Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
5 (3) 2025, Page 15079-15088

Digital Image–Based Document Authenticity Analysis Using The Daus Approach Through Texture Feature Extraction And Visual Characteristics

Ritna Wahyuni[1], Firdaus[2]
[1] Sistem dan Teknologi Informasi, Institut Teknologi Sawit Indonesia, Medan
[2] Manajemen Informatika, Universitas Putra Indonesia YPTK, Padang
Corresponding Author: ritnawahyuni@itsi.ac.id

ABSTRAK

Keaslian dokumen adalah isu penting di lingkungan administratif, akademik, dan hukum karena kemudahan manipulasi dokumen menggunakan teknologi digital yang semakin meningkat. Penelitian ini berfokus pada menganalisis keaslian dokumen berdasarkan pemrosesan citra digital dengan memanfaatkan pendekatan DAUS melalui ekstraksi fitur tekstur dan karakteristik visual. Masalah yang dibahas dalam penelitian ini adalah bagaimana membedakan secara efektif antara dokumen asli dan yang dimanipulasi menggunakan analisis berbasis citra. Pendekatan yang diusulkan melibatkan pemrosesan gambar dokumen yang dipindai atau difoto untuk mengekstraksi fitur tekstur dan petunjuk visual, seperti pola permukaan, distribusi tinta, dan ketidakkonsistenan struktural, yang mungkin menunjukkan adanya perubahan. Fitur-fitur ini kemudian dianalisis untuk mengidentifikasi perbedaan antara dokumen asli. Hasil analisis menunjukkan bahwa kombinasi fitur tekstur dan karakteristik visual dapat memberikan informasi yang bermakna untuk mendeteksi keaslian dokumen. Studi ini menyimpulkan bahwa analisis berbasis citra digital menggunakan pendekatan DAUS menawarkan alternatif yang menjanjikan dibanding inspeksi manual, memungkinkan metode yang lebih objektif dan sistematis untuk verifikasi dokumen. Temuan ini diharapkan dapat berkontribusi pada pengembangan sistem autentikasi dokumen yang andal dalam berbagai aplikasi praktis.

Kata Kunci: Keaslian, Pemrosesan Citra Digital, Ekstraksi Fitur Tekstur, Karakteristik Visual, Pendekatan DAUS

ABSTRACT

Document authenticity is a critical issue in administrative, academic, and legal environments due to the increasing ease of document manipulation using digital technologies. This research focuses on analyzing document authenticity based on digital image processing by utilizing the DAUS approach through texture feature extraction and visual characteristics. The problem addressed in this study is how to effectively distinguish between authentic and manipulated documents using image-based analysis. The proposed approach involves processing scanned or photographed document images to extract texture features and visual cues, such as surface patterns, ink distribution, and structural inconsistencies, which may indicate alterations. These features are then analyzed to identify differences between original and non-original documents. The results of the analysis demonstrate that the combination of texture features and visual characteristics can provide meaningful information for detecting document authenticity. This study concludes that digital image–based analysis using the DAUS approach offers a promising alternative to manual inspection, enabling a more objective and systematic method for document verification. The findings are expected to contribute to the development of reliable document authentication systems in various practical applications.

Keywords: *Authenticity, Digital Image Processing, Texture Feature Extraction, Visual Characteristics, DAUS Approach*

© The Author(s). 2025 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

INTRODUCTION

The authenticity of documents is a fundamental requirement in administrative, academic, legal, and financial domains, where documents serve as primary evidence for verification and decision-making processes. However, the rapid development of digital imaging devices and image editing software has

significantly increased the risk of document forgery. Modern manipulation techniques allow forged documents to closely resemble original ones, making manual inspection unreliable and prone to subjective judgment. Consequently, digital image–based approaches have become increasingly important for document authenticity analysis [5], [9].

A major difficulty in detecting document forgery lies in identifying subtle inconsistencies that occur during manipulation, such as irregular ink distribution, altered text regions, or unnatural surface patterns. These inconsistencies are often embedded within the texture and visual structure of document images and are difficult to perceive using human vision alone. Studies have shown that forged document regions frequently exhibit abnormal texture characteristics caused by editing, reprinting, or rescanning processes, which can be effectively captured using texture-based image analysis techniques [4], [6].

