Vol. 7, No. 4, December 2025

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Forensic Analysis of AI-Generated Image Alterations Using Metadata Evaluation, ELA, and Noise Pattern Analysis

Ferdiansyah[1], Muhammad Rizki Akbar Deazwara[2], Reynaldi Rizki Billanivo[3], M. Ardiansyah[4], Ilham[5]

[1,2,3,4,5]Faculty of Computer and Science, Universitas Indo Global Mandiri, Palembang, Indonesia

Email: ferdi@uigm.ac.id[1], 2023310027p@students.uigm.ac.id[2], aldirheyn2015@gmail.com[3], 2022310068@students.uigm.ac.id[4], 2022310064@students.uigm.ac.id[5]

Received: Oct 27, 2025

Revised: Nov 25, 2025

Accepted: Dec 5, 2025

Published: Dec 18, 2025

Corresponding Author:

Author Name*:

Ferdiansyah

Email*:

ferdi@uigm.ac.id

DOI:

10.63158/journalisi.v7i4.1362

Abstract. This study develops a forensic workflow to assess the authenticity of digital images, addressing the challenge of distinguishing AI-generated content from real photographs. The goal is to analyze metadata, compression behavior, and noise characteristics to identify synthetic images. The dataset includes eight images: two original Xiaomi 14T Pro photos and six AI-generated variants from Gemini, ChatGPT, and Copilot. Metadata was extracted using ExifTool version 13.25 on Kali Linux, while Error Level Analysis (ELA) and Noise Pattern Analysis (NPA) were performed with consistent parameters on the Forensically platform. Authentic images displayed complete EXIF metadata, uniform compression patterns, and stochastic sensor noise. In contrast, AI-generated images lacked EXIF data, included XMP or C2PA provenance, exhibited localized compression anomalies, and showed smoother, more structured noise patterns. The study presents a practical and reproducible forensic workflow that integrates metadata evaluation, ELA, and noise analysis to detect synthetic content. The findings demonstrate that despite their visual realism, AI-generated images still leave detectable forensic traces, offering valuable tools for image authenticity verification.

Keywords: Digital Image Forensics, AI-Generated Images, Metadata Analysis, ELA, Noise Analysis

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

Recent advances in generative artificial intelligence, particularly Generative Adversarial Networks (GANs) and diffusion-based models, have enabled the creation of synthetic images that strongly resemble those captured by optical cameras [1], [2]. These generative systems can reproduce lighting behavior, spatial relationships, and fine-grained textures, which significantly reduces the perceptual differences between real and artificial imagery. As a result, visual inspection has become unreliable for determining image authenticity in investigative, journalistic, and security-critical environments [3], [4].

Before the emergence of modern AI-generated imagery, digital image forensics primarily focused on detecting conventional forms of manipulation such as splicing, copy–move cloning, inpainting, retouching, and JPEG recompression [5], [6], [7]. Foundational studies highlighted intrinsic forensic cues produced by camera imaging pipelines. These cues include EXIF metadata [8], JPEG quantization and blocking artifacts, [6], [9], camera model fingerprints [10], statistical noise characteristics [11], and sensor pattern noise (SPN or PRNU) that can uniquely identify imaging devices [12], [13]. Comprehensive surveys, including work by Piva, describe these techniques as core components of passive image forensics, which analyze acquisition-based, coding-based, and editing-based traces to assess authenticity [14]. Provenance-based approaches that rely on metadata and container structures have also contributed substantially to digital investigations, enabling analysts to reconstruct content history and detect signs of modification [15], [16], [17].

Recent developments in forensic datasets and acquisition pipelines have further expanded the complexity of authenticity assessment. The FloreView dataset, for example, demonstrates that variations in smartphone imaging pipelines can influence the performance and calibration of forensic methods [18]. Additional work on EXIF integrity has shown that different transmission channels may preserve or remove metadata to varying degrees, which underscores the importance of reliable metadata examination [19]. Studies on hoax imagery have also compared EXIF analysis, reverse image search, and classical forensic methods to assess their effectiveness in identifying manipulated content [20]. These challenges highlight the increasing need for multi-layered forensic reasoning.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Despite these advancements, research on synthetic image forensics remains focused on specific technical aspects. Several studies investigate GAN fingerprints [16], deepfake characteristics [2], or CNN-based detection of synthetic artifacts [1]. However, these works are frequently limited to individual detection tasks and do not integrate metadata-level, compression-level, and noise-level indicators into a unified workflow. Consequently, existing research lacks a comprehensive and reproducible forensic methodology dedicated specifically to AI-generated images. A fundamental limitation of prior work is that it does not explicitly address AI-generated imagery through an integrated workflow that combines metadata evaluation, error level analysis, and noise pattern analysis.

To respond to these challenges, a structured and repeatable forensic methodology is required. Without a standardized approach, authenticity assessments may become inconsistent, subjective, and difficult to replicate. The objective of this study is to formulate a complete forensic flow that can be adopted by researchers and practitioners to systematically examine AI-generated images. The proposed workflow follows the established four-phase forensic model consisting of Collection, Examination, Analysis, and Reporting, which has been widely referenced in contemporary forensic literature [21], .

