WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Handwritten Document Image Forgery Detection in Blurry and Noisy Environments using Deep Learning

Nandini Ammanagi [a*], Gayatri Patil [b]

[a] *Student, Department of Computer Science, Rani Channamma University, Belagavi, Karnataka, India-591156*
[b] *Research Scholar, Department of Computer Science, Rani Channamma University, Belagavi, Karnataka, India-591156*

A B S T R A C T

Handwritten document images, including text and handwritten image documents, can be subject to manipulation through a variety of digital technologies and photo editing software applications. The paper utilizes a dataset of handwritten samples, consisting of genuine and forged instances with blurry and Noisy environments. Forgery of handwritten image documents can lead to increased crime. For example, forged documents can be used to commit fraud, identity theft, or other crimes. And it can damage a person's or organization's reputation. We have collected a dataset that will undergo pre-processing steps, including image cropping, resizing, noise reduction, and normalization, to improve the quality and consistency of the input data. This paper contributes to the field of forgery detection by showcasing the capabilities of CNNs in analysing and distinguishing genuine and forged handwritten samples. The outcome of the paper is to detect the original or forged. If it is forged then highlight the forged area.

Keywords: Handwritten forgery detection, convolutional Neural Networks, Document authentication, Fraud detection, Deep Learning.

1. INTRODUCTION

Handwritten documents hold significant value in various domains such as legal, historical and administrative sectors. However, these documents are vulnerable to forgery, posing a threat to their authenticity and reliability. Detecting forged signatures, altered content, or fabricated documents is a challenging task that traditionally relies on manual inspection and expert analysis. In recent years, many industries, including image identification and natural language processing, have been transformed by deep learning approaches. Convolutional neural networks and recurrent neural networks are two examples of deep learning models that have displayed impressive skills in learning complex patterns and features from large datasets. There is a chance to advance using the strength of deep learning automated and efficient systems for handwritten document forgery detection.

The study's goal is to investigate how deep learning techniques can be used for handwritten document forgery detection. By training deep learning models on a diverse dataset containing genuine and forged handwritten documents, we can leverage the models' ability to extract intricate features and patterns. This automated approach offers the capacity to greatly improve the precision efficiency, and scalability of forgery detection, providing a valuable tool for document authentication. This work focuses on the development of a Handwritten Forgery Detection system using Convolutional Neural Networks (CNN). This paper's main goal is to create and use a CNN model that can accurately identify and categorize handwritten forgeries. The model will be trained on a dataset of real and fake documents and handwritten samples, allowing it to learn the distinguishing features and patterns associated with forgery.

The proposed Handwritten Forgery Detection system has the potential to significantly impact various industries and applications. It can be employed in banking and financial institutions to detect forged signatures on checks or legal documents, aiding in the prevention of fraud. Further the study encompasses several key steps. First, a comprehensive dataset of genuine and forged handwritten documents will be collected, covering various types of forgeries and writing styles. Next, the collected dataset will undergo pre-processing steps, including image cropping, resizing, noise reduction, and normalization, to improve the quality and consistency of the input data. Subsequently, an appropriate deep learning architecture will be designed, considering the unique requirements of handwritten document forgery detection. The model will be trained using the prepared dataset, optimizing its parameters to minimize the difference between predicted and ground truth labels.

(a). Original Image (b). Forged Image

Figure 1. Sample examples of original image and forged image

2. LITERATURE WORK

The literature review reveals that recent studies have focused on document forgery detection using Deep Learning.

Jaleed Khan et. al [1] explore the application of hyperspectral image analysis and deep learning techniques for the detection of ink mismatches in questioned documents, which can indicate forgery. The paper proposes a novel method that utilizes Convolutional Neural Networks (CNN) to classify spectral responses of ink pixels extracted from hyperspectral document images. The proposed method achieves high accuracy in identifying different ink types for forgery detection, with 98.2% accuracy blue inks exhibit a color accuracy of 92%, while black inks demonstrate an impressive accuracy rate of 88% on the UWA WIHSI database.