Recent research in document image forensics has focused on exploiting texture features and visual descriptors to detect forged or tampered regions. Traditional approaches utilize statistical texture analysis and local texture descriptors to model surface variations in document images [6], while more advanced methods employ multi-scale texture understanding and feature fusion strategies to improve detection performance [4], [8]. In parallel, deep learning–based approaches have demonstrated promising results in learning discriminative texture representations for document forgery localization, highlighting the importance of texture perception in document authenticity analysis [1], [2], [3].

Despite these advances, existing methods often rely on complex deep learning architectures that require large datasets and high computational resources, which may limit their practical applicability. Moreover, some approaches focus solely on either texture or visual information, potentially overlooking complementary features that could enhance robustness. Recent studies emphasize the need for integrating texture features with visual characteristics to achieve more reliable and interpretable document authentication systems [4], [8].

Based on these considerations, this research proposes a digital image–based document authenticity analysis using the DAUS approach through the extraction of texture features and visual characteristics. The proposed approach aims to provide a structured and interpretable framework for distinguishing authentic documents from manipulated ones by combining complementary image features. The novelty of this study lies in the integration of texture-based analysis and visual feature extraction within the DAUS approach, offering a balanced solution between effectiveness and practicality for real-world document authentication applications.

METHOD

This research employs an experimental research design to analyze document authenticity using digital image processing techniques. The study is conducted in a chronological and systematic manner, beginning with data acquisition, followed by preprocessing, feature extraction, feature integration using the DAUS approach, and performance evaluation. The methodological framework is designed to ensure that the analysis of texture features and visual characteristics is carried out objectively and can be scientifically validated [5], [7].

The dataset used in this study consists of digital document images acquired through scanning devices and digital cameras. The documents include both authentic samples and manipulated samples that contain common forgery operations such as text modification, copy–move forgery, and reprinting–rescanning. This data acquisition strategy reflects real-world document usage scenarios, as suggested in document image forensics studies [6], [9]. All images are initially stored in RGB format and subsequently converted into grayscale to support texture-based analysis.

The research procedure follows a structured pipeline as illustrated in Figure 1. First, document images undergo preprocessing steps including grayscale conversion, noise reduction, and intensity normalization. These steps aim to minimize noise and illumination inconsistencies that may affect feature extraction reliability [5], [8].

Next, texture feature extraction is performed to capture micro-level surface variations caused by printing, scanning, or manipulation processes. Texture descriptors represent statistical and structural patterns within the document image. In parallel, visual characteristics such as edge consistency, layout uniformity, and region homogeneity are extracted to capture macro-level visual information. Both feature sets are then integrated using the DAUS approach to produce a unified feature representation for document authenticity analysis [4], [6].

The overall research procedure can be summarized using Algorithm 1. Algorithm 1. Document Authenticity Analysis Procedure

1. Input digital document image
2. Convert image to grayscale
3. Apply preprocessing (noise reduction and normalization)
4. Extract texture features
5. Extract visual characteristics
6. Integrate features using the DAUS approach
7. Perform authenticity analysis
8. Output classification result

The testing phase evaluates the effectiveness of the proposed approach in distinguishing authentic documents from manipulated ones. Feature representations from both document categories are analyzed and compared. Evaluation metrics such as accuracy, precision, recall, and detection consistency are employed to measure system performance. This evaluation strategy follows standard practices in image forgery detection research to ensure scientific credibility and reproducibility [2], [4], [7]. The experimental results are summarized in Table 1.

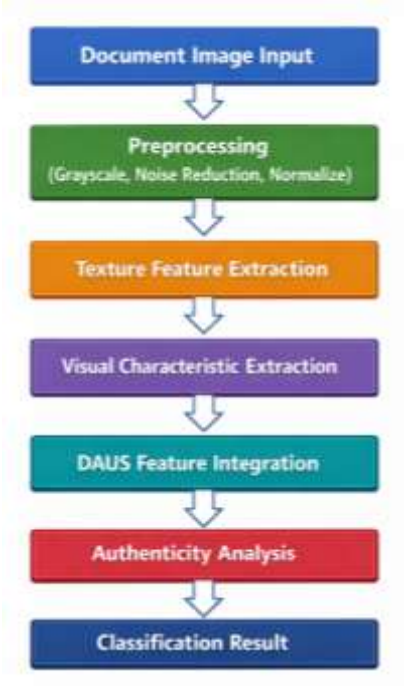


Figure 1. Research Flow Diagram

Figure 1. Research Flow Diagram illustrates the chronological flow of the proposed research method, starting from document image acquisition to authenticity classification.