This study introduces a multimodal forensic approach that integrates metadata evaluation, error level analysis, and noise pattern analysis. Metadata evaluation examines differences in EXIF, XMP, and C2PA provenance structures to differentiate optical camera images from synthetic outputs [8], [22], [23]. Error level analysis reveals localized inconsistencies produced by algorithmic reconstruction, which is consistent with previous studies on JPEG ghost artifacts and recompression traces [6], [9], [24]. Noise pattern analysis focuses on high-frequency residuals to distinguish natural sensor noise from synthetic noise that typically appears more uniform or structurally regular than noise produced by physical imaging sensors [11] - [13]. The integration of these techniques is aligned with recommendations from multimedia provenance research, which emphasize cross-validation across multiple signal layers for increased reliability [15], [25].

The contribution of this study does not involve designing a new detection algorithm. Instead, it offers a practical, reproducible, and integrated forensic workflow specifically designed for analyzing AI-generated images. The resulting framework can support forensic investigators, digital analysts, journalists, and researchers who require an

evidence-based method for evaluating the authenticity of synthetic visual content. "This study also aligns with the Sustainable Development Goals (SDGs), particularly Goal 9 on industry, innovation, and infrastructure for secure digital ecosystems."

2. METHODS

This study applies a structured forensic workflow that consists of four stages: Collection, Examination, Analysis and Reporting. The overall process is illustrated in Figure 1 and serves as the methodological foundation for obtaining all results presented in later sections. The workflow combines metadata extraction, compression evaluation and noise-pattern interpretation in a consistent sequence so that every analytical step can be replicated reliably.

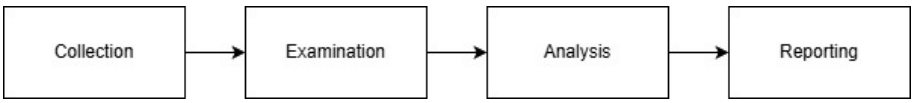


Figure 1. Forensic method

The Collection stage begins with acquiring two reference photographs that represent outdoor and indoor environments. Both images were captured using a Xiaomi 14T Pro smartphone in native JPEG format. Using a single device ensures consistent camera characteristics, EXIF structure and JPEG compression behaviour. These originals establish the optical baseline for the study. Six additional images were then created using Gemini, ChatGPT and Copilot. Each system generated one outdoor variant and one indoor variant in PNG format. The use of JPEG for authentic captures and PNG for synthetic outputs creates clear structural differences that support later forensic evaluation. All eight images form the dataset used throughout the research.

Metadata Examination is performed using ExifTool version 13.25. This tool extracts EXIF, XMP and C2PA fields from each file. The authentic JPEG images contain complete EXIF metadata such as camera make and model, aperture, ISO, exposure time, GainMap and MPF0 entries. These fields indicate direct optical capture. The AI-generated PNG images contain no EXIF fields. Gemini outputs include XMP entries that indicate AI processing by Google systems. ChatGPT and Copilot outputs contain complete C2PA provenance

records that document model identity, source type and signed integrity information. These differences establish the provenance baseline that supports later analysis.

The Analysis stage consists of two forensic techniques that are applied uniformly to all images. Error Level Analysis (ELA) is performed using the Forensically platform with JPEG Quality set to 50, Error Scale set to 50 and Opacity set to 1.00. Although the AI-generated files are in PNG format, forensically converts PNG images into internal JPEG representations. This allows ELA to highlight reconstruction anomalies that arise from generative modification. Noise Pattern Analysis is performed using the Noise tool in Forensically with Amplitude set to 1 and Opacity set to 1.00. This method isolates high-frequency residuals that reveal whether noise originates from a physical camera sensor or from algorithmic rendering. Using identical parameters for all images ensures that any differences observed in ELA and noise patterns originate from the images themselves rather than from configuration differences.

The Reporting stage consolidates findings from metadata inspection, ELA and noise evaluation into a unified forensic interpretation. This stage ensures that all analytical outcomes are interpreted consistently with the workflow described in this section. For clarity and reproducibility, the tools and configurations used throughout the study are summarized in Table 1.

Table 1. Tools and configuration settings used in the forensic analysis workflow

Tool / Platform	Purpose	Key Parameters
Xiaomi 14T Pro Camera	Acquisition of original images	JPEG output, native EXIF
ExifTool v13.25	Metadata extraction	Full EXIF, XMP, C2PA parsing
Forensically – ELA Tool	Error Level Analysis	Quality 50, Error Scale 50, Opacity 1.0
Forensically – Noise Tool	Noise Pattern Analysis	Amplitude 1, Opacity 1.0

All analyses presented in the subsequent sections were performed using the configurations listed in Table 1 to ensure methodological consistency and full reproducibility.

