International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

# Fake Document Detection

**Merin Ann George[1], Shyma Kareem[2]**

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *merinanngeor[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

**Abstract:** ***The growing worry about the accuracy of computerized and manual reports has raised the need of professional and reliable methods for the detection of forged or altered documents. This particular project aims to develop an intelligent Fake Report Detection Framework that employs Artificial Intelligence (AI), Machine Learning (ML), and Digital Forensics to automatically detect and flag false documents. With the help of image processing techniques and advanced anomaly detection models, the system analyzes documents for discrepancies in textual and visual elements, including signatures and logos. Along with text retrieval, the framework's key functionalities include visual component examination, peculiarity detection using machine learning algorithms. It also issues a detailed report stressing areas of concern together with a confidence score assessing the document's authenticity. A web application developed using the Django framework allows users to conveniently upload documents and receive instantaneous evaluations. The project utilizes several datasets of authentic and synthetic documents to train machine learning models, incorporating preprocessing techniques of document image and signature verification. The expected results will significantly increase the reliability of document authentication.***

**Keywords:** Artificial Intelligence, Machine Learning, Digital Forensics

## 1. Introduction

In the computerized era, report extortion has come to be a significant issue over assorted businesses, including lawful, administrative, monetary, and corporate portions. The ability to create or change with records has brought serious issues about information shrewdness and authenticity. With the increasing dependence on complex reports, there's a growing need for robust frameworks to recognize and anticipate deceptive exercises. Traditional methods of archive verification, e.g., manual evaluation, are labour-intensive, time-consuming, and susceptible to human error. To overcome this difficulty, advanced innovations such as Manufactured Insights (AI), Machine Learning (ML), and Advanced Forensics are being integrated into automated systems that can quickly and accurately identify counterfeit or manipulated reports. This project aims to develop an automated Fake Archive Discovery Framework that uses these advances in order to enhance the efficiency and accuracy of confirmation of reports.

The framework utilizes picture extricate printed substance from checked pictures, PDFs, and other archive groups. It too utilizes progressed picture handling strategies to dissect visual components such as logos and marks, which are frequently controlled in manufactured archives. By utilizing machine learning models prepared on datasets of true and false records, the framework is outlined to distinguish irregularities and hail potential imitation. Through an easy-to-use web interface, this framework allows clients to transfer reports, conduct real-time analysis, and obtain detailed reports on the authenticity of the record. The application provides a certainty score based on the likelihood of the record being fictitious or genuine, in this way aiding decision-making templates in record authentication operations.

## 2. Related Works

Kumar, V. (2020) V. Kumar's work "Fake Symbol Discovery Utilizing Profound Learning Strategies" presents a deep learning-based model to identify counterfeit logos in digital media. The research uses Convolutional Neural Systems (CNNs) to make distinctions among genuine and counterfeit logos. The process uses a diverse dataset of authentic and forged logos, image preprocessing, and CNN architectures such as ResNet and Initiation. The framework undergoes intensive preparing and optimisation, through the use of exchange learning and information expansion procedures. The programme achieves an exactness of 94.2%, surpassing standard machine learning methodologies by 9.2%. Nonetheless, the study identifies limitations, including dependence on datasets that will never totally reflect genuine world situations and the need for standardised datasets and evaluation measures.[1]

Singh S et (2019) The study proposes a mobile application for consumers to scan product images, focusing on logo recognition, to determine authenticity. This user-friendly solution aims to reduce human error and increase efficiency in counterfeit detection. However, the system's effectiveness may be influenced by factors like image quality, lighting conditions, and logo variability. Additionally, maintaining a comprehensive database of authentic and counterfeit logos is crucial for performance. Despite these challenges, the paper presents a promising approach to counterfeit detection.[2]

Zhou D et (2019) The paper "Web Scraping for Data Collection in Fake Product Detection" by Zhou and Wang discusses the use of web scraping techniques to gather data for identifying counterfeit products. The authors explain methodologies for extracting information from various online sources, such as e-commerce platforms and social media, to build comprehensive datasets. This approach enhances the accuracy and efficiency of counterfeit detection systems and allows for real-time data acquisition. However, the paper also discusses limitations, such as potential legal and ethical considerations, and the need to address these challenges for responsible and effective application.[3]