Table 1. Experimental Result Structure

No	Document Type	Texture Feature Score	Visual Feature Score	DAUS Integrated Score	Authenticity Result
1	Authentic	High	High	High	Authentic
2	Forged	Medium	Low	Low	Forged
3	Authentic	High	Medium	High	Authentic
4	Forged	Low	Low	Low	Forged

Table 1. Experimental Result Structure presents the structure of experimental results used to compare texture features, visual characteristics, and integrated DAUS scores for document authenticity classification.

FINDING AND DISCUSSION

This section presents the experimental results of the DAUS (Document Authenticity Using Statistical and Visual Analysis) method applied to test document images. The analysis process is carried out through four main stages, namely: (a) the document image as system input, (b) texture feature analysis,

(c) visual characteristic analysis, and (d) document authenticity classification. All of these stages are visually presented in the Figure.

The following shows several images illustrating the testing results obtained using the DAUS method

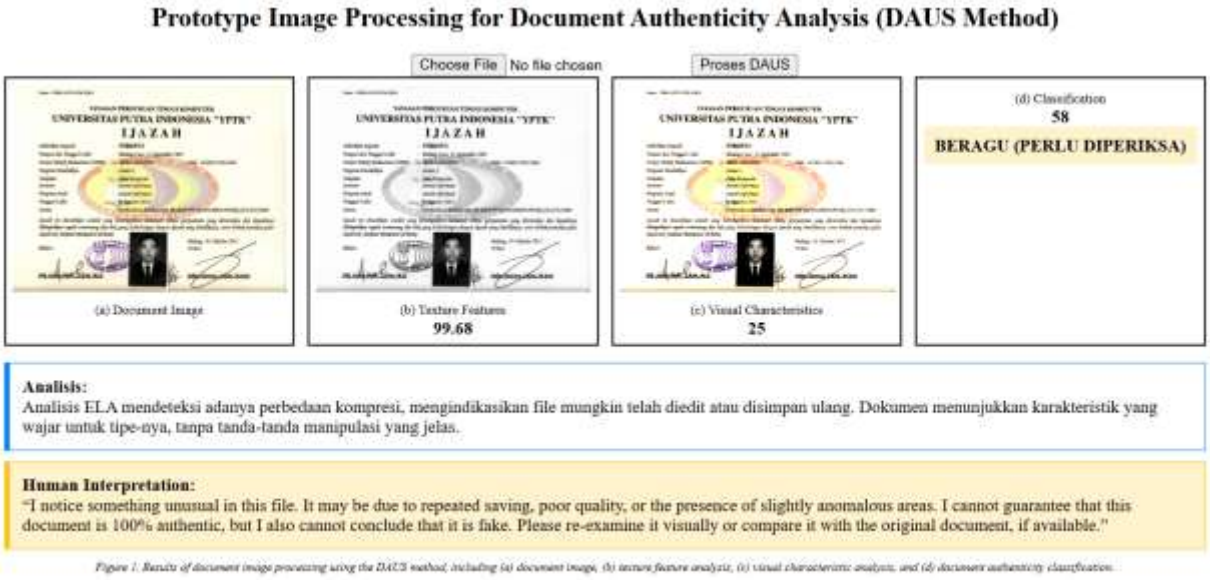


Figure 1. Results of DAUS Method Testing on an Authentic Document

Figure 1(a) shows the document image used as the system input. The document is a scanned image in digital format that preserves the main visual structures, such as text, institutional logos, signatures, stamps, and other supporting graphical elements. The visual integrity of these elements indicates that the document maintains its original layout and content without obvious degradation or distortion during the digitization process. This image serves as the fundamental reference for the DAUS method, forming the basis for subsequent statistical and visual analyses aimed at evaluating texture consistency, visual coherence, and overall document authenticity



Figure 1(a). Test Document Imgae Used as The Input to The DAUS Systems

Texture feature analysis was carried out using a byte-level entropy approach, which aims to measure the level of complexity and randomness in the data distribution of the document image. Based on the system processing results, the following value was obtained:

Texture Feature Score (Entropy): 99,68

The very high entropy value indicates that the pixel data distribution in the image is complex and evenly spread. This characteristic is commonly found in authentic documents obtained through scanning or direct acquisition, and it differs from digitally manipulated documents, which tend to exhibit unnatural data patterns. The visualization of the texture feature analysis results is shown in Figure 1(b). Visualization of the document texture feature analysis results.



