

---

# CAN MULTI-MODAL (REASONING) LLMs DETECT DOCUMENT MANIPULATION?

---

Zisheng Liang<sup>\*1</sup>, Kidus Zewde<sup>\*2</sup>, Rudra Pratap Singh<sup>\*3</sup>, Disha Patil<sup>\*3</sup>, Zexi Chen<sup>\*4</sup>, Jiayu Xue<sup>\*5</sup>, Yao Yao<sup>\*6</sup>, Yifei Chen<sup>\*7</sup>, Qinzhe Liu<sup>\*8</sup>, and Simiao Ren<sup>\*2</sup>

<sup>1</sup>Duke University, zisheng.liang@duke.edu

<sup>2</sup>Scam.ai, kidus.zewde@scam.ai

<sup>3</sup>Indian Institute of Technology, Roorkee, p\_dchetan/r\_psingh@ma.iitr.ac.in

<sup>4</sup>New York University, zc2610@nyu.edu

<sup>6</sup>University of Wisconsin Madison, yyao39/xzhan23@wisc.edu

<sup>5</sup>University of North Carolina at Chapel Hill xuejiayu@ad.unc.edu

<sup>7</sup>Columbia University, yc3503@columbia.edu

<sup>8</sup>qinzhe1126@gmail.com

August 18, 2025

## ABSTRACT

Document fraud poses a significant threat to industries reliant on secure and verifiable documentation, necessitating robust detection mechanisms. This study investigates the efficacy of state-of-the-art multi-modal large language models (LLMs), including OpenAI O1/4o, Gemini Flash (thinking), Deepseek Janus, Grok, Llama 3.2 / 4, Qwen 2/2.5 VL, Mistral Pixtral, and Claude 3.5/3.7 Sonnet, in detecting fraudulent documents. We benchmark these models against each other and prior work on document fraud detection techniques using a standard dataset with real transactional document. Through prompt optimization and detailed analysis of the models' reasoning processes, we evaluate their ability to identify subtle indicators of fraud, such as tampered text, misaligned formatting, and inconsistent transactional sum. Our results reveal that top-performing multi-modal LLMs demonstrate superior zero-shot generalization, outperforming conventional methods on out-of-distribution datasets, while several vision LLMs exhibit inconsistent or subpar performance. Notably, model size and advanced reasoning capabilities show limited correlation with detection accuracy, suggesting task-specific fine-tuning is critical. This study underscores the potential of multi-modal LLMs in enhancing document fraud detection systems and provides a foundation for future research into interpretable and scalable fraud mitigation strategies.

## 1 INTRODUCTION

The emergence of artificial intelligence has yielded significant advancements across various domains, from material design [1], energy infrastructure [2] to deepfake detection [3]. However, the rapid advancement of generative models has facilitated the creation of highly convincing forged documents, such as receipts, posing serious risks to financial integrity, legal authenticity, and institutional trust. Traditional forgery detection methods often rely on rule-based systems or convolutional neural networks (CNNs) to identify inconsistencies in document features [4, 5, 6, 7, 8, 9]. Such methods have been extensively surveyed in the literature on image forgery detection [10, 11]. Yet, as forgery techniques become more sophisticated, these methods struggle to generalize, particularly when encountering novel manipulations not present in training data.

---

<sup>†‡</sup> Correspondence author.

<sup>\*\*</sup> Equal contributions, order randomly generated.

Recent developments in multi-modal large language models (LLMs) have showcased their ability to process and reason across multiple data modalities, including text and images. Models like GPT-4V and Gemini, with their extensive pretraining corpora and emergent reasoning capabilities, are promising tools for detecting forged documents. Unlike traditional methods, multi-modal LLMs can leverage contextual understanding, analyze visual and textual document features, and adapt to previously unseen forgery patterns.

In this study, we systematically evaluate the effectiveness of multi-modal LLMs for detecting forged receipts using the "FindIt Again" dataset, which contains a diverse collection of forged and authentic receipts. We benchmark several state-of-the-art (SOTA) models to assess their generalization capabilities across this dataset. Additionally, we perform ablation studies and probe their reasoning processes to uncover the key factors influencing their decision-making. Our analysis provides insights into how these models reason about forged documents, highlighting their interpretability and limitations.