Garima Jaiswal and her colleagues (Jaiswal et al., 2) have presented an unsupervised deep learning methodology for detecting ink mismatches in hyperspectral document images. The technique employs a Convolutional Autoencoder (CAE) for extracting features and logistic regression (LR) for identifying ink mismatches. Through the utilization of unsupervised deep learning techniques, the approach endeavors to address the difficulties inherent in supervised classification, which typically necessitates labeled training data.

In the study conducted by [3], an investigation is carried out on Fourier coefficients for the purpose of identifying fraudulent documents. This particular approach employs a divide-and-conquer strategy to detect forgeries in handwritten document images. It should be emphasized that the caliber of the photographs will determine how effective this procedure is. Consequently, it may not yield satisfactory results when applied to degraded documents or distorted text images.

Khan et al. [4] propose a method for detecting forgeries in document images that is based on fuzzy clustering. The features put forth in their proposal, however, prove to be ineffective when applied to documents that suffer from poor quality or have been tampered with through multiple operations.

Shivakumara et al. [5] introduced a novel approach for detecting forged IMEI (International Mobile Equipment Identity) using a fusion operation in conjunction with the color space. The detection process involved a connected component analysis technique. It is important to note that the method was specifically tested on IMEI number images and not on handwritten text images. Consequently, its effectiveness in detecting forgery in handwritten text images may be limited.

L. Nandanwar and colleagues [6] introduced a novel approach for identifying modified text within document images. The method in question involves utilizing discrete cosine transform (DCT) coefficients in a unique manner to generate fused images from the original images. The proposed method then uses quality indicators and histogram-based features to extract features from these fused photos.

Charles C. Tappert et al [7] introduced an Automated of Forgery Detection system and conducted an experiment to evaluate its efficacy. The results of the experiment revealed the alarming ease with which handwriting can be forged, as many participants were able to successfully replicate the shape and size of authentic handwriting through training.

Ahmed et al. [8] introduced a forgery detection method that relies on intrinsic document features. The primary concept underlying their proposed approaches is to automatically discern the sections of a document that pertain to the template, subsequently identifying distortions solely within those sections. This methodology has led to a notable enhancement of up to 29% in the accuracy of forgery detection.

G. Patil et al [9] presented a technique for the classification of counterfeit handwritten and printed document images. The method focuses on the extraction of image quality metrics. By employing the Random Forest classifier, the approach attains a precision rate of 94% for forged printed document images and 98.80% for forged handwritten document images.

G. Patil et al [10] introduced a novel and robust approach for detecting altered handwritten text. The proposed methodology explores traditional features to tackle intricate classification challenges posed by manipulated text images, which are subjected to multiple operations in a noisy and blurred environment.

Upon careful examination of the aforementioned discourse, it becomes apparent that the majority of the techniques employed focus on the identification of specific forged images for classification purposes. However, these methods may prove inadequate when confronted with handwritten documents that are situated in environments characterized by blurriness and noise. Consequently, it can be deduced that there exists a pressing need to devise a resilient approach for detecting forgery in handwritten document images that are subject to such conditions.

3. PROPOSED METHODOLOGY

Proposed methodology consists of several stages, the three important types are Feature extraction, Image acquisition, and Pre-processing as illustrated below in figure 2. The distortions in the original images are caused by tampering operations such as copy-paste, copy-paste with blur, and noise. This is due to the fact that our primary objective is to distinguish between original and forged documents based on various forgery operations.

