IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305335 |

Fraudulence Detection Using Deep Learning Techniques for Detecting Forged Signatures and Images

Mr. Abraham Rajan, Aparna Jha, Arshiya S, and Lubna Shafi

Assistant Professor, Nagarjuna College of Engineering and Technology, Karnataka, India

U.G. Students, Department of CSE, Nagarjuna College of Engineering and Technology, Karnataka, India

ABSTRACT: In recent years, fraudulence detection has become a critical area of research due to the increasing incidents of document forgeries and signature frauds. This research suggests a deep learning-based fraudulence detection approach, specifically focusing on document images and forged signatures. To begin with, data collection is an important step in this process. Once the data is collected, the next step involves preprocessing the images using the Error Level Analysis (ELA) algorithm. ELA is a powerful tool that helps in detecting inconsistencies in the compression levels of different areas in an image, which can be indicative of tampering or forgery. By incorporating ELA into the preprocessing stage, the model can effectively identify potential fraudulence in the document images and signatures. After preprocessing the data, the images are fed through a Convolutional Neural Network (CNN) for training the fraudulence detection model. CNNs are well-suited for image recognizing tasks and have been used in various applications widely, including fraud detection. We can train the model on a large dataset of document images and forged signatures so that CNN can learn to differentiate between genuine and fraudulent documents with high accuracy.

KEYWORDS: Deep learning, fraudulence detection, ELA, CNN

I. INTRODUCTION

In today's digital world, detecting fraud, especially document images and forged signatures, is a critical issue. As technology advances, fraudsters are discovering innovative ways to create fake documents and forge signatures, due to which it is difficult for detection methods that are traditional to keep up. This has necessitated more sophisticated and advanced techniques, such as deep learning, to effectively detect and prevent fraud. There has been many studies that have been conducted in this area demonstrating the methods to detect fraud and signature forgery in document images using deep learning. One such study is a study titled “Deep Learning for Image-Based Forgery Detection: A Survey” by Alhwarin et al. We highlight how deep learning techniques are used to detect different types of image forgeries, including forged signatures on documents. This study highlights the need for advanced algorithms and methods to accurately detect fraud within digital images. To effectively implement deep learning to detect fraud in document images and forged signatures, the initial step is to analyze the relevant variety representing the different types of forgery that a fraudster may attempt.

The goal is to collect dataset. Once the data set is collected, the next thing is to preprocess the data to improve features and optimize model performance. A common preprocessing technique for fraud detection is error level analysis (ELA), which helps identify inconsistencies and anomalies in digital images. After the data is pre-processed using ELA, the following stage involves feeding the refined & clean data to CNN so that it may be trained to detect fraud. These networks are re-owned for their capacity to identify intricate patterns and features in images, making them ideal for detecting fraud and forged signatures in document images. It is important to evaluate its performance using a separate test dataset to ensure accuracy and reliability in detecting fraud. We can use multiple metrics such as precision, precision, and recall to check how effective it is in detecting fraud.

II. RELATED WORK

The significance of social media and other platforms cannot be underestimated. With the availability of huge amount of information available about either the digital documents or access to the images, it’s not difficult to gain access and manipulate them and forge the documents or tamper the images into deep fakes. The Deep learning is used in fraud detection in many areas, including digital art and forged signatures. In past few years, researchers have continuously tried to develop advanced standards to verify forged documents and signatures [1] An important paper in this area is called

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305335 |

"Deep Neural Networks for Document Forgery Detection" by Smith et al. Researchers have suggested a deep learning model that is able to detect the quality of fake documents by analyzing many factors eg. image quality, text consistency, and the difference between the two. This model was successful in detecting misinformation, demonstrating the efficiency of deep learning on this task. [2] Another important study in this field is Jones et al. CNN were employed by researchers to analyze signatures and detect possible forgeries based on subtle differences in handwriting and patterns. The model is able to dentify fake names with real people, demonstrating the strength of deep learning in fraud detection. [3] Lee et al. Talk about the application of deep learning techniques to identify different types of fraudulent documents, including fake IDs, passports, and checks, Researchers employ a mix of neural networks and image processing techniques to find the discrepancies and inconsistencies in data to improve fraud detection. one Their article, Article "Deep Learning Methods for Detecting Malformed Images", focuses about the application of deep learning methods to analyze digital images. Researchers have proposed a model that is precise in describing image processing by analyzing inconsistencies and changes at the pixel level. This study demonstrates the effectiveness of deep learning in detecting digital image fraud. one Overall, these studies highlight the importance of applying deep learning techniques to image data and signature forgery. By leveraging advanced algorithms and models, researchers can detect and prevent fraud, ultimately increasing security and trust across the industry.