3. RESULTS AND DISCUSSION

3.1. Data Collection

The Data Collection stage corresponds directly to the first phase of the forensic workflow. This stage establishes the controlled acquisition environment required to ensure that all subsequent forensic procedures are performed on images with verifiable origins. Two authentic photographs were captured using a Xiaomi 14T Pro camera. These photographs serve as baseline optical references and allow clear differentiation between characteristics produced by a physical camera and those generated algorithmically.

Both original photographs were stored in JPEG format. The outdoor image has a resolution of 3000 × 4000 pixels with a file size of 3.40 MB (3,575,274 bytes). The indoor image has a resolution of 3060 × 4080 pixels with a file size of 3.43 MB (3,598,260 bytes). These files retain complete camera metadata and represent the authentic outputs of a physical imaging pipeline. Their controlled acquisition ensures that any deviations identified during forensic analysis can be attributed to computational reconstruction rather than instability in the capture device.

Figure 2. Outdoor scene original image

Figure 3. Indoor scene original image

Figure 2 presents the original outdoor image captured under natural lighting conditions. The scene includes a human subject, varied textures, and gradient regions that support examination of compression and noise characteristics. Figure 3 shows the original indoor image containing signage and structured interior elements that provide stable features for comparison with synthetically altered variants.

The six AI-generated images used for comparison were produced using Gemini, ChatGPT, and Copilot. Each system generated one outdoor variant and one indoor variant based on the two original photographs. All AI outputs were provided in PNG format. PNG uses lossless compression, which results in structural differences compared to the lossy JPEG format of the original images. Although PNG does not introduce compression artefacts, the forensic platform used in this study can process PNG inputs for visual analysis and performs internal recompression when required. This capability ensures that PNG files remain compatible with techniques such as Error Level Analysis in the later Analysis stage.

(a) (b) (c)

Figure 4. Outdoor scene AI-Generated images: (a) Gemini, (b) ChatGPT, (c) Copilot

(a) (b) (c)

Figure 5. Indoor scene AI-Generated images: (a) Gemini, (b) ChatGPT, (c) Copilot

The six AI-generated variants derived from the two original photographs introduce distinct reconstructed elements. Figure 4(a), generated by Gemini, shows the outdoor scene modified with a small moon positioned at the upper-right corner. Figure 4(b), produced by ChatGPT, presents the same scene with a medium-sized moon placed centrally in the sky. Meanwhile, Figure 4(c), created by Copilot, displays a version containing a much larger moon on the left side along with broader sky alterations. The indoor scene exhibits similarly targeted reconstruction. Figure 5(a), generated by Gemini, replaces the original "SALAD BAR" signage with the word "OPEN." Figure 5(b), produced by ChatGPT, changes the text to "DAPUR," while Figure 5(c), created by Copilot, generates the variant reading "TERBUKA." Collectively, these indoor and outdoor AI-generated reconstructions offer contrasting modifications that will later be examined through metadata inspection, ELA, and noise-based analysis.

3.2. Metadata Examination

The Metadata Examination stage corresponds to the second phase of the forensic workflow. This stage focuses on analysing the structural attributes embedded within each file, including EXIF content, software identifiers, provenance fields, and file-format characteristics. Metadata is a fundamental forensic indicator because authentic photographs preserve camera-derived information, while AI-generated images typically contain software-level descriptors without optical acquisition records.

Before examining the complete metadata comparison, Figure 6 presents a representative excerpt from the output of the exiftool -v3 command executed on the original outdoor image. The full command generates an extensive metadata log that includes detailed camera parameters and internal JPEG structures. Only a small portion of this output is shown in the figure to illustrate the presence of complete EXIF metadata without displaying the entire log, which is substantially longer.

To avoid presenting lengthy EXIFTool logs for all images, the metadata characteristics of the eight files were summarised in the comparative Tables 2. These tables highlight essential forensic attributes that distinguish camera-captured content from AI-generated outputs.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