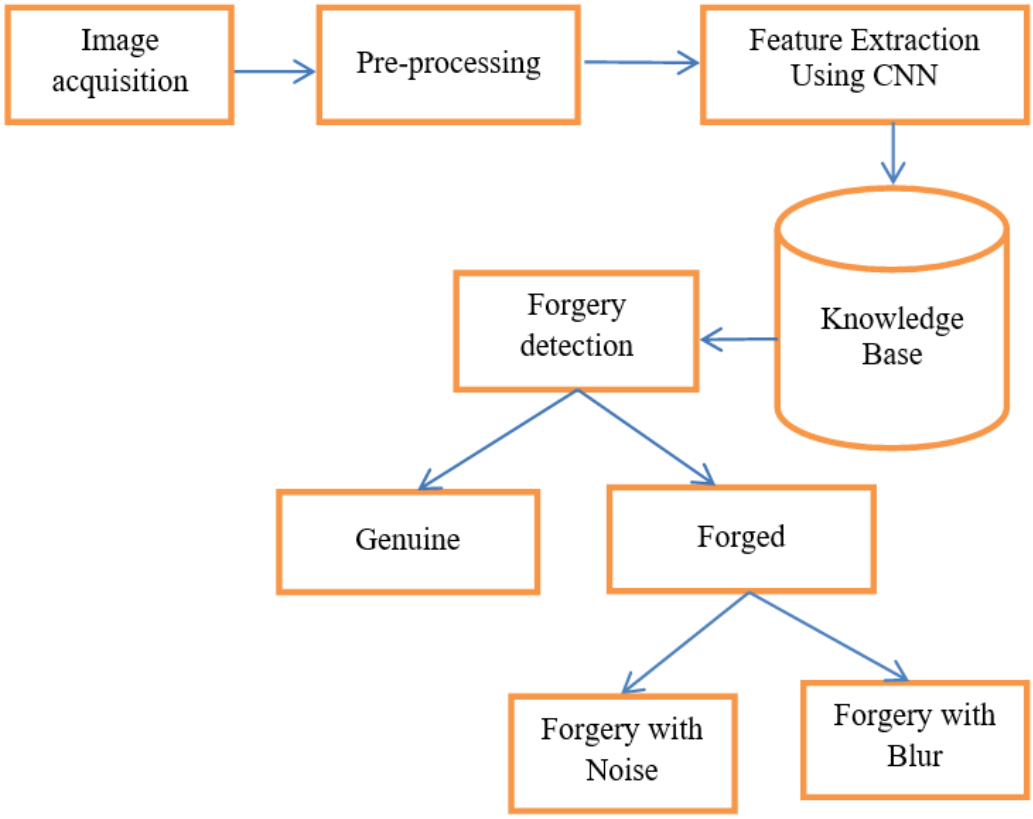

Figure 2. General Architecture of the proposed methodology

Image Acquisition:

This is the initial step where you obtain the handwritten document that needs to be analysed. The document is typically scanned or photographed to create a digital image.

Pre-Processing:

Pre-processing is essential to clean up the acquired image and enhance its quality for further analysis. The few pre-processing steps used in the work, such as: Noise Removal: Reducing any unwanted elements like speckles or Artifacts. Contrast Enhancement: Adjusting the image's contrast to make the text more legible and Normalization: Ensuring consistent image size, resolution, and orientation.

Feature Extraction:

Feature extraction involves identifying and quantifying distinctive characteristics of the handwritten document images. The major features that can be extracted from the handwritten document images are:

a) Texture: Patterns and textures in the handwriting.

b) Shape: Information about the shapes of letters and symbols.

c) Size: Measuring the dimensions of characters or words.

d) Spacing: Analyzing the spaces between words or letters.

e) Pressure: Variations in the pressure applied while writing.

f) Stroke Direction: The direction of pen strokes.

g) These extracted features act as input data for the forgery detection algorithm

Convolutional Neural Networks (CNNs):

A Deep supervised learning architecture is used by convolutional neural networks (CNNs), which are multi-layer neural networks. It is renowned for its capacity to autonomously extract features for classification. An autonomous features extractor and a Trainable classifier are the two major parts of a CNN. Two operations—convolution Filtering and Downsampling—perform feature extraction from the given data via the feature extractor.

An image is represented as a matrix I in convolution filtering, where I(x, y) stands for the brightness of the pixel at the specified coordinates. The kernel matrix, which denotes the kind of filter, and the matrix I are combined to create a convolution product. The three-by-three or five-by-five dimensions of the kernel matrix, abbreviated K, are both possible. The outcome of this operation determines the pixel's new brightness (x, y). For a kernel of size 3 3, the convolution product of the product * is defined as follows:

$$I * K = \begin{pmatrix} I(1,1) & I(1,2) & \dots & I(1,n) \\ \vdots & & I(x,y) & \vdots \\ I(m,1) & I(m,2) & \cdots & I(m,n) \end{pmatrix} * \begin{pmatrix} K(1,1) & K(1,2) & K(1,3) \\ K(2,1) & K(2,2) & K(2,3) \\ K(3,1) & K(3,2) & K(3,3) \end{pmatrix} \quad (1)$$

The selection of a filter is contingent upon the value of K. The fully connected layer of the Back propagation method is used to train the trainable classifiers, which then uses the aforementioned features to produce classification results. A Multilayer feed forward neural network is used by the back propagation technique to learn, iteratively gaining the set of weights for predicting the class label of tuples. A multilayer feed-forward neural network consists of an input layer, one or more hidden layers, and an output layer.