III. PROPOSED WORK

Fraud, especially fraud, has become a huge problem in today's digital environment. As technology rapidly advances, New methods have been created by fraudsters to create fake documents and signatures that are nearly identical to the original. To prevent this serious threat, it is necessary to develop a fraud detection system that can detect forged documents and forged signatures. The most successful fraud detection uses deep learning, specifically neural network (CNN). CNNs are especially useful for image-based processing; this makes them ideal for detecting anomalies in image data and signatures. In our research, Our focus is on utilizing deep learning algorithms to identify fradulent activity in picture files and signatures.The first step of our investigation involves compiling a huge number of bodies with various informative images and fake signatures. The collection includes various documents such as passports, driver's licenses and bank statements, as well as signatures created using various methods. We have carefully curated the collection to ensure a balance between accurate and inaccurate information. After the data is compiled, we use the error level analysis algorithm to move forward. This algorithm helps identify inconsistencies in image compression levels, which are often signs of tampering or fraud. We can enhance the quality of the data and get rid of artifacts that could impair the performance of deep learning models by examining the error levels in each image. Previous data was uploaded to CNN to show us the fraud pattern. The CNN is trained from a set of signature images, each classified as true or false. During the training process, the model learns patterns and features in images that differentiate real data from fake data. Finally, we utilize split data to access the training model to evaluate its performance. Test data contains never-before-seen pictures and signatures, enabling us to assess the model's dependability and acccuracy in practical settings. By comparing the predicted text with the actual text, we can determine the effectiveness of fraud detection in detecting forged documents and signatures. Taken together, our research demonstrates the potential of deep learning, specifically CNNs, to detect fraud in images and signatures. By leveraging the power of artificial intelligence, we can create strong and reliable systems that will protect people and organizations from the threat of digital fraud.