Our contributions are threefold:

- Benchmarking SOTA Multi-Modal LLMs on document forgery detection: We evaluate the performance of leading multi-modal LLMs against traditional forgery detection methods on the "FindIt Again" [12] dataset, marking the first comprehensive study of reasoning multi-modal LLMs in this context.
- Ablation studies into their reasoning capabilities & Interpretability: We investigate the reasoning steps employed by multi-modal LLMs, identifying critical features and logical pathways that drive their forgery detection decisions.
- Our findings demonstrate that SOTA multi-modal LLMs exhibit robust generalization and competitive performance compared to traditional detection approaches. This study offers valuable insights into the role of reasoning in document forgery detection and establishes a foundation for future research into reliable, interpretable, and generalized detection systems.

## 2 Related work

### 2.1 Machine learning for Document forgery analysis

The detection of document forgeries has evolved significantly with the advent of machine learning (ML) and deep learning (DL) techniques. More recently, specialized DL-based methods for document image forgery detection have been proposed, including spatial-frequency and multi-scale feature networks [13], multiscale edge similarity analysis [14], and log-transform histogram equalization techniques [15]. Unsupervised approaches leveraging deep feature clustering have also shown promise for forged document classification [16]. Additionally, methods exploiting RGB channel inconsistencies [17] and CNN architectures tailored to administrative documents have achieved strong performance [18].

### 2.2 Datasets for Imagery forgery detection

While the broader field of image forgery has been more widely investigated, as shown in Table 1, the topic of document forgery has gained significantly less traction. To date, only one dataset specifically focused on ID document copy-move forgeries has been introduced [19]. Given the scarcity of dedicated benchmarks, we evaluate our model performance on the publicly available RDDFD ("Receipt dataset for document forgery detection") dataset. Notably, a similar dataset in a Japanese context was constructed by Okamoto et al., though it is not publicly accessible [20].

### 2.3 State of the Art Multi-Modal LLMs: Capabilities and Advances

We list the SOTA LLMs that we benchmark in Table 2, including their MMMU benchmark scores and publication dates. At the time of writing, several of these models' APIs have only recently become available, enabling novel contributions to this field.

## 3 Methodology

This study addresses the problem of receipt forgery detection comparing SOTA LLMs with traditional methods like CNN and SVM which provide a baseline as stated in [12].

Table 1: Public Datasets for Forgery image Detection

Dataset	#images	Image Type	Forgery Type
FID [21]	4k	General-purpose images from public repositories	Cut-paste, copy-move, erase-filling
<b>CG-1050</b> [22]	1k	Indoor and outdoor scenes (e.g., streets, parks, malls)	Copy-move, cut-paste, retouching, colorizing
<b>MIDV-2020</b> [23]	74.4k	Synthetic identity documents with unique text fields and artificially generated faces	Simulated identity documents for tasks like text field recognition and face detection
<b>ForgeryNet</b> [24]	3M	Faces and general scenes	Various, including identity-replaced and identity-retained forgeries
<b>DF2023</b> [25]	1M	Various, including manipulated images from online social networks	Splicing, copy-move, enhancement, removal
<b>CASIA v2.0</b> [26]	4.8K	Natural scenes, objects, people	Splicing, copy-move
<b>MICC-F220</b> [4]	220	Natural scenes	Copy-move
<b>CoMoFoD</b> [27]	260	Various scenes	Copy-move with transformations (translation, rotation, scaling, distortion)
<b>RDDFD</b> [12]	1K	Retail receipts	Not explicitly focused on forgery; primarily for OCR and information extraction tasks