The proposed methodology employs a Convolutional Neural Network (CNN) as both a feature extractor and classifier. The architecture of the proposed CNN-AE model is depicted in the figure below.

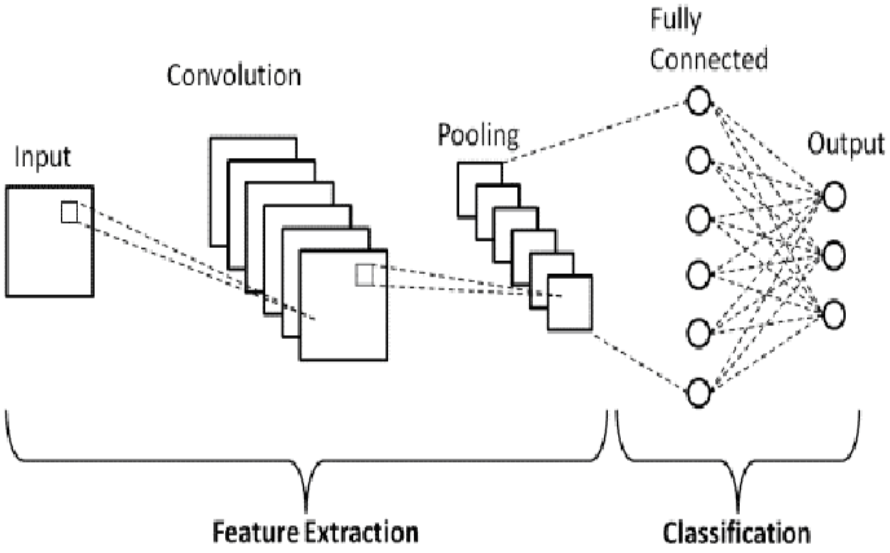

Figure 3. General Architecture of the CNN

An auto encoder is a form of artificial neural network utilized for unsupervised learning of efficient data coding's. Its purpose is to acquire a representation (encoding) for a dataset, typically for the purpose of reducing dimensionality, by training the network to disregard extraneous signal "noise".

The Rectified Linear Activation function (ReLU), which is described in the equation, is then fed the output of ci. The original and fake photos in this study are arranged in a file directory structure that is compatible with the Keras Python library. In order to understand the patterns associates with real and fake words, the CNN has subsequently been implemented in python utilizing Keras and the Tensor Flow backend. In order to determine how well the generated model fits the data, accuracy and loss metrics have been used to evaluate it. In order to confirm that the model's predictions are accurate, it has also been evaluated using photos from a different set.

Table 1: Model Architecture

Layer (type)	Output Shape	Param #
conv2d_1 (Conv2D)	(None, 510, 510, 32)	896
max_pooling2d_1 (MaxPooling2D)	(None, 255, 255, 32)	0
conv2d_2 (Conv2D)	(None, 253, 253, 64)	18496
max_pooling2d_2 (MaxPooling2D)	(None, 126, 126, 64)	0
conv2d_3 (Conv2D)	(None, 124, 124, 128)	73856
max_pooling2d_3 (MaxPooling2D)	(None, 62, 62, 128)	0
conv2d_4 (Conv2D)	(None, 60, 60, 256)	295168
max_pooling2d_4 (MaxPooling2D)	(None, 30, 30, 256)	0
conv2d_5 (Conv2D)	(None, 28, 28, 256)	590080
max_pooling2d_5 (MaxPooling2 D)	(None, 14, 14, 256)	0
conv2d_6 (Conv2D)	(None, 12, 12, 512)	1180160
max_pooling2d_6 (MaxPooling2D)	(None, 6, 6, 512)	0
flatten_1 (Flatten)	(None, 18432)	0
dense_1 (Dense)	(None, 256)	4718848
dense_2 (Dense)	(None, 60)	15420