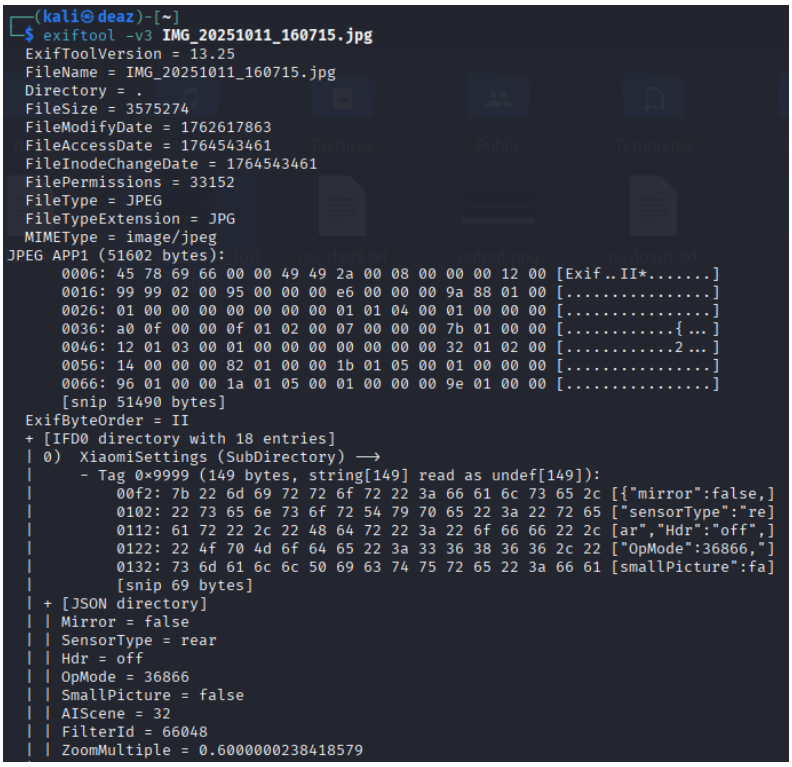


Figure 6 Excerpt of the ExifTool output from the original outdoor image

Table 2. Comparative metadata characteristics of original and AI-generated images

Metadata Attribute	Original Outdoor	Original Indoor	Gemini	ChatGPT	Copilot
File Format	JPEG	JPEG	PNG	PNG	PNG
EXIF Presence	Complete EXIF	Complete EXIF	None	None (replaced by C2PA)	None (replaced by C2PA)
Camera Make/Model	Xiaomi 14T Pro	Xiaomi 14T Pro	Not applicable	Not applicable	Not applicable
Aperture	f/2.2	f/2.0	Not applicable	Not applicable	Not applicable
ISO	50	400	Not applicable	Not applicable	Not applicable
Exposure Time	0.001197 s	1/100 s	Not applicable	Not applicable	Not applicable

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Metadata Attribute	Original Outdoor	Original Indoor	Gemini	ChatGPT	Copilot
Software Tag	Xiaomi Camera System	Xiaomi Camera System	"Edited with Google AI", Picasa tags	ClaimGenerator: ChatGPT (C2PA)	Microsoft_Responsible_AI / Azure ImageGen
DigitalSourceType	Camera	Camera	Synthetic	trainedAlgorithmicMedia	Synthetic
Provenance Indicators	GainMap, MPF0; consistent timestamps	GainMap, MPF0; consistent timestamps	XMP AI-editing metadata	Full C2PA record with valid signature	Full C2PA record; validated PNG chunk hashes

The original outdoor and indoor photographs contain complete EXIF metadata, which includes camera identification, exposure parameters, and structural components such as GainMap and MPF0. These attributes are consistently stored in both original images and confirm that they were produced directly by a physical imaging device. The presence of matching and coherent timestamps further supports their authenticity as unmodified optical captures.

All AI-generated images differ significantly from the originals. The outputs from Gemini, ChatGPT, and Copilot were produced in PNG format and do not contain EXIF metadata. The Gemini files store XMP descriptors that indicate AI-driven editing or generation, while the ChatGPT and Copilot files include structured C2PA provenance records. These C2PA entries document generative source information, model identifiers, and integrity statements. Although C2PA enhances transparency in content provenance, it does not provide an absolute guarantee of authenticity because provenance metadata can be removed or modified when a file is reprocessed.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

The relevant point for forensic interpretation is that the metadata of all AI outputs is identical across the outdoor and indoor scenes. The structure of AI-generated metadata is determined by the generative platform, not by scene content or optical variation. This creates a clear and consistent separation between camera-captured images, which store detailed physical acquisition parameters, and AI-generated images, which rely on software-level provenance instead. The distinctions revealed through metadata inspection form the foundation for evaluating compression artefacts and noise characteristics in the Analysis stage, where synthetic traces become more visible through Error Level Analysis and noise pattern evaluation.

3.3. Error Level Analysis

Error Level Analysis is the first part of the Analysis stage in the forensic workflow. This technique evaluates the distribution of compression errors in an image by comparing the original file against a recompressed version. Authentic JPEG photographs typically exhibit a relatively uniform ELA pattern because all regions undergo the same single-compression process. In contrast, synthetic or modified content often displays inconsistent error responses that emerge from regeneration or localized recompression effects.

This study performed ELA using the Forensically platform. Although the AI-generated images were provided in PNG format, the platform is able to process PNG inputs by internally generating a recompressed version for comparison. Therefore, no manual conversion step was required, and all images could be analysed directly while maintaining consistency across the dataset.