Table 2: Comparative Vision Performance of Multi-Modal LLMs

Publisher	Model Version	MMMU (%)	VQA v2 Acc (%)
OpenAI	GPT-4o	69.1	85.3
	GPT-o1	78.2	N/A
Meta	Llama 3.2	71.3	78.1
	Gemini 2	68.5	84.5
Google	Gemini 2 Thinking	75.4	N/A
	Qwen 2 VL	45.2	N/A
Alibaba	Qwen 2.5 VL	70.3	N/A
	Claude 3.5 Haiku	50.2	N/A
Anthropic	Claude 3.7 Sonnet	71.8	N/A
	Janus-Pro 1B	36.3	N/A
Deepseek	Janus-Pro 7B	41.0	N/A
	Pixtral	52.5	N/A

### 3.1 SVM-Based Approach

Each receipt image was preprocessed by resizing to  $250 \times 250$  pixels to ensure uniform input dimensions. Pixel intensities were normalized using the standard mean and standard deviation values derived from the ImageNet dataset. The metadata files were parsed to assign binary labels (authentic or forged) to each image, ensuring that corrupted or unreadable files were excluded from further processing.

For the SVM-based approach, the resized images were flattened into one-dimensional feature vectors. These vectors were standardized using z-score normalization to ensure consistent scaling across features. A linear-kernel Support Vector Machine was trained on the extracted features, with class weights adjusted to mitigate class imbalance in accordance with the method used in [12]. Further, grid search was used to experiment with different 'kernel', 'gamma', 'c' and 'class weight' parameters to find best model that does not overfit.

### 3.2 CNN-Based Approach

the method is a deep learning approach (CNN) applied on OH-JPEG/OH-JPEG+PQL features for detecting document forgeries mentioned in [12].

The OH-JPEG method utilizes a one-hot encoding of the DCT (Discrete Cosines Transformed) coefficients of JPEG images to capture spatial and frequency patterns in JPEG images. The methods work by transforming each 128x128 pixel block into DCT coefficients, where low frequencies (top-left of DCT block) represent basic structure and high frequencies (bottom-right) represent fine details, allowing the network to learn both obvious manipulations through structural changes and subtle forgeries through compression artifacts.

while OH-JPEG+PQL enhances this by incorporating PQL that multiplies features with the image's quantization matrix to capture compression artifacts and quality inconsistencies.

The Parity Quantization layer (PQL) enhancement makes the system particularly robust for real-world document forensics as it can detect various forgery types, e.g copy and paste inside/outside the document, as mentioned in [12]) by analyzing both content and compression characteristics, with the quantization information helping identify even subtle manipulations that maintain visual consistency but leave traces in compression patterns. The methods are particularly effective for document forgery detection because they analyze both structural changes (through Discrete Cosine Transform(DCT) coefficients) and compression characteristics (through PQL), making them suitable for detecting copy-paste operations (by identifying repeated DCT patterns), text imitation (through compression inconsistencies), and pixel modifications (via local pattern disruptions).

After extracting features, The CNN-based model utilized a lightweight convolutional neural network architecture composed of sequential convolutional layers with ReLU activations and pooling layers, followed by fully connected layers for binary classification. The network was trained using the cross-entropy loss function optimized with the Adam optimizer. Evaluation was performed at the end of each epoch on the test datasets.

### 3.3 LLM Approach

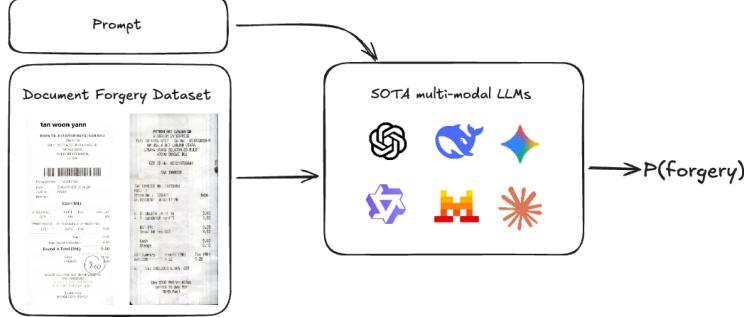


Figure 1: Overall Experiment Design

This section outlines the methodology employed to investigate the efficacy of state-of-the-art (SOTA) LLMs in detecting document forgery images using a structured pipeline, as depicted in the provided diagram Fig. 1. The pipeline leverages the find-it-2 datasets, processes them through SOTA multi-modal LLMs with tailored prompts, and generates a probability of an image being forgery, denoted as  $P(\text{forgery})$  in a zero-shot manner.

