ranging from cropping images [2], adjusting lighting, adding backgrounds, to changing certain elements in the photo. The increasingly sophisticated manipulation techniques pose a challenge in distinguishing which images are authentic and which have been modified [3].

Digital Forensics is an investigative process carried out in an effort to uncover criminal cases in cyberspace [4]. Digital forensics is a branch of science that studies ways of handling crimes related to the use of computer technology. Efforts are needed to uncover crimes that occur in the digital realm. The forensic investigation process on computers or similar devices can be carried out using two digital evidence acquisition methods, namely live forensics and static forensics. In its implementation, digital forensic processes can adopt one of the available frameworks and several standards commonly used in the forensic process, one of which is the National Institute of Standards and Technology (NIST) [5]. This technique is applied to analyze computer systems statically, that is, without changing the contents of the system, and usually focuses on data stored in non-volatile storage media. The static forensics approach is very effective in uncovering digital traces, digital artifacts, and patterns of technology-based crimes with the support of computer systems. The process of tracking these digital traces can be carried out through digital data acquisition techniques by utilizing specific forensic applications or software [6].

Previous research that became the reference for this study was conducted by [7], showing that metadata in digital images can provide important information to distinguish between original and manipulated photos. In that study, an analysis was conducted on two images and their edited results using the offline tool Metadata++. The results revealed differences in metadata such as the software used and the modification date, which became indicators that the image had been engineered. This study serves as an important foundation that metadata can be utilized as digital evidence in uncovering image manipulation.

This study focuses on metadata analysis of two similar images used as evidence in a case study of manipulation by certain individuals. The analysis process is carried out using the NIST (National Institute of Standards and Technology) method, which is a standard in digital forensic procedures [8]. To support this analysis process, the researcher uses offline tools such as JPEGsnoop and online tools like Forensically Beta as supporting tools in examining metadata from images or digital photos that are the object of research. JPEGsnoop and Forensically Beta are used in this study to help reveal the authenticity of an image that is used as evidence. JPEGsnoop is capable of providing a fairly in-depth analysis of images, including information about whether the image has undergone manipulation or not [9]. In addition, JPEGsnoop also has a simple interface and is relatively easy to use, making it easier to identify metadata and compression characteristics of the analyzed image [10]. Forensically Beta is a free tool that can be used to perform forensic analysis on image or photo files. This tool functions like a magnifying glass, helping users observe fine details in an image or photo [11].

This study applies the method from the National Institute of Standards and Technology (NIST), which is designed to describe the steps and workflow of the research in a structured and systematic manner. This method serves as a guide in solving the problems studied, especially in the context of digital forensic analysis of images. The NIST approach consists of several main stages, namely Collection, Examination, Analysis, and Reporting [12]. In this study, the method is used to recognize and analyze changes that occur in metadata due to the digital engineering process on images used as evidence. It also aims to evaluate the effectiveness of metadata in detecting digital manipulation of images, and to examine the extent to which metadata can provide accurate and consistent indications of digital tampering. By analyzing metadata on digitally engineered images, this research is expected to make a significant contribution in the field of digital forensics, particularly in efforts to enhance the integrity and validity of digital evidence used in judicial processes.

2. Methods

In this study, the research methodology follows guidelines based on the provisions and requirements of the Indonesian National Standard (SNI) 27037:2014. Several previous studies have also adopted acquisition procedures in accordance with this standard, integrating investigative methods from the National Institute of Standards and Technology (NIST) [13]. The following are the stages of analysis based on the NIST method:

Figure 1. Digital Forensic Analysis Flowchart

Figure 1 illustrates the flowchart of digital forensic analysis, which consists of the following four stages [13]:

Collection This stage involves the process of gathering information through various activities aimed at acquiring data that can support the investigation in uncovering evidence of digital crimes. During this phase, data is collected from relevant sources while ensuring the integrity and authenticity of the evidence is preserved without any modification.