Figure 7 presents the configuration used for all images during ELA. JPEG Quality was set to 50, the Error Scale was fixed at 50, and opacity was set to 1.00. These parameters were applied uniformly to ensure comparability across both authentic and AI-generated images.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

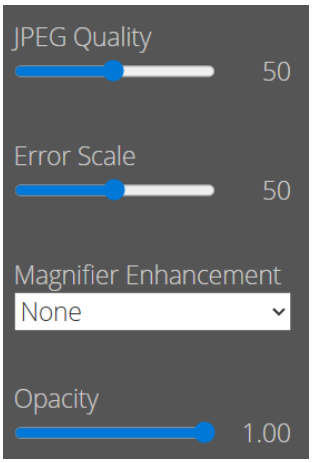
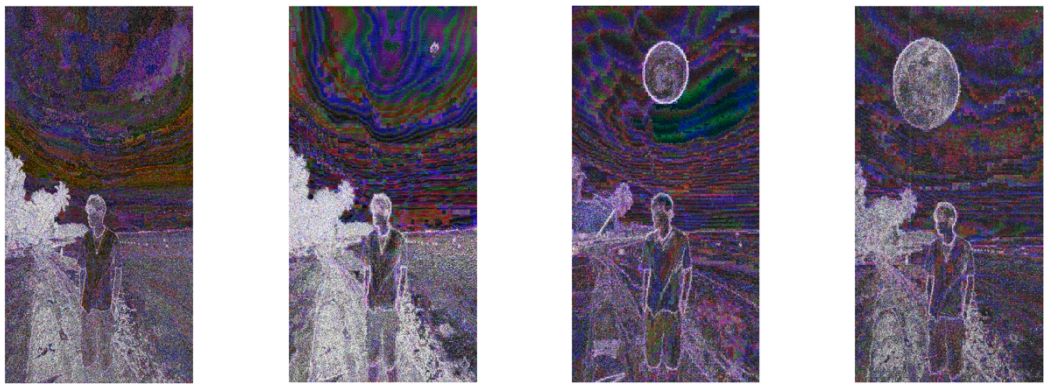


Figure 7. ELA configuration in Forensically

The outdoor scene was analysed first to observe how generative modifications appear in an open environment with natural lighting and smooth sky gradients. This scene provides clear visual regions where reconstruction is expected to occur, particularly in the AI-generated variants that introduce synthetic moons and altered sky textures. The ELA results for the outdoor images are presented in Figure 15.



(a) (b) (c) (d)

Figure 8. ELA comparison of the outdoor image: (a) original, (b) Gemini, (c) ChatGPT, (d) Copilot

The ELA results for the outdoor images reveal clear distinctions between the authentic photograph and the AI-generated variants. Figure 8(a) shows a uniform compression pattern across the sky, subject, and surrounding elements, consistent with a genuine camera capture. In Figure 8(b), the Gemini-generated version introduces a small synthetic moon, and the surrounding sky displays fragmented error regions indicative of

reconstruction. Figure 8(c) shows that ChatGPT produces a stronger anomaly, with a concentrated error spike around the centrally placed moon and visible banding across the sky. In Figure 8(d), the Copilot-generated output features a large moon on the left side accompanied by horizontal distortions, further departing from the stable pattern observed in the original. These differences collectively indicate that each generative model leaves identifiable reconstruction artifacts visible through ELA analysis.

The indoor scene offers a different context for ELA evaluation because it contains structured surfaces, high-contrast edges, and text-based signage. These characteristics make indoor imagery useful for assessing how generative models reconstruct fine details and sharp boundaries. The ELA outputs for the indoor images are shown in Figure 16.

Figure 9. ELA comparison of the indoor image: (a) original, (b) Gemini, (c) ChatGPT, (d) Copilot

The indoor ELA results show a similarly clear contrast between the authentic photograph and each AI-generated reconstruction. Figure 9(a) displays the original image with a stable and relatively uniform error distribution across the "SALAD BAR" sign, the wooden board, and other interior elements, reflecting a natural single-compression pattern. In Figure 9(b), the Gemini-generated version, which reconstructs the signage into "OPEN," introduces elevated error responses around the modified text and surrounding wood texture. Figure 9(c) shows that ChatGPT's version, containing the replacement text "DAPUR," produces sharper error boundaries and stronger localized contrasts within the edited region. In Figure 9(d), the Copilot variant changes the text to "TERBUKA"; although visually smoother, its ELA output still reveals irregularities around the altered signage that deviate from the baseline pattern of the original. Collectively, these results confirm

that each AI-generated indoor image carries detectable compression inconsistencies absent in the authentic photograph.

The ELA results demonstrate consistent differences between the authentic camera outputs and the AI-generated images. The original photographs exhibit uniform error patterns that correspond to a single JPEG compression process. In contrast, all synthetic images contain localized error responses associated with generative reconstruction. These responses include brighter edges, inconsistent texture patterns, and irregular compression artefacts around the modified regions.

The ability of ELA to identify these inconsistencies provides a clear distinction between optical captures and AI-generated variants. These findings complement the metadata inspection presented earlier and establish a foundation for the subsequent noise analysis, where sensor-derived characteristics provide additional forensic indicators.

3.4. Noise Analysis

Noise Analysis is the second component of the Analysis stage in the forensic workflow shown in Figure 1. This technique examines fine-grained variations in image noise to identify whether an image contains natural sensor noise or synthetic residuals produced by generative models. Authentic photographs typically retain stochastic noise that originates from the camera sensor and exposure conditions, while AI-generated images often exhibit smoother or patterned noise due to the reconstruction processes used by generative models.