Bengio Y et (2013) The paper examines deep learning's role in advancing artificial intelligence by enabling hierarchical feature learning. It discusses training techniques such as restricted Boltzmann Machines and Deep Belief Networks, which help deep models uncover complex patterns in data. The authors highlight how deep learning overcomes challenges like the curse of dimensionality, making it valuable for tasks in vision, speech, and natural language processing. However, deep architectures face issues like high computational demands, difficulties in optimization due to non-convexity, and the necessity for large labelled datasets, which can lead to overfitting.[4]

Krizhevsky A et (2012) This landmark paper introduced Alex Net, a deep convolutional neural network (CNN) architecture that dramatically improved image classification accuracy on the ImageNet Large Scale Visual Recognition Challenge (ILSVRC). The model significantly outperformed traditional methods, achieving top-5 test error rates of 15.3%, compared to the previous best of 26.2%. Alex Net consisted of eight layers, with five convolutional layers and three fully connected layers, and utilized the ReLU (Rectified Linear Unit) activation function for faster training. It also incorporated dropout in the fully connected layers to reduce overfitting to improve generalization.[5]

Drouhard et (1996) This paper presents a neural network-based approach for off-line handwritten signature verification, where signatures are verified from scanned images rather than real-time input. The core feature extraction method involves the use of a Directional Probability Density Function (PDF), which captures the distribution of strokes in various orientations across the signature image. The extracted features are then fed into a multi-layer neural network, which learns to distinguish between genuine and forged signatures. The research focuses on improving the reliability of signature verification systems, particularly under the constraint that only static images (off-line) are available—making it applicable in document verification scenarios such as banking and legal authentication.[6]

Jun Cao et (1995) This paper proposes a multistage classification system for the recognition of handwritten numerals, combining various types of features and classification strategies. The system integrates multiple feature extraction techniques—such as zoning, projection histograms, crossings, and profiles—to capture different structural characteristics of handwritten digits. Instead of relying on a single classifier, the authors implement a multistage classifier framework, where the decision process occurs in sequential steps. At each stage, classifiers either accept a digit or pass ambiguous cases to the next stage for more refined analysis. Classifiers such as k-nearest neighbor's (k-NN) and neural networks are used, depending on the feature set and stage. This approach improves accuracy by reducing the chance of early misclassification and allowing complex or confusing patterns to receive more detailed scrutiny.[7]

Bobby et (1994) This paper presents a method for off-line signature verification by utilizing a combination of global and grid-based local features. The authors aim to enhance the accuracy of verifying whether a signature is genuine or forged by capturing both the overall structure and localized variations in a signature image. Global features include characteristics such as height, width, aspect ratio, slant angle, and stroke density, which give a general overview of the signature's shape and style. Grid features divide the signature image into small regions (grids) and extract features from each part. This helps detect subtle local distortions or inconsistencies common in forgeries. The combined feature set is then used to train a classifier (like a neural network or statistical model) to distinguish between genuine and forged signatures. The method is tested on standard signature datasets and shows promising performance.[8]

Edson Justino et (2010) This paper focuses on improving the accuracy and robustness of writer-independent off-line signature verification systems. Unlike writer-dependent systems (which are trained for specific individuals), writer-independent systems aim to generalize across different users without requiring personalized training. The authors propose techniques to reduce false acceptance of forgeries, especially skilled forgeries, by using a modular classifier architecture and multiple representations of signature data. This includes: Feature extraction from binary signature images (like geometric and statistical features). Classifier ensembles, where multiple classifiers are trained and their results are combined using decision fusion strategies.[9]

Hong Yan (1994) This paper introduces a method for recognizing handwritten digits using an optimized nearest neighbor (NN) classifier. The traditional nearest neighbor algorithm is simple but often suffers from high computational cost and sensitivity to noise. To overcome these limitations, the author proposes an enhanced version that optimizes the feature space and distance computation to improve both accuracy and efficiency. The optimization involves selecting the most discriminative features, reducing the dimensionality of the data, and refining the distance metric used in classification. The system was tested on standard digit datasets, demonstrating high recognition rates and faster computation compared to standard NN approaches.[10]

## 3. Outlined Method

***Information Gathering & Preprocessing:***

The first and most fundamental phase of constructing the Fake Record Location Framework is information gathering and preprocessing, for the quality and organization of the information practically determine the performance of the models. In this phase for fake news location, the ISOT Fake News Dataset is used, which has more than 25,000 articles evenly divided into genuine (obtained from Reuters) and fake (obtained from renowned unreliable sources). The content information undergoes extensive preprocessing, including evacuation of halt words, accentuation, unusual characters, and lowercasing. Tokenization is then linked to split the content into meaningful units (words or sub words). The processed tokens are then transformed into numeric vectors using TF-IDF (Term Frequency-Inverse Document Recurrence) or word embeddings such as Word2Vec, Glove, or the applicable embeddings from BERT, which allow the machine learning models to access it semantic relationships between words. olives collecting various and labeled datasets for fake news texts, logos, and marks.