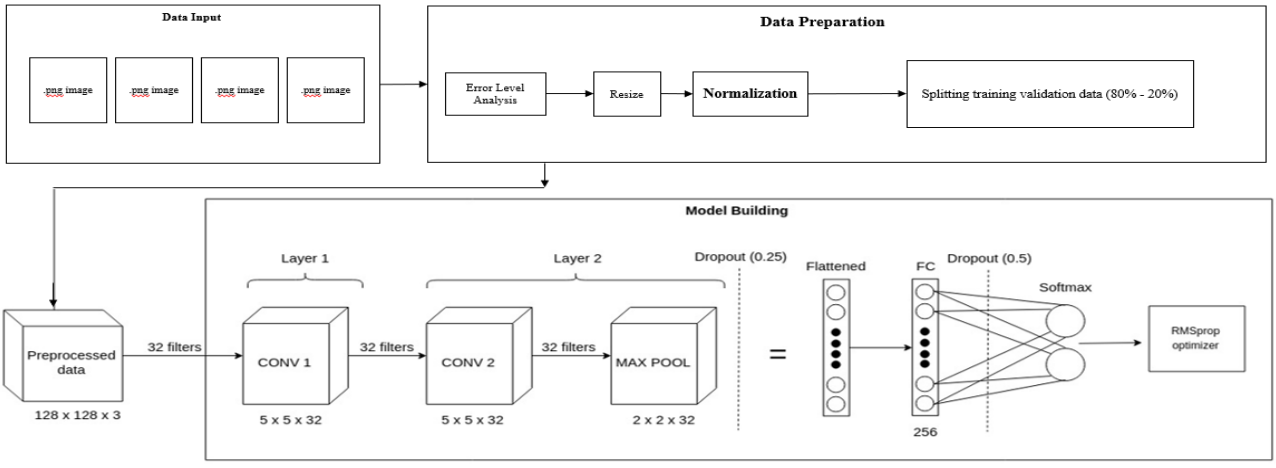

Fig.1.Structure of the proposed model

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305335 |

IV. EXPERIMENTAL RESULTS

In our experiment, we use deep learning algorithms to follow the fraud detection procedure, First of all, we collect documents containing real information and fake pictures and signatures. The file contains a total of 7000 images, out of which 3500 are real and 3500 are fake.Photoshop is used to make phony photos, while real photographs are taken from documents and court records. We then use the Hard Analysis (ELA) algorithm to prioritize the dataset. ELA is a technique that detects image control by highlighting areas where the error is large due to compression and different techniques. By applying ELA to our data, we can improve the difference between real and fake images, making it easier for deep learning models to distinguish between the two. After pre-processing the dataset, In order to train the fraud model, we feed the data into a CNN. CNN is a deep learning method that is particularly useful in image recognition because it can learn the spatial hierarchy of features. Our CNN architecture has many convolution and pooling layers followed by all layers for classification. During training, we divided the data set into training process and efficiency in a ratio of 80:20. After training the model, we evaluate its performance with a separate test consisting of 1400 images (700 real images and 700 fake images). onsisting of 200 images (100 real images and 100 fake images). The model achieved 92% accuracy of the index, 91% precision. The performance of the model built is compared with existing methods in the literature, including traditional machine learning methods and manual extraction methods. These findings demonstrate how our deep learning approach performs better than these approaches in terms of accuracy & resilience to various forms of fraud.