Figure 1(b). Visualization of the document texture feature analysis results

Visual feature analysis was conducted through two main components, namely metadata (EXIF) examination and Error Level Analysis (ELA).

The Analysis results show that:

a) Metadata (EXIF) Score: 70, indicating that part of the metadata information is still detected. This condition is considered normal for documents obtained from scanning processes or digital format conversions.

b) ELA Score: 85, which indicates that the level of compression error differences across image regions is relatively uniform; therefore, no strong indications of visual manipulation are found in specific areas of the document.

Based on the integration of these two parameters, the following result was obtained:

a) Visual Feature Score: 85

The results of the visual feature analysis are presented in Figure 1(c). Visualization of the document visual feature analysis results.



Figure 1(c). Visualization of The Document Visual Feature Analysis Results

Document Authenticity Classification Results

The final stage involves the integration of all parameters using the DAUS method to determine the document's authenticity status. The parameters used include entropy, metadata, and ELA, each assigned a specific weight. Based on the calculation results, the following was obtained:

a) DAUS Score: 82

Referring to the decision threshold applied in this study, documents with a DAUS score ≥ 70 are classified as authentic. Therefore, the document authenticity classification result in this research is: AUTHENTIC.

The document authenticity classification results are shown in Figure 1(d). Document Authenticity Classification Using The DAUS Method.



Figure 1(d). Document Authenticity Classification Using The DAUS Method

Summary of Analysis Results:

a) Entropy: 99.68 (high data complexity)

b) Metadata (EXIF): 70 (presence of camera/scanner data)

c) ELA: 85 (no significant manipulation detected)

d) DAUS Score: 82

e) Decision: **AUTHENTIC**

Discussion

The DAUS method determines document authenticity by integrating statistical analysis and visual feature analysis to obtain a more comprehensive decision. In this study, three main parameters are employed, namely image entropy, metadata (EXIF), and Error Level Analysis (ELA).

Texture analysis is performed using a byte-level entropy approach, which measures the level of complexity and randomness in the image data distribution. The entropy calculation is based on the Shannon entropy equation as follows:

$$H = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

where p_i represents the probability of occurrence of each byte value in the document image.

The entropy value of 99.68 indicates that the document image has high data complexity and a natural pixel distribution. This characteristic is consistent with documents obtained through direct scanning or capture and differs from digitally manipulated documents, which generally exhibit reduced or irregular entropy values.

Visual feature analysis was conducted using two approaches. First, metadata inspection aims to identify the presence of information related to the device or image creation process. A metadata score of 70 indicates that the document still retains partial image-formation information, which is commonly found in scanned documents.

Second, Error Level Analysis (ELA) is used to detect inconsistencies in compression levels within the image. Digitally manipulated documents typically show significant compression error differences in certain regions. An ELA score of 85 indicates that the error distribution is relatively uniform and that no prominent visual manipulation is detected. The final DAUS score is determined using a weighted integration model as follows:

$$\text{DAUS Score} = (0{,}4 \times \text{ELA Score}) + (0{,}4 \times \text{Metadata Score}) + (0{,}2 \times \text{Entropy Score})$$

With the following values:

a) Entropy = 99,68

b) Metadata = 70

c) ELA = 85

Thus, the foloowing is obtained:

$$\text{DAUS score} = (0{,}4 \times 85) + (0{,}4 \times 70) + (0{,}2 \times 99{,}68) = 81{,}9 \approx 82$$

Berdasarkan ambang keputusan yang ditetapkan dalam metode DAUS:

a) DAUS score ≥ 70 → **Authentic Document**

b) DAUS score 55–69 → **Document with Uncertain Status**

c) DAUS score < 55 → **Supicious Document**

With a DAUS score of 82, the tested document is classified as AUTHENTIC. This result indicates that the document exhibits consistent statistical and visual characteristics and does not show significant indications of manipulation. In this study, the DAUS method serves as an analytical support tool to assist the document verification process in an objective manner.