Table 2: List of equation for CNN

Operation	Formula	
Convolution	$Z^1=h^{1-1} * w^1$	(2)
Max Pooling	$h^1{}_{xy} = max_{i=0,s,j=0,s} h^{1-1}(x+1)(y+j)$	(3)
Fully-connected layer	$Z_l = W_l * h_{l-1}$	(4)
ReLu(Rectifier)	$\text{ReLU}(z_i) = \max(0, z_i)$	(5)
Softmax	$\text{Softmax}(z_i) = e^{zi} / \sum_j e^{zj}$	(6)

In our technique, an image travels through alternating layers of convolution and Max pooling. A predetermined number of feature maps are created during the convolution process and are then sent to a Max Pooling layer. The feature maps obtained from the preceding convolution layer are pooled in this layer's max-pooling step. The following convolution layer receives the resulting pooled feature map, and so on until the fourth maximum pooling layer is reached.

The final max pooling layer flattens and sends the pooled feature map to the fully connected layers. The model is trained after numerous iterations of forward and backward propagation, allowing predictions to be produced. Table 2 contains the formulas for each phase of the convolutional neural network (CNN).

Algorithm:

Input: Handwritten Forged Document Image

Output: Detection of Forged Document Image

Step 1: Acquisition of Handwritten Forged Document Image

Step 2: Pre-processing i.e., enhance its quality for further analysis such as Enhancement and Normalization

Step 3: Computation of features using Texture, Size, Spacing, Shape, Pressure, Stroke Direction

Step 4: Display whether the document is genuine or suspected of being forged.

4. IMPLEMENTATION RESULTS

Data Set: The dataset utilized in this research endeavor is a compilation of 1000 genuine word written images and forged, with 500 genuine and 500 forged. This dataset was obtained from the Kaggle Dataset repository. We have constructed the dataset from the original text images. In this text image, we have to crop and edit the college in the form of words. Initially, Adobe Scanner was used to scan handwritten documents and in this forged dataset, some words are noisy and blurry.

The split between Training and Testing will be 80:20. We have used a dataset of 1000 photos, and we divided them into groups for train and testing. The distribution of data used for training purposes: Handwritten documents category includes documents that consist of handwritten images, such as

handwritten letters, notes, or forms. Handwritten document forgery detection aims to detect forged or altered sections of handwritten within these documents. The total data is 1000, the genuine dataset is 500, forged dataset is 500 in this dataset we have classified two types noise and blur, noise is 250, and blur is 250.

The following results show the outcome of the proposed methodology which is tested on handwritten document images. figure 4 shows that the method recognized an original document as an original image with some noisy environment and also the method correctly predicts the text present in the given input image. Figure 5 shows that the proposed method recognized the forged document image as a forged image with forged characters in the images.