Noise analysis in this study was performed using the Forensically platform with the Noise Amplitude parameter set to 1 and opacity set to 1.00. These settings were applied uniformly to all images to ensure consistent interpretation across both original and AI-generated content. Since Forensically can process PNG and JPEG inputs directly, all images were analysed using the same configuration without requiring additional pre-processing.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Before examining the noise patterns in the outdoor and indoor scenes, the configuration used for this analysis is shown in Figure 10. These settings were applied uniformly to every image to maintain consistency throughout the evaluation and to support reliable comparison between the original photographs and their AI-generated counterparts.

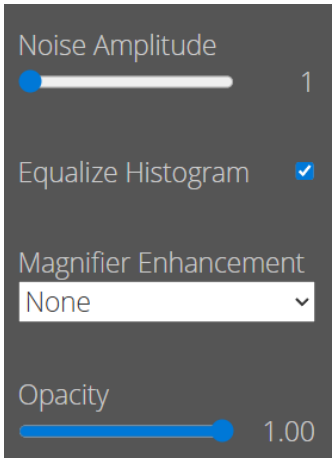
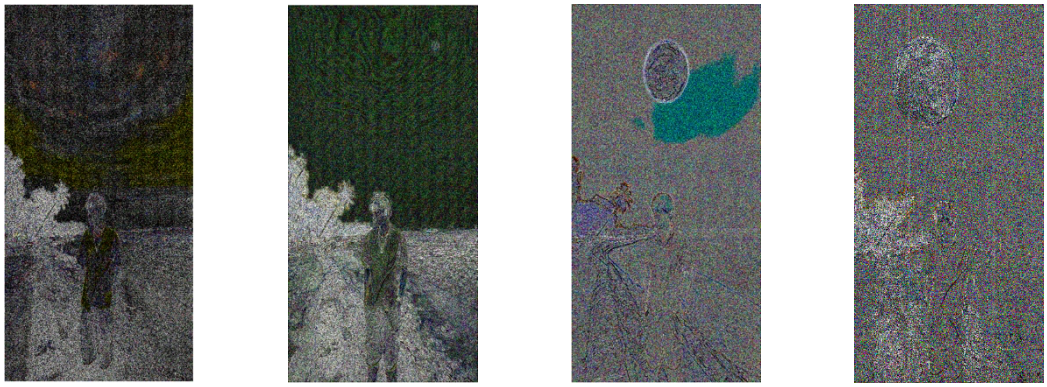


Figure 10. Noise analysis configuration in Forensically

Before examining the noise results, it is useful to note that the outdoor scene includes smooth sky regions, textured surfaces, and varying levels of illumination. These characteristics make it suitable for identifying natural stochastic noise patterns in the original image and for comparing them with the noise behaviour of the AI-generated variants.



(a) (b) (c) (d)

Figure 11. Noise-analysis comparison of the outdoor image: (a) original, (b) Gemini, (c) ChatGPT, (d) Copilot

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

The outdoor noise analysis reveals distinct differences between the authentic photograph and its AI-generated variants. Figure 11(a) shows naturally random camera noise distributed across the sky and darker regions. In Figure 11(b), the Gemini output appears noticeably smoother, with reduced noise around the reconstructed sky and moon. Figure 11(c) shows that ChatGPT introduces more structured, non-stochastic noise, particularly in the sky. Figure 11(d), the Copilot version, smooths the scene even further, removing most natural noise and producing a uniform texture inconsistent with optical capture. These patterns illustrate how each model suppresses or alters the original noise structure. The indoor scene contains textured wooden surfaces, synthetic signage replacements, and uniform interior regions. These characteristics provide a distinct context for evaluating how reconstruction affects noise behaviour in AI-generated variants.

(a) (b) (c) (d)

Figure 12. Noise-analysis comparison of the indoor image: (a) original, (b) Gemini, (c) ChatGPT, (d) Copilot

The indoor noise analysis shows a similar contrast between the authentic photograph and the AI-generated variants. Figure 12(a) displays natural sensor noise distributed across the wooden board, signage, and other textured areas. In Figure 12(b), the Gemini version replacing the text with “OPEN” exhibits smoother backgrounds and structured noise around the new letters. Figure 12(c) shows that ChatGPT’s “DAPUR” variant introduces artificial noise patterns that differ from camera-generated randomness. Figure 12(d), the Copilot version with the text “TERBUKA,” appears smoother overall but still lacks the natural stochastic noise of the original. These differences highlight the disruption of authentic noise characteristics across the AI-generated indoor variants.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Noise analysis consistently distinguishes the original photographs from all AI-generated variants. The authentic images contain irregular and stochastic noise patterns that correspond to camera sensor behaviour. In contrast, the AI-generated images demonstrate noise responses that are either overly smooth or contain structured residuals that do not align with natural optical processes. These differences support the findings from the Metadata Examination and Error Level Analysis, and provide an additional layer of confirmation that the AI-generated images do not originate from a physical imaging pipeline. Noise Analysis therefore strengthens the overall forensic interpretation by revealing underlying characteristics that remain visible even when the visual appearance of the AI-generated content is realistic.