Examination In this phase, the collected digital data undergoes in-depth examination. This includes analyzing metadata, file structures, and other essential elements. The objective is to gain a comprehensive understanding of the content and characteristics of the digital evidence and to identify any indications related to the case under investigation.

Analysis The analysis phase involves the processing and interpretation of the previously collected data. Digital forensic experts employ appropriate analytical methods and tools to uncover hidden or deleted information, recognize specific patterns, and correlate digital evidence with actual events. This step aims to reconstruct the chronology of events and reinforce the basis for drawing accountable conclusions.

Reporting At this stage, a report is prepared detailing the results of the analysis. It includes a description of the procedures undertaken, such as analysis based on the NIST methodology. The report also outlines the tools and techniques used, and provides recommendations for improving policies, procedures, tools, and other aspects related to the digital forensic process.

3. Results and Discussion

3.1 *Collection*

In this initial stage, a data collection process is carried out to obtain evidence used for identification purposes. The digital evidence collected consists of two digital images. The aim of this analysis is to reveal differences in digital information that may indicate manipulation or content modification. The following section presents the digital evidence in the form of images or photographs that serve as the objects of analysis in this study.

Figure 2. The first photograph

Figure 3. The second photograph

Figure 2 represents a digital image in its original condition, which will be analyzed through its metadata to assess its level of authenticity. Meanwhile, Figure 3 is an image that will be subjected to metadata analysis to identify any indications of alteration or digital manipulation.

3.2 *Examination*

In this second stage, an examination is conducted on the two digital images previously collected as evidence. The examination focuses on metadata analysis of each image to identify key information

related to the authenticity of the files. This process is supported by the use of JPEGsnoop, a desktop-based tool capable of deeply reading metadata and analyzing JPEG image compression traces [11]. Through this metadata examination, information regarding the origin of the image files can be obtained, allowing determination of whether the images are original or have undergone digital editing. The following are screenshots of the analysis results obtained using JPEGsnoop.

```
Signature:          017806585049CFE74CB0FC8FB07FFE79
Signature (Rotated): 017806585049CFE74CB0FC8FB07FFE79
File Offset:        0 bytes
Chroma subsampling: 2x2
EXIF Make/Model:    OK    [samsung] [SM-A507FN]
EXIF Makernotes:    NONE
EXIF Software:      OK    [A507FNXXS6DVC3]

Searching Compression Signatures: (3347 built-in, 0 user(*) )

       EXIF.Make / Software       EXIF.Model                          Quality          Subsamp Match?
       ------------------------   ---------------------------------   --------------   --------------

Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 2 - Image has high probability of being processed/edited
```

Figure 4. Metadata of the First Photograph

```
Signature:          01E76B1145D4662F80BA198358A896A4
Signature (Rotated): 01E76B1145D4662F80BA198358A896A4
File Offset:        0 bytes
Chroma subsampling: 1x1
EXIF Make/Model:    NONE
EXIF Makernotes:    NONE
EXIF Software:      NONE

Searching Compression Signatures: (3347 built-in, 0 user(*) )

       EXIF.Make / Software       EXIF.Model                          Quality          Subsamp Match?
       ------------------------   ---------------------------------   --------------   --------------
   SW :[Adobe Photoshop          ]                                    [Save For Web 100]

Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited
```

Figure 5. Metadata of the Second Photograph

Figures 4 and 5 present the metadata results obtained using the JPEGsnoop tool. The metadata analyzed from both images serves as evidence in the identification process. Based on the output from JPEGsnoop, information is obtained that indicates whether an image remains in its original state or has undergone editing.

3.3 *Analysis*

Previously, both photo files were examined to identify the metadata of each image. At this stage, further observation was carried out on both images to analyze the level of authenticity or possible errors present in the photos, as well as to apply the Error Level Analysis (ELA) technique. The use of the image splicing approach in detecting the authenticity of digital images is highly beneficial, as it can identify specific areas in the image that are suspected to have been manipulated. When applied to digital image samples, this method can increase the likelihood of detecting tampering, as the distribution pattern of the error level will appear different compared to an original, unedited image. One of the methods that can be used to detect such manipulation is Error Level Analysis (ELA), which serves as a tool to display the areas in an image suspected to have been altered [15].