## 4. System Design

The framework is defined using a balanced and tiered engineering to ensure flexibility, functionality, and productivity. It is actually divided into three main layers: The Introduction Layer, the Trade Rationale Layer, and the Information Layer.

1) **Introduction Layer:** This layer addresses the client interface and has a web-based front conclusion developed using Django. Clients are able to send records (content, images, or PDFs) via this interface for analysis. The interface is designed to be user-friendly and responsive across devices.
2) **Trade Rationale Layer:** This center layer is responsible for all preparing rationale. It has machine learning models specifically prepared for identifying fake news, fashioned logos, and signature confirmation. Each type of archive is guided to its comparing show through backend rationale. REST APIs are used for communication between the front conclusion and this layer.
3) **Information Layer:** This layer supervises data capacity and recovery. SQLite3 is used as the fundamental database for storing user-uploaded documents, examination results, and logs. It also maintains metadata about each report for auditing and future retrieval. Additional plan pieces include:
   **a) Preprocessing Modules:**
   These sanitize and transform the raw input data (e.g., vectorization of content, image resizing).
   **b) Demonstrate Choice Reasoning:**
   Accordingly identifies the archive type and directs it to the relevant location demonstrate.
   **c) Security & Logging:**
   The framework provides safe taking care of records and maintains logs to ensure ease of use and searching.

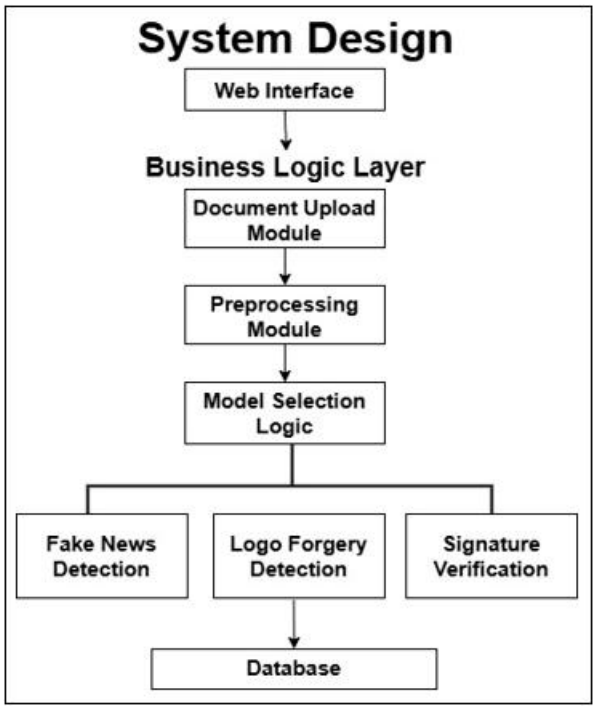


**Figure 1:** System Design

## 5. Dataset Description

The extend makes use of three main datasets to train and evaluate models for fake news detection, symbol imitation detection, and signature verification.

The Fake News Dataset used in this project is the ISOT Fake News Dataset, which contains more than 25,000 news articles divided equally between real and artificial passages. Actual news articles were obtained from Reuters.com, a reliable global news source, while the fake news articles were gathered from sites that have been commended by fact-checking phases like PolitiFact and excerpts cited in Wikipedia. Every article in the dataset has a feature, complete content, category (actual or fake), and date of distribution. The articles cover various topics, despite the fact that most of them are focused on political and global news events between the years 2016 and 2017. The content information was preprocessed to remove unnecessary characters while retaining the dialect anomalies present in fake news to support practical show training.

The Fake Symbol Dataset consists of a wide range of both authentic and synthetic logos. For the purpose of ensuring consistency and reducing computational complexity, all symbol images were resized to 70x70 pixels. This dataset allows the framework to memorize symbol control designs using picture classification methods. The images include a selection of modified parts like modified shapes, text styles, and minimal mutilations defined to simulate real logos, which makes a difference the demonstrate differentiate between authentic and counterfeit brand marks.