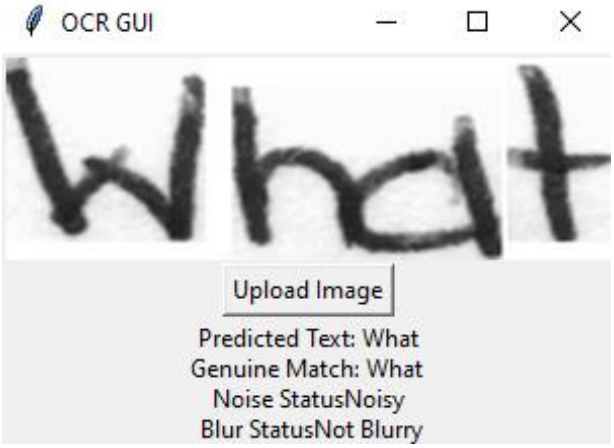

Figure 4. Sample example of original document image recognised as original

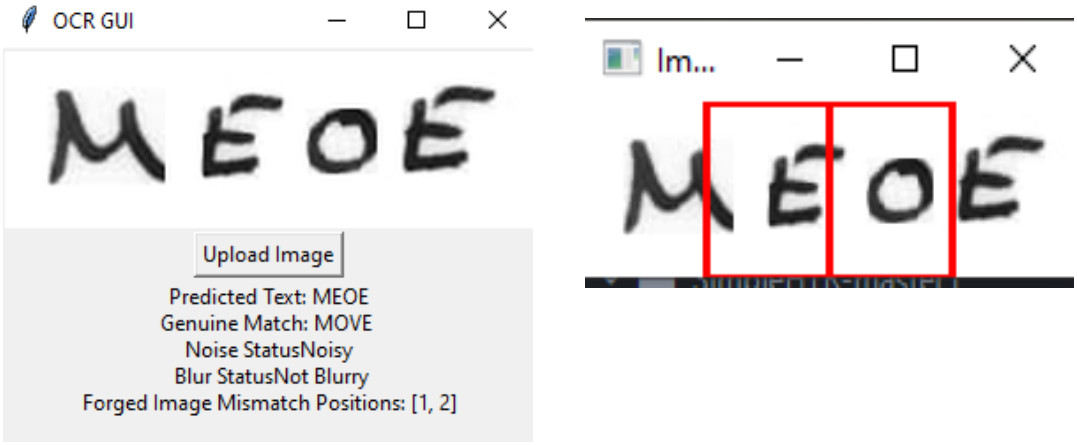

Figure 5. Sample example of forged document image recognised as forged with forged characters.

5. CONCLUSION

In conclusion, handwritten document image forgery detection using Deep Learning paper aims to leverage advanced techniques and algorithms to identify forged or manipulated content within handwritten documents. By applying deep learning models, feature extraction, and forgery detection algorithms, the system can analyze forgery in various types of handwritten documents, such as signature documents, handwritten text documents, official documents, bank and financial documents, legal documents, and historical documents.

References

1. Muhammad Jaled Khan, Adel Yousaf, Asad Abbas, Khurram Khrushid. “Deep learning for automated forgery detection in hyper spectral document images.” Journal of Electronic Imaging, vol.27, no.5, September 2018, https://doi.org/10.1117/1.JEI.27.5.053001
2. Garima Jaiswal, Arun Sharma, Sumit Kumar Yadav. "Deep feature extraction for document forgery detection with convolutional auto encoders”, Computers and Electrical Engineering, vol. 99, June 2022, https://doi.org/10.1117/1.JEI.27.5.053001
3. Raghunandan KS, Shivakumara P, Navya BJ, Pooja G, Prakash N, Kumar GH, Pal U, Lu T (2016) “Fourier coefficients for fraud handwritten document classification through age analysis”. 15th International Conference on Frontiers in Handwriting Recognition (ICFHR), pp 25–30. https://doi.org/10.1109/icfhr.2016.0018

4. Khan MJ, Yousaf A, Khurshid K, Abbas A, Shafait F (2018) "Automated forgery detection in multispectral document images using fuzzy clustering". 13th IAPR International Workshop on Document Analysis Systems (DAS), pp 393–398. https://doi.org/10.1109/das.2018.26

5. Shivakumara P, Basavaraja V, Gowda HS, Guru DS, Pal U, Lu T (2018) "A new RGB based fusion for forged IMEI number detection in Mobile images". 2018 16th international conference on Frontiers in handwriting recognition (ICFHR), pp 386–391. https://doi.org/10.1109/icfhr-2018.2018.00074

6. L. Nandanwar. et al. "A New Method for Detecting Altered Text in Document Image". In: Lu Y., Vincent N., Yuen P.C., Zheng WS., Cheriet F., Suen C.Y. (eds) Pattern Recognition and Artificial Intelligence. ICPRAI 2020. Lecture Notes in Computer Science, vol 12068. Springer, Cham. https://doi.org/10.1007/978-3-030-59830-3_8, 2020

7. Cha and c.c. Tappert, "Automatic detection of handwriting forgery", In Proc.IWFHR, 2012.

8. A. Ahmed and F. Shafait, "Forgery detection based on intrinsic document features", In Proc.DAS, 252-256, 2014.

9. G. Patil, "Method for classifying forged handwritten and printed document images"

10. Gayatri Patil, Shivanand S. Gornale, Umapada pal, P Shivakumar, "A new robust approach for altered handwritten text detection", Multimedia Tools and Applications 2023, https://doi.org/10.1007/s11042-022-14242-8