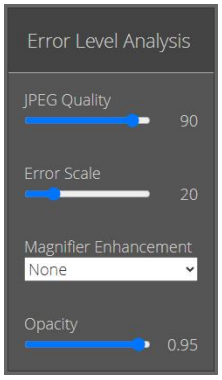

Figure 6. Indicator ELA

Figure 6 illustrates the settings used to analyze the first and second photographs. In the analysis process using Forensically Beta, a JPEG quality of 90 was applied, followed by an error scale of 20 and a darkness level of 0.95. These settings were implemented to detect the level of errors or digital discrepancies present in both images.

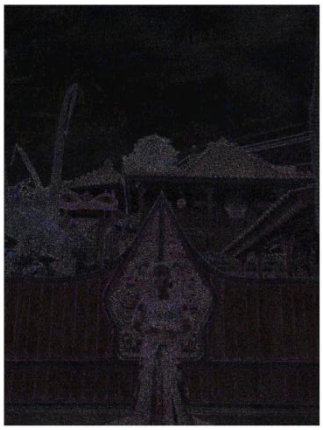

Figure 7. ELA result of the first photograph

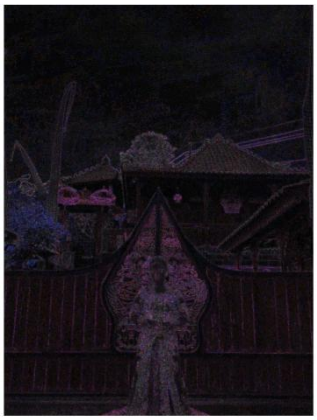

Figure 8. ELA result of the second photograph

The analysis results, after applying the same settings to both the first and second photographs using the Error Level Analysis (ELA) technique with Forensically Beta, revealed that the first photograph exhibits a uniform error distribution,

indicating that the image is likely original and free from digital manipulation. In contrast, the second photograph showed variations in compression levels, particularly in the main subject and background areas, suggesting the possibility of digital alteration. These findings reinforce the effectiveness of ELA in detecting visual integrity in JPEG images.

3.4 *Reporting*

Based on the analysis conducted on the two images, it is possible to compare them through their metadata using the tools JPEGsnoop and Forensically Beta. The following is the simulation report generated from the use of JPEGsnoop, presented in the form of the table below:

Table 1. JPEGsnoop Metadata Analysis

Metadata	**First Photograph**	**Second Photograph**
Model	samsung SM-A507FN	None
Chroma subsampling	1x1	2x2
DateTime Original	2022:04:19 14:18:29	2024:05:01 19:53:55
Software	None	Adobe Photoshop

From the report results, we can observe the differences between the two images based on the metadata analysis using the JPEGsnoop tool. The first photograph was taken and detected from a Samsung SM-A507FN camera on April 19, 2022, at 14:18:19. In contrast, the second photograph shows evidence of manipulation performed using Adobe Photoshop software on May 1, 2024, at 19:53:55.

Table 2. Analysis Report

	Error Level Analysis Technique	**Metadata**	**Status**
Photo 1	The error distribution is uniform, with no prominent patterns observed	samsung SM-A507FN 2022:04:19 14:18:29	**Original**
Photo 2	The error areas appear bright or uneven on both the subject and the background	Adobe Photoshop 2024:05:01 19:53:55	**Proven Edited Result**

Based on the analysis using the Error Level Analysis (ELA) technique, Photo 1 exhibits a uniform error distribution without noticeable patterns, indicating that the image is original and has not undergone digital manipulation. The metadata of this photo also supports this conclusion, showing that it was captured using a Samsung SM-A507FN device on April 19, 2022. In contrast, Photo 2 displays uneven bright areas in the ELA results, particularly around the subject, suggesting the presence of editing. This is further corroborated by the metadata, which records the use of Adobe Photoshop on May 1, 2024, leading to the conclusion that Photo 2 is an edited image.