#### 3.3.1 Prompt Engineering and Input to SOTA Multi-Modal LLMs

The preprocessed images from the fake receipt datasets are fed into a suite of SOTA multi-modal LLMs, which are capable of processing both visual and textual data. The input process is guided by carefully crafted prompts designed to

elicit reasoning and classification capabilities from the models. The prompt, as indicated in the diagram, directs the LLMs to analyze the input images and determine their authenticity. After some iterations we landed on the final prompt, shown in Appendix. Each model receives the same prompt, ensuring consistency across evaluations.

## 4 Results

### 4.1 Evaluation and Analysis

To assess the performance of the pipeline, the P(forgery) scores generated by each SOTA multi-modal LLM are benchmarked against ground truth labels from the document forgery datasets. Since language models does not necessarily returns structured outputs, we process the output with string processors to extract the numeric answer of the model. Note that this process does not guarantee full recovery of the prediction score, combined with a small probability that LLMs refuse to give a numeric estimation or just fails to reply. We omit those examples in our result calculation.

For the evaluation metrics, we use the ROC curves with area under the receiver operating characteristic curve (AUC). Additionally, an in-depth analysis of the reasoning pathways is conducted to identify the key contributing factors.

To further understand and benchmark whether the LLMs can perform, we benchmarked traditional SVM and Computer Vision models that were in prior publications.

Given the potential class imbalance between authentic and forged receipts, particular attention was given to the AUC score to ensure balanced performance across both classes.

### 4.2 SVM and CNN Performance

On the one hand, SVM performed poorly with f1 score of **0.18** without hypertuning. The best model found after gridsearch did some effort of reducing overfitting, and the f1 score for that was found to be **0.24**. The best model however gives AUC of **0.48**, which is even worse than random guessing. The first CNN model described in [12] gave best f1 score of **0.69** on test dataset , but its confusion matrix shows the model has overfitted and predicted everything as forged. We tried more adjustments like adjusting classification thresholds and increasing weights of minority classes, but the model ended up overfitting and marking all documents as forged. A similar thing happened on using ResNet50 pretrained model, because its architecture becomes too complex for this task.

On the other hand, while the original paper[12] claimed a 0.79 precision on OH-JPEG model and 0.78 precision on OH-JPEG/PQL, which we reproducued(OH-JPEG: 0.80 F1 score, and 0.71 precision, and the OH-JPEG-PQL variant similarly delivers strong performance with 0.74 F1, 0.77 precision). These results are on patch level, which a forged image contribute a forged patch and two pristine patches, according to the paper[12]. To get the performance on image level, which is more intuitive on inference, when aggregate predictions for each image (use OR logic to determine if any crop is forged). At image-level aggregation, although we have matched the reported performance in F1 scores with previous publication, we found the AUROC of the detection performance of such traditional method is actually around 0.5, show casing strong gap in the reporting metric from previous work.

### 4.3 LLM Performances

In this section, we show the performance results on different LLMs and discuss the following questions. and analysis the performance on GPT-O1 because it has the best performance on this task.

#### 4.3.1 Is Document Forgery Detection a Simple Task for LLMs?

For most of the LLMs, the AUC scores are close to 0.5, which is a random guess. among which, GPT-O1 is the top performer with a 0.71 AUC score. All ROC curves are shown in Figure2 and Table. 3 summarizes the AUC scores of LLMs.

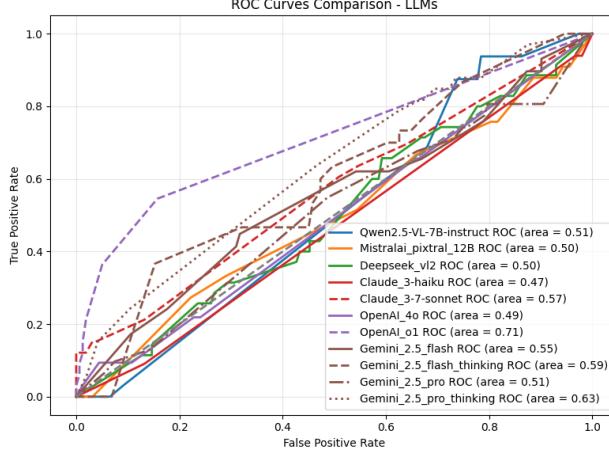


Figure 2: ROC curves showing LLM performance on document forgery detection.