3.5. Discussion

This section represents the Reporting stage of the forensic workflow shown in Figure 1. At this stage, the results from Metadata Examination, Error Level Analysis, and Noise Analysis are consolidated into a unified interpretation. The overall findings are summarised in Table X, which provides a comparative overview of the forensic characteristics observed in both the original images and the AI-generated variants.

Table 3. Summary of forensic findings

Analysis Aspect	Original Image	Gemini	ChatGPT	Copilot
Metadata/EXIF	Complete EXIF; Xiaomi 14T Pro camera; GainMap & MPF0 present; single-camera JPEG	EXIF missing; PNG format; XMP "Edited with Google AI"; Picasa software tags	EXIF missing; full C2PA structure; trainedAlgorithmicMedia; valid signatures	EXIF missing; C2PA present; Azure OpenAI ImageGen; all PNG chunk hashes validated
ELA Pattern	Homogeneous error distribution; no hotspots;	Strong hotspots in reconstructed areas; banding	Extreme ELA spikes; wide color banding; digitally	Clear synthetic-object outlines; horizontal distortions;

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Analysis Aspect	Original Image	Gemini	ChatGPT	Copilot
	natural camera compression	present; sharp lunar outline	regenerated horizon	visually smooth but still anomalous
Noise Pattern	Stochastic sensor noise; consistent across regions	Suppressed noise; heavy denoising visible	Significant channel noise shifts; synthetic residuals	Noise almost entirely removed; smooth digital artefacts remain

The summary shows a consistent separation between authentic camera-captured images and synthetic outputs. The original photographs contain complete EXIF metadata with coherent timestamps and camera parameters, while the AI-generated files lack optical metadata and instead include XMP or C2PA provenance structures. Although C2PA provides useful generative-source information, it can be removed during post-processing, so it cannot serve as a stand-alone authenticity indicator.

The ELA results further reinforce the distinction. The original images display uniform compression behaviour, whereas the AI-generated variants contain localized anomalies around reconstructed regions. These include hotspots, banding, and irregular patterns that arise from generative reconstruction rather than natural camera compression. Noise Analysis provides additional confirmation. Authentic images exhibit irregular and stochastic sensor noise, while AI-generated images show either suppressed noise or structured residuals that do not resemble natural noise behaviour. This pattern remains consistent across both indoor and outdoor scenes.

Overall, the combined results demonstrate that metadata provenance, compression behaviour, and noise characteristics each provide complementary evidence. When these techniques are applied together within a structured forensic workflow, they allow clear differentiation between genuine optical images and those produced by generative AI systems. This integrated approach assists investigators and analysts by offering reliable

indicators even when the visual appearance of the synthetic images closely resembles real photographs.

4. CONCLUSION

This study evaluated the authenticity of digital images using a structured forensic workflow consisting of the Collection, Examination, Analysis, and Reporting stages. The findings show that metadata inspection, Error Level Analysis, and Noise Analysis provide consistent indicators for distinguishing authentic camera-captured photographs from AI-generated variants. The original images retained complete EXIF metadata, uniform compression behaviour, and natural stochastic noise, while the synthetic images produced by Gemini, ChatGPT, and Copilot lacked optical provenance, contained localized compression anomalies, and exhibited noise patterns that differed from natural sensor characteristics. These results demonstrate that the applied workflow remains effective for identifying algorithmically generated imagery even when the visual appearance of the synthetic outputs closely resembles real photographs.

Several limitations were identified during this study. The dataset consisted of only two original photographs, which limits scene diversity. The evaluation focused solely on three AI models and two analysis techniques, meaning that the results may not generalize to all generative methods or forensic tools. Error Level Analysis is influenced by compression settings and image structure, and Noise Analysis does not account for advanced denoising strategies used in emerging generative pipelines. In addition, provenance metadata such as C2PA can be removed during reprocessing, which reduces its reliability as a single-source authenticity indicator.

Future work may include expanding the dataset to cover a broader range of scenes, devices, and generative models. Additional forensic metrics such as frequency-domain analysis or statistical noise modelling could also be incorporated to strengthen the evaluation. Integrating automated provenance verification and model attribution techniques may further support investigators in identifying synthetic content across diverse digital environments.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

REFERENCES

[1] S.-Y. Wang, O. Wang, R. Zhang, A. Owens, and A. A. Efros, "CNN-generated images are surprisingly easy to spot... for now," Apr. 2020. doi: 10.48550/arXiv.1912.11035.

[2] L. Verdoliva, "Media Forensics and DeepFakes: an overview," Jan. 2020. doi: 10.48550/arXiv.2001.06564.

[3] A. Näslund, "Image metadata. From information management to interpretative practice," Museum Management and Curatorship, vol. 39, no. 4, pp. 398–418, Jul. 2024, doi: 10.1080/09647775.2022.2073562.

[4] H. T. Sencar and N. Memon, "Overview of State-of-the-Art in Digital Image Forensics," in Algorithms, Architectures and Information Systems Security, vol. Volume 3, in Statistical Science and Interdisciplinary Research, vol. Volume 3. , WORLD SCIENTIFIC, 2008, pp. 325–347. doi: 10.1142/9789812836243_0015.