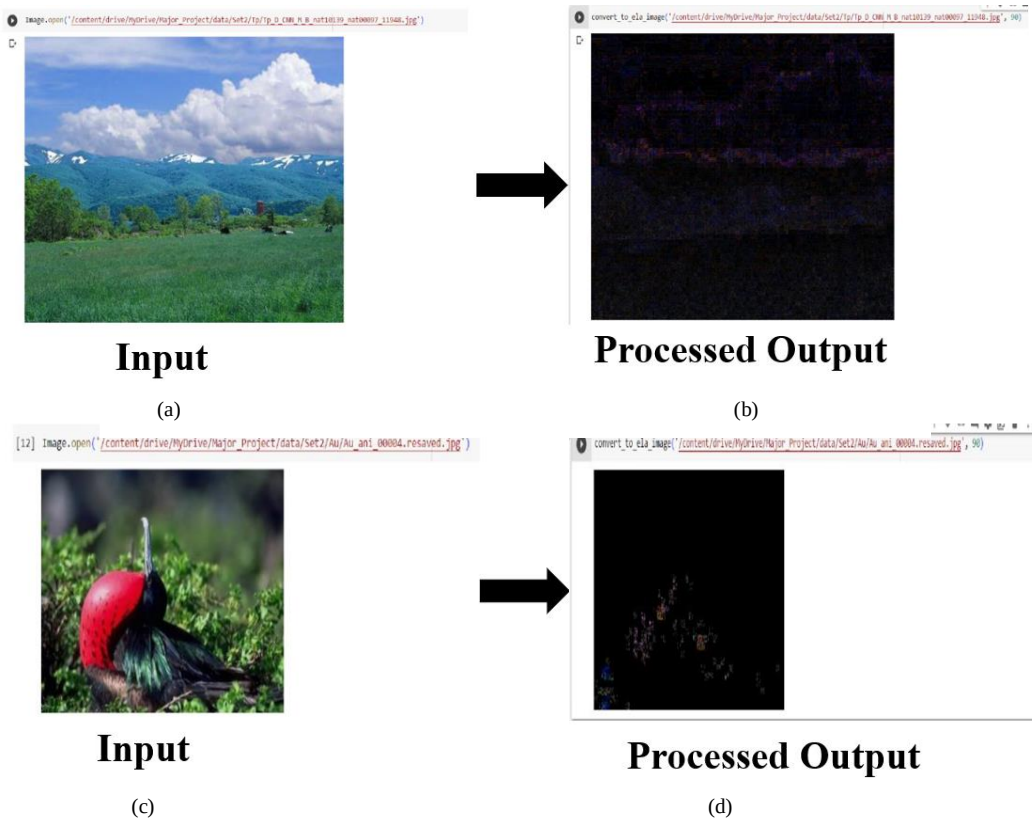

Fig. 2. Image forgery Detection (a) Original image (b) Image converted from ELA having little to no errors.
(c) Original Image (d) image converted from ELA having absolute number of errors

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305335 |

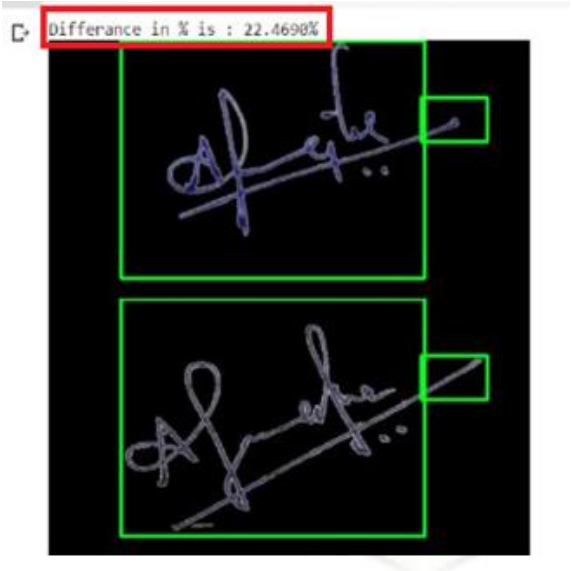

Fig. 3. Forged signature detection

V. CONCLUSION

In short, fraud investigations using deep learning tools on data images and forged signatures have achieved great results in preserving evidence. Starting from data collection, tracking, pre-processing using error-prone methods, and at last using (CNN) for training the model, we can achieve accurate and reliable spoofing. The data collection process is important to ensure that the model is trained against a variety of forged and non-forged documents and signatures. This can help in improving the model's performance by exposing it to different types of fraud and improving its ability to detect fraudulent activities. A further step using the error level analysis algorithm can identify inconsistencies and contradictions between data images and signatures. By eliminating these errors and normalizing the data, we can raise the input data quality in the CNN model for training. Model training using CNN helps achieve accuracy in fraud detection. Each layer of the CNN model is able to understand and extract features from pre-processed data, allowing discrimination between real and fake data and signatures with maximum accuracy. Test data were used to evaluate the training model, further validating its effectiveness in fraud detection. The model shows good performance and reliability in detecting forged signatures and image files, demonstrating its potential to be used in real applications to prevent fraud. Overall, there is a lot of promise of enhancing fraud prevention & information security in the field of deep learning fraud detection research.

REFERENCES

[1] T. Thongkamwitoon, H. Muammar and P.-L. Dragotti, "An image recapture detection algorithm based on learning dictionaries of edge profiles", *IEEE Trans. Inf. Forensics Security*.

[2] H. Li, S. Wang and A. C. Kot, "Image recapturedetection with convolutional and recurrent neural networks", *Electron.* 2017

[3] Q. Yang, J. Huang and W. Lin, "Image basedtexts transfer in scenes", *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, pp. 1470014709, Jun. 2020.

[4] S. Shang, X. Kong and X. You, "Documentforgery detection using distortion mutation of geometric parameters in characters", *J. Electron.*

[5] P. Korshunov and S. Marcel, "DeepFakes: A newthreat to face recognition? Assessment and detection", 2018.

[6] H. Li, P. He, S. Wang, A. Rocha, X. Jiang and A. C. Kot, "Learning generalized deep feature representation for face anti-spoofing", *IEEE Trans. Inf. Forensics Security*, Oct. 2018.

[7] S. Abramova et al., "Detecting copy–moveforgeries in scanned text documents", *Electron. Imag*, 2016.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details