Model	AUC
<b>GPT-O1</b>	<b>0.71</b>
GPT-4o	0.49
<b>Gemini-2.5-Pro-Think</b>	<b>0.63</b>
Gemini-2.5-Flash-Think	0.59
Llama-4	0.60
<b>Claude-3.7</b>	<b>0.57</b>
Claude-3-Haiku	0.47
Qwen2.5-VL-7B-Instruct	0.51
Pixtral-12B-2409	0.50
Deepseek-v12	0.50
SVM	0.49
CNN (OH-JPEG)	0.51
Baseline (random)	0.50

Table 3: AUC scores of all models.

### 4.3.2 Does Model Improvement Generalize to Document Forgery Detection?

We conducted a comparative analysis between the GPT series and Claude series models. Our findings demonstrate that the latest model releases exhibit superior performance in detecting document forgeries compared to their predecessors. The results presented in Table. 3

### 4.3.3 Does Model Size Correlate with Performance?

We conducted an investigation into three mid-sized LLMs (<12B) on the Document forgery detection task. Our findings demonstrate that Document forgery detection presents a formidable challenge for widely adopted mid-sized language models (LLMs). Notably, all AUC scores obtained were approximately 0.5. The results presented in Table. 3

#### 4.3.4 Do Reasoning Models Perform Better?

We conducted an experiment on the latest Gemini-2.5 model series. This version of Gemini enables the control of reasoning through a reasoning-token-length variable. In the non-thinking experiment, we explicitly set the reasoning-token-length to zero. Our findings demonstrate that reasoning enhances the model’s performance on this task, as presented in Table. 4

Model	w/o Thinking	w/ Thinking
Gemini-2.5-Flash	0.55	0.59
Gemini-2.5-Pro	0.51	0.63

Table 4: AUC scores for Gemini-2.5 variants w/ and w/o thinking.

#### 4.3.5 Performance Analysis of GPT-O1

GPT-O1 is the top performer among all LLMs on this test. This part details the performance analysis of GPT-O1 evaluated in this study, focusing on its reasoning capabilities, and specific strengths and weaknesses in detecting document fraud within the benchmark dataset (218 receipt images compared against `test.txt` ground truth).

GPT-O1 demonstrated a moderate overall performance, achieving an accuracy rate of **83.85%**, correctly classifying 161 out of 192 samples (31 incorrect determinations). The model showcased impressive capabilities in:

- **Mathematical Verification:** Excelling at detecting incorrect line totals, subtotals, flawed Goods and Services Tax (GST) calculations, and incorrect change amounts.
- **Contextual and Temporal Logic:** Successfully identifying inconsistencies related to dates (e.g., transaction time vs. closing time) and historically accurate tax rates (e.g., applying correct GST percentages based on the transaction date).
- **Content Consistency:** Reliably flagging conflicting information within the document, such as discrepancies between merchant names or addresses in the header versus the footer.
- **Visual Anomaly Detection:** Identifying clearly suspicious visual elements like deliberately obscured values or significant font mismatches in critical areas.
- **Detailed Reasoning:** Providing clear, specific, and logically structured justifications for its determinations.

Confidence calibration revealed that GPT-O1 expresses its predictions with generally low probability scores, indicating cautious but underconfident behavior (see Figure 3). True Negatives (pristine) overwhelmingly received scores clustered around 0.02–0.05, and True Positives (forged) were similarly distributed at 0.05–0.15. Only a handful of cases—namely the 2 false positives and a few true positives—spiked above 0.8, accounting for the rare overconfident peaks in the histogram. Critically, the 29 false negatives lie almost entirely in the lowest bin (<0.05), demonstrating extreme underconfidence when missing forged samples. This mismatch between score magnitude and correctness highlights calibration issues: GPT-O1 seldom expresses strong confidence even for correct predictions, while its infrequent overconfident errors could mislead any fixed-threshold decision rule.