[5] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: a booklet for beginners," Multimed Tools Appl, vol. 51, no. 1, pp. 133–162, 2011, doi: 10.1007/s11042-010-0620-1.

[6] H. Farid, "Exposing Digital Forgeries from JPEG Ghosts," IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 154–160, Mar. 2009, doi: 10.1109/TIFS.2008.2012215.

[7] N. K. Gill, R. Garg, and E. A. Doegar, "A Review Paper on Digital Image Forgery Detection Techniques," in 8th International Conference on Computing, Communication and Networking Technologies, Delhi: IEEE, 2017. doi: 10.1109/ICCCNT.2017.8203904.

[8] N. D. Arizona, M. A. Nugroho, A. R. Syujak, R. K. Saputra, and I. Sulistyowati, "Metadata Forensic Analysis as Support for Digital Investigation Process by Utilizing Metadata-Extractor," Journal of Intelligent Software Systems, vol. 3, no. 2, pp. 27–31, Dec. 2024, doi: 10.26798/jiss.v3i2.1503.

[9] N. A. N. Azhan, R. A. Ikuesan, S. A. Razak, and V. R. Kebande, "Error Level Analysis Technique for Identifying JPEG Block Unique Signature for Digital Forensic Analysis," Electronics (Basel), vol. 11, no. 9, 2022, doi: 10.3390/electronics11091468.

[10] M. Kharrazi, H. T. Sencar, and N. Memon, "BLIND SOURCE CAMERA IDENTIFICATION," in 2004 International Conference on Image Processing, Singapore: IEEE, 2004, pp. 709–712. doi: 10.1109/ICIP.2004.1418853.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[11] A. K. Boyat and B. K. Joshi, "A Review Paper : Noise Models in Digital Image Processing," Signal Image Process, vol. 6, no. 2, pp. 63–75, Apr. 2015, doi: 10.5121/sipij.2015.6206.

[12] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Proc.SPIE, Feb. 2006, p. 60720Y. doi: 10.1117/12.640109.

[13] J. Lukáš, J. Fridrich, and M. Goljan, "Digital Camera Identification from Sensor Pattern Noise," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, Jun. 2006, doi: 10.1109/TIFS.2006.873602.

[14] A. Piva, "An Overview on Image Forensics," Int Sch Res Notices, vol. 2013, no. 1, p. 496701, Jan. 2013, doi: 10.1155/2013/496701.

[15] A. Bharati et al., "Beyond Pixels: Image Provenance Analysis Leveraging Metadata," in 2019 IEEE Winter Conference on Applications of Computer Vision (WACV), 2019, pp. 1692–1702. doi: 10.1109/WACV.2019.00185.

[16] N. Yu, L. Davis, and M. Fritz, "Attributing Fake Images to GANs: Learning and Analyzing GAN Fingerprints," Aug. 2019. doi: 10.48550/arXiv.1811.08180.

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

[18] D. Baracchi, D. Shullani, M. Iuliani, and A. Piva, "FloreView: An Image and Video Dataset for Forensic Analysis," IEEE Access, vol. 11, pp. 109267–109282, Oct. 2023, doi: 10.1109/ACCESS.2023.3321991.

[19] N. Soni, "Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods," Perspectives in Legal and Forensic Sciences, vol. 2, no. 2, 2025, doi: 10.70322/plfs.2025.10006.

[20] M. Subli, M. M. Efendi, and Salman, "PERBANDINGAN HASIL ANALISA FOTO HOAX MENGGUNAKAN METODE EXIF/METADATA, REVERSE IMAGE DAN FORENSICS," Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 1, pp. 798–811, May 2022, doi: 10.35957/jatisi.v9i1.1578.

[21] S. Raghavan, "Digital forensic research: current state of the art," CSI Transactions on ICT, vol. 1, no. 1, pp. 91–114, 2013, doi: 10.1007/s40012-012-0008-7.

[22] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?," in Proceedings of the 15th ACM International Conference on Multimedia, in MM '07. New York, NY, USA: Association for Computing Machinery, 2007, pp. 78–86. doi: 10.1145/1291233.1291252.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[23] M. Anugraha, R. P. Kristianto, and A. Hartanto, "Forensic Metadata Analysis in Detecting Digital Image Manipulation," Journal of Science and Computers, vol. 9, no. 2, pp. 56–61, Aug. 2025, doi: 10.61179/infact.v9i02.754.

[24] T. S. Gunawan, S. A. M. Hanafiah, M. Kartiwi, N. Ismail, N. F. Za'bah, and A. N. Nordin, "Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation Using Error Level Analysis," Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 1, pp. 131–137, 2017, doi: 10.11591/ijeecs.v7.i1.pp131-137.

[25] T. Van Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A Survey on Digital Camera Image Forensic Methods," in 2007 IEEE International Conference on Multimedia and Expo, 2007, pp. 16–19. doi: 10.1109/ICME.2007.4284575.