4. Conclusion

Both photographs were examined using the JPEGsnoop and Forensically Beta tools. The first photo showed no alterations in its metadata, including the DateTime information, and no indications of manipulation using image editing software were found. Conversely, the second photo exhibited changes in metadata, such as the use of Adobe Photoshop and modifications in the DateTime, indicating that the image had undergone editing. Further analysis using the Error Level Analysis (ELA) technique and metadata reinforced these findings. The first photo demonstrated a uniform error distribution without notable patterns, confirming its authenticity, while the second photo displayed irregular error distribution, especially around the subject, strengthening the evidence of digital tampering. Based on the analysis of the digital evidence, it was revealed that among the two photos used as evidence, one had been manipulated. The photos consisted of an original image and a manipulated version derived from that original, rather than images that had been previously circulated.

It is hoped that through this approach, various new tools and techniques can be developed with the aim of comparing the existing forensic image devices, in order to identify the most effective solutions for detecting manipulation in photographs.

References

[1] M. M. Fajar, A. Johari, and H. Atmami, "Analisis Visual Fotografi Pre-Wedding Konsep Street Fotografi Karya Naturallica Photo," *J. Desain*, vol. 8, no. 3, p. 207, 2021, doi: 10.30998/jd.v8i3.8579.

[2] M. Badri, "Analisis Forensik Originalitas Gambar Menggunakan Autopsy Dan Opencv," *J. Satya Inform.*, vol. 8, no. 01, pp. 43–49, 2023, doi: 10.59134/jsk.v8i01.236.

[3] M. Ali Diko Putra, A. Wirawan Muhammad, B. Parga Zen, R. Yunita Kisworini, and T. Rohayati, "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," *J. Sist. Inf. Galuh*, vol. 2, no. 1, pp. 44–54, 2024, doi: 10.25157/jsig.v2i1.3695.

[4] K. Khairunnisak, H. Ashari, and A. P. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 3, no. 2, pp. 72–81, 2020, doi: 10.31598/jurnalresistor.v3i2.634.

[5] T. Ruslan, I. Riadi, and S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," *J. Fasilkom*, vol. 13, no. 02, pp. 286–292, 2023, doi: 10.37859/jf.v13i02.5540.

[6] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," *J. Pengabdi. Masy. dan Penerapan Ilmu Pengetah.*, vol. 3, no. 2, pp. 1–6, 2022, doi: 10.25299/jpmpip.2022.11003.

[7] M. Fransiskus and N. P, "Analisis Digital Forensik Metadata pada Rekayasa Digital Image sebagai barang bukti Digital," *J. Sains Dan Komput.*, vol. 8, no. 01, pp. 1–5, 2024, doi: 10.61179/jurnalinfact.v8i01.439.

[8] I. Riadi, Nasirudin, and Sunardi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 89–94, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/informatika89

[9] J. Informatika, "IMPLEMENTASI METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK UNTUK MENDETEKSI," vol. 16, no. 1, pp. 219–226, 2024.

[10] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.

[11] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 2, pp. 1100–1107, 2023, doi: 10.36040/jati.v7i2.6660.

[12] F. Isnaeni *et al.*, "ANALISIS FORENSIK SMARPHONE ANDROID," vol. 9, no. 1, pp. 1404–1410, 2025.

[13] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[14] M. R. Al-fajri, Caruddin, and D. Yusup, "Jurnal Sistem dan Teknologi Informasi Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist," *J. Sist. dan Teknol. Inf.*, vol. 6, no. 2, pp. 84–90, 2021, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

[15] H. Bisri and M. I. Marzuki, "Forensik Citra Digital Menggunakan Metode Error Level Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar," *G-Tech J. Teknol. Terap.*, vol. 7, no. 2, pp. 586–595, 2023, doi: 10.33379/gtech.v7i2.2363.