The primary weaknesses leading to the 31 errors were:

- **False Positives (2 cases):** The most common error type. The model tended to flag legitimate receipts as fraudulent primarily due to conflicting merchant information (e.g., HQ address vs. branch location) which the ground truth considered acceptable, or minor calculation/rounding differences deemed suspicious by the model but legitimate according to the label.
- **False Negatives (29 cases):** Less frequent but notable. The model occasionally missed subtle calculation errors or showed over-reliance on internal mathematical consistency, potentially overlooking other red flags if the (flawed) numbers added up correctly.

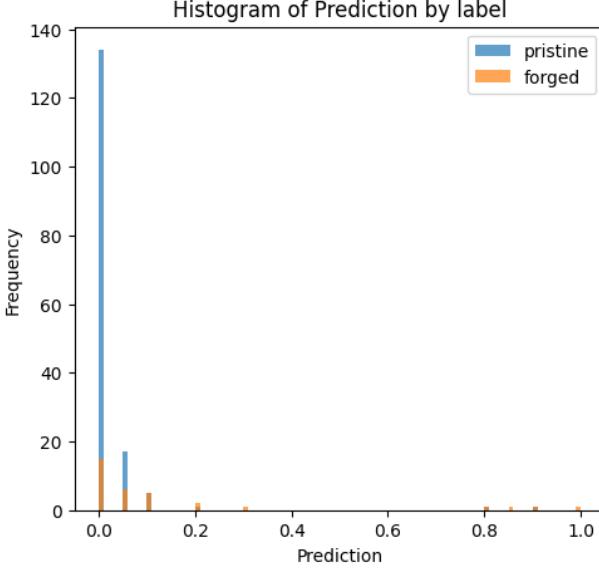


Figure 3: Histogram of predicted probabilities by true label.

Overall, GPT-O1 displayed advanced analytical capabilities suitable for detailed document verification, with its main deviation from the ground truth stemming from a stricter interpretation of certain inconsistencies like header/footer discrepancies.

#### 4.3.6 Do Models Hallucinate on Forgery Detection?

In our experiments, all LLMs demonstrated difficulties in differentiating fraudulent document images from legitimate document images. Details (histogram figures) are shown in the Appendix. The histogramgram figure shows that even the top-performing GPT-o1 model cannot classify fraudulent images effectively. These findings suggest the inherent difficulty of the task and the necessity of employing a specially trained model for this purpose.

#### 4.4 LLMs compared with traditional computer vision solutions

By comparing the performance of traditional models, SVM and CNN, that were trained on the tasks with zero-shot performance with the top performing LLMs. We can see that both conventional models and the best LLMs are struggling on this document forgery task. under zero-shot settings (we hypothesize given document forgery detection is too niche, LLMs are very unlikely to have been trained specifically on this task), the best LLMs show limited ability to classify document forgery, and the traditional models consistently performs around random guessing.

## 5 Conclusions

This study demonstrates that state-of-the-art multi-modal large language models (LLMs) with reasoning capabilities offer moderate potential for document forgery detection, achieving competitive performance and notable generalization compared to traditional methods. Our benchmarking reveals that while model size can enhance performance, as seen with GPT series consistent improvements, newer model versions and reasoning-augmented approaches translate to limited outcomes in this niche task (e.g Gemin-2.5-Flash and Pro), with some models (e.g.Qwen, Pixtral and reasoning variants) performing near or below random guessing. OpenAI's LLMs stood out, surpassing traditional svm and

computer vision models in zero-shot generalization, though they remain outperformed by specialized networks on datasets these were trained on. Additionally, our analysis suggests that poor performance is not solely attributable to numerical output limitations, as categorical prompting yielded similar results. These findings underscore the value of integrating multi-modal reasoning into deepfake detection frameworks while highlighting the need for further exploration into failure modes and model hallucination to enhance robustness and interpretability in real-world applications.