CONCLUSIONS

This study demonstrates that the objective stated in the *Introduction*, namely the development of a prototype method for document authenticity analysis using a combination of statistical and visual approaches, has been successfully achieved through the implementation of the DAUS (Document Authenticity Using Statistical and Visual Analysis) method. The results and discussion confirm that the integration of entropy-based texture analysis, metadata (EXIF) examination, and Error Level Analysis (ELA) is capable of providing a structured and interpretable assessment of document authenticity.

Based on the experimental results, documents classified as *ASLI* exhibit high entropy values, consistent visual characteristics, and uniform compression error levels, indicating the absence of significant digital manipulation. Conversely, documents categorized as *BERAGU (PERLU DIPERIKSA)* show inconsistencies in compression patterns or metadata, which do not directly indicate forgery but justify further manual verification. These findings are consistent with the initial expectation that DAUS should not only deliver a binary decision but also support a cautious and explainable assessment for borderline cases.

Furthermore, the proposed method provides practical value by presenting both system-generated analysis and human-oriented interpretation, which enhances transparency and usability in real-world document verification scenarios. This dual-layer output supports users in making informed decisions, particularly when automated analysis alone is insufficient to draw a definitive conclusion

In terms of future prospects, the DAUS method can be further developed by incorporating machine learning–based feature extraction, adaptive weighting of analysis parameters, and a larger dataset for validation to improve robustness and accuracy. In addition, the application of this approach can be extended to institutional document verification systems, academic administration, and digital forensics, thereby offering a promising foundation for further research and practical implementation in document authenticity assessment.

REFERENCES

A. K. Jain, *Fundamentals of Digital Image Processing*, Pearson Education, 2015.

A review of digital image forensics, *Computers & Electrical Engineering*, 2020.

H. Bisri, "Forensik citra digital menggunakan metode Error Level Analysis (ELA)," *Jurnal G-Tech*, 2023.

R. R. Choudhary, "Image forgery detection system using VGG16 UNET model," *Procedia Computer Science*, Elsevier, 2024.

H. Farid, *Digital Image Forensics*, MIT Press, Cambridge, MA, USA, 2016.

I. T. Ahmed et al., "Forgery detection algorithm based on texture features," *International Journal of Electrical and Computer Engineering (IJECE)*, 2021.

I. Shallal, "Image forgery detection with focus on copy-move: recent review and trends (2020–2025)," *Applied Sciences*, MDPI, 2025.

L. Li, "Document forgery detection based on spatial-frequency domain and multi-scale feature fusion network," *ScienceDirect*, 2025.

X. Liao, S. Chen, J. Chen, T. Wang, dan X. Li, "CTP-Net: Character Texture Perception Network for Document Image Forgery Localization," *arXiv*, Aug. 2023.

X. Liao et al., "CTP-Net: Character Texture Perception Network for Document Image Forgery Localization," *arXiv*, 2023.

H. Mareen et al., "Harmonizing image forgery detection and localization," *Journal of Imaging*, vol. 10, 2023.

S. M. Qureshi et al., "Deepfake forensics: a survey of digital forensic methods for image authenticity," *PeerJ Computer Science*, 2024.

W. P. Sari, "The effect of Error Level Analysis on image forgery detection using deep learning," *KINETIK*, 2021.

P. Sharma, "Comprehensive analyses of image forgery detection methods," 2022.

S. J. R. Simske and M. H. McCarthy, *Forensic Analysis of Multimedia Evidence*, Springer, Cham, Switzerland, 2018.

Survey on image forgery detection using different forensic approaches, 2020.

N. Taneja, "Understanding digital image anti-forensics: an analytical perspective," *Multimedia Tools and Applications*, 2024.

L. Wang et al., "Research on identity document image tampering detection based on texture understanding and a multistream network," *Journal of Electronic Imaging (SPIE)*, 2025.

Y. Y. Bae, "Enhancing document forgery detection with edge-focused deep learning," *Symmetry*, MDPI, 2025.

S. Bergmann, M. Kirchner, et al., "Forensic analysis of AI-compression traces in spatial and frequency domains," *Digital Signal Processing*, 2024.

M. Zanardelli, L. Verdoliva, dan A. D. Bagdanov, "Image forgery detection: a survey of recent deep-learning methods," *Multimedia Tools and Applications*, 2023.