The Signature Confirmation Dataset was created by gathering manually signed marks from 37 participants aged 20 to 58. Each participant was provided with 37 authentic signature tests on exceptionally arranged figures. Shortly after, members were shown others' signatures and asked to replicate them, resulting in a significant number of fashioned marks. The templates were by then filtered out, and 2,812 genuine and fictitious signature images were digitized for use. This set of data is particularly lucrative in readied deep learning models to be able to spot fakes using inconspicuous handwriting attributes and visual motifs.

Together, these data sets form the establishment of the discovery capability of the system and allow for a variegated, multi-modal technique to spot impostor records to that of content and image clusters.

## 6. Result & Discussion

The developed Fake Document Detection System was rigorously tested using real-world datasets comprising fake and genuine examples of signatures, logos, and news articles. Each category was processed through dedicated Convolutional Neural Network (CNN) models optimized for their specific detection task. During testing, the models displayed high accuracy and reliability in identifying forged elements. The signature detection module achieved precise results by analyzing stroke patterns, pressure inconsistencies, and alignment issues. The logo detection system leveraged image-based CNN features to distinguish manipulated logos

from genuine ones, while the fake news detector applied Natural Language Processing (NLP) techniques to classify textual content as authentic or fake based on linguistic features and misinformation markers. The system was benchmarked against existing tools, revealing significant improvements in detection speed and reduced dependency on manual verification. The user-friendly interface enabled quick uploads and delivered results in a comprehensible and intuitive format. This efficiency makes the system well-suited for real-world applications, including legal documentation, journalism, and corporate communication. In summary, the integrated use of AI across multiple document types proved highly effective, with the system demonstrating strong generalization and adaptability. Users benefited from a seamless experience, from document upload to forgery detection, which supports the project's objective of automating and streamlining authenticity checks.to symbol color schemes or figures, emphasizing the sufficiency of CNN in visual design recognition. In any event, difficulties remain in recognizing immensely unobtrusive changes where changed logos closely resemble firsts.

**Table 1:** Accuracy & Precision

| Training Level | Accuracy (%) | Precision (%) |
|---|---|---|
| Base (Basic Training) | 70%-75% | 60%-70% |
| Structured Training Modules | 80%-85% | 75%-85% |
| Peak (Real World Use & Refined Evaluation) | 85%-90% | |

## 7. Conclusion

In the modern increasingly sophisticated world, the authenticity of records plays a fundamental role across boundaries like back, law, education, and media. This extend introduced an extensive Fake Archive Location Framework capable of identifying styled news stories, imitation logos, and imitation marks by taking advantage of advanced machine learning and image processing techniques.

The framework was sketched with deliberate quality in intellect, demarcating errands into self-contained components, each tailored to a specific discovery category—fake news, symbol deceit, and signature verification. Leverage cutting-edge techniques such as CNN for image classification and NLP models such as LSTM and BERT for literary research, the framework achieved promising results in separating false content. The incorporation of these models within a user-friendly web-based application promotes upgrades the system's convenience, rendering it accessible to both technical and non-technical clients.

Through extensive testing and validation against actual-world datasets, the framework demonstrated its potential for reliable and computerized imitation discovery. It literally reduces the need for manual confirmation and reduces human error, assuring faster and more accurate report approval.

This work underscores the common sense of amalgamating AI-driven arrangements into everyday situations to fight archive extortion. It paves the way for future improvement and arrangement in skilled contexts where record judgment is fundamental.

## References

[1] Ahmed, H., Traore, I., & Saad, S. (2018). Detecting opinion spams and fake news using text classification. Security and Privacy, 1(1), e9. https://doi.org/10.1002/spy2.9

[2] Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake News Detection on Social Media: A Data Mining Perspective. ACM SIGKDD Explorations Newsletter, 19(1), 22–36. https://doi.org/10.1145/3137597.3137600

[3] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems, 25.

[4] Kingma, D. P., & Ba, J. (2014). Adam: A Method for Stochastic Optimization. arXiv preprint arXiv:1412.6980.

[5] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770-778.

[6] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[7] Bird, S., Klein, E., & Loper, E. (2009). Natural Language Processing with Python. O'Reilly Media.

[8] Y. Zhou and S. Zafarani, "A survey of fake news: Fundamental theories, detection methods, and opportunities," ACM Computing Surveys (CSUR), vol. 53, no. 5, pp. 1–40, 2020.

[9] R. Gupta, A. Kumar, and H. Joshi, "Deep learning-based detection of forged and fake images on social media," Procedia Computer Science, vol. 132, pp. 1371–1379, 2018.

[10] M. Abadi et al., "TensorFlow: A system for large-scale machine learning," in 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI), pp. 265–283, 2016.