## References

- [1] O. Khatib, S. Ren, J. Malof, and W. J. Padilla, “Deep learning the electromagnetic properties of metamaterials—a comprehensive review,” *Advanced Functional Materials*, vol. 31, no. 31, p. 2101748, 2021.
- [2] S. Ren, W. Hu, K. Bradbury, D. Harrison-Atlas, L. M. Valeri, B. Murray, and J. M. Malof, “Automated extraction of energy systems information from remotely sensed data: A review and analysis,” *Applied Energy*, vol. 326, p. 119876, 2022.
- [3] S. Ren, Y. Yao, K. Zewde, Z. Liang, N.-Y. Cheng, X. Zhan, Q. Liu, Y. Chen, H. Xu, *et al.*, “Can multi-modal (reasoning) llms work as deepfake detectors?,” *arXiv preprint arXiv:2503.20084*, 2025.
- [4] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy–move attack detection and transformation recovery,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.
- [5] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012.
- [6] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,” in *Proceedings of the Digital Forensic Research Workshop (DFRWS)*, pp. 19–23, 2003.
- [7] X. Pan, X. Zhang, and S. Lyu, “Exposing image splicing with inconsistent local noise variances,” in *2012 IEEE International Conference on Computational Photography (ICCP)*, pp. 1–10, IEEE, 2012.
- [8] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” in *Security, Steganography, and Watermarking of Multimedia Contents VI, Proc. SPIE*, vol. 5306, pp. 55–65, SPIE, 2004.
- [9] S. Teerakanok and T. Uehara, “Copy-move forgery detection: a state-of-the-art technical review and analysis,” *IEEE Access*, vol. 7, pp. 40550–40568, 2019.
- [10] P. Sharma, M. Kumar, and H. Sharma, “Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation,” *Multimedia Tools and Applications*, vol. 82, no. 12, pp. 18117–18150, 2023.
- [11] M. Zanardelli, F. Guerrini, R. Leonardi, and N. Adami, “Image forgery detection: a survey of recent deep-learning approaches,” *Multimedia Tools and Applications*, vol. 82, pp. 17521–17566, 2023.
- [12] B. M. Tornés, T. Taburet, E. Boros, K. Rouis, A. Doucet, P. Gomez-Krämer, N. Sidere, and V. P. d’Andecy, “Receipt dataset for document forgery detection,” in *International Conference on Document Analysis and Recognition*, pp. 454–469, Springer, 2023.
- [13] L. Li, Y. Bai, S. Zhang, and M. Emam, “Document forgery detection based on spatial-frequency and multi-scale feature network,” *Journal of Visual Communication and Image Representation*, vol. 107, p. 104393, 2025.
- [14] F. Sun, L. Sun, and J. Wang, “Document image forgery detection based on multiscale edge similarity,” in *International Conference on Image Processing and Artificial Intelligence (ICIPAI)*, vol. 13213 of *Proceedings of SPIE*, p. 132132S, SPIE, 2024.
- [15] Y.-Y. Bae, D.-J. Cho, and K.-H. Jung, “A new log-transform histogram equalization technique for deep learning-based document forgery detection,” *Symmetry*, vol. 17, p. 395, 2025.

- [16] P. Tyagi, K. Agarwal, G. Jaiswal, A. Sharma, and R. Rani, “Forged document detection and writer identification through unsupervised deep learning approach,” *Multimedia Tools and Applications*, vol. 83, pp. 18459–18478, 2024.
- [17] S. S. Gornale, G. Patil, and R. Benne, “Document image forgery detection using RGB color channel,” *Transactions on Machine Learning and Artificial Intelligence*, vol. 10, no. 5, pp. 1–14, 2022.
- [18] K. Maamouli, H. Benhamza, A. Djeffal, and A. Cheddad, “A CNN based architecture for forgery detection in administrative documents,” in *2022 International Symposium on Innovative Informatics of Biskra (ISNIB)*, pp. 1–6, IEEE, 2022.
- [19] G. Mahfoudi, F. Morain-Nicolier, F. Retraint, and M. Pic, “CMID: A new dataset for copy-move forgeries on ID documents,” in *2021 IEEE International Conference on Image Processing (ICIP)*, pp. 3028–3032, IEEE, 2021.
- [20] Y. Okamoto, G. Osada, I. Yahiro, R. Hasegawa, P. Zhu, and H. Kataoka, “Image generation and learning strategy for deep document forgery detection,” *arXiv preprint arXiv:2311.03650*, 2023.
- [21] F. Hossain, A. Gul, R. Raja, T. Dagiuklas, and C. Galkandage, “Forgery image dataset.” <https://ieee-database.org/documents/forgery-image-dataset>, 2022. Accessed: 2025-04-23.
- [22] M. Castro, D. M. Ballesteros, and D. Renza, “Cg-1050: Original and tampered images (color and grayscale).” <https://data.mendeley.com/datasets/dk84bmnyw9/2>, 2019. Accessed: 2025-04-23.
- [23] K. Bulatov, E. Emelianova, D. Tropin, N. Skoryukina, Y. Chernyshova, A. Sheshkus, S. Usilin, Z. Ming, J.-C. Burie, M. M. Luqman, and V. V. Arlazarov, “Midv-2020: A comprehensive benchmark dataset for identity document analysis,” *arXiv preprint arXiv:2107.00396*, 2021.
- [24] Y. He, B. Gan, S. Chen, Y. Zhou, G. Yin, L. Song, L. Sheng, J. Shao, and Z. Liu, “Forgerynet: A versatile benchmark for comprehensive forgery analysis,” *arXiv preprint arXiv:2103.05630*, 2021.
- [25] D. Fischinger and M. Boyer, “Df2023: The digital forensics 2023 dataset for image forgery detection,” *arXiv preprint arXiv:contentReference[oaicite:0]index=0*, 2025.
- [26] J. Dong, W. Wang, and T. Tan, “CASIA image tampering detection evaluation database,” in *2013 IEEE China Summit and International Conference on Signal and Information Processing*, IEEE, July 2013.
- [27] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, “Comofod—new database for copy-move forgery detection,” in *Proceedings ELMAR-2013*, pp. 49–54, IEEE, 2013.

## A Prompt Used for Model Experiments

Below is the exact prompt we supplied to the model in our experiments:

Prompt:

Task: Receipt Fraud Detection Analysis

Examine the provided receipt image carefully and perform a comprehensive fraud detection analysis. Determine if the receipt is fraudulent.

Step 1: Systematic Visual Assessment

- Analyze the document layout, including alignment, spacing, and formatting consistency
- Examine text quality (font consistency, printing quality, resolution)
- Check for visual artifacts (smudges, unusual erasures, digital manipulation signs)
- Assess color consistency and transitions across the document

Step 2: Content Verification

- Verify date and time formatting consistency and logical sequence
- Examine merchant information (name, address, contact details) for completeness and consistency
- Analyze item descriptions, quantities, and pricing for logical coherence
- Verify mathematical accuracy (subtotals, taxes, discounts, final amounts)
- Check transaction identifiers (receipt numbers, transaction IDs) for proper formatting

Step 3: Contextual Evaluation

- Assess logical relationships between items purchased
- Check for reasonable pricing in relation to items purchased
- Verify time of purchase is appropriate for the merchant type
- Evaluate authenticity markers (barcodes, QR codes, watermarks, security features)

Step 4: Potential Fraud Indicators

- Identify inconsistencies in numerical values or calculations
- Detect misaligned text or irregular spacing patterns
- Note any unusual edits, erasures, or modifications
- Flag unrealistic purchases, prices, or merchant information

Conclusion:

Based on your analysis, provide a decisive determination of the question: Is this receipt fraudulent?

1. confidence level
2. List specific evidence supporting your determination.
3. Identify any remaining uncertainties or areas requiring further investigation.

State your confidence level from 0 to 1, 0 for not confident at all(it's legitimate), 1 for certainty (it's definitely fraudulent).

Give your conclusion in json format:

```
{
    "confidence": float,
    "evidence": string,
    "remaining uncertainties": string.
}
```