

Forensic Handwritten Signature Identification Using Deep Learning

Omar Tarek

Faculty of Computer Science,
October University for Modern
Sciences and Arts (MSA).
Giza, Egypt
omar.tarek22@msa.edu.eg

Ayman Atia

HCI-LAB, Faculty of Computers and
Artificial Intelligence, Helwan University.
Faculty of Computer Science, October University
for Modern Sciences and Arts (MSA).
Giza, Egypt
aezzat@msa.edu.eg

Abstract—Forgery is a type of fraud defined as the act of forging a copy or an imitation of a document, signature, or banknote which is considered a form of illegal criminal activity. In this paper, we are focusing on the identification and detection of handwritten signature forgeries inside documents. The proposed system uses contemporary methods that utilize a deep learning approach of CNNs (Convolutional Neural Networks) for binary image classification and aims to help forensic examiners measure the genuineness of handwritten signatures. We considered using a number of five different classification models of CNN which are, VGG-16, ResNet50, Inception-v3, Xception, and Our CNN model. The purpose for using these different CNN models is to determine and study which model is best at identifying images containing text data containing similar resemblances. Upon comparing these CNN models, we concluded that the ResNet50 model was able to reach the highest score at identifying handwritten signatures with an accuracy of 82.3% and 86% when tested on datasets of 300 images and 140 images respectively. Regarding future work, this is a required step that determines what model to focus on for more in-depth analysis and classification of the characteristics of handwritten signatures.

Keywords— *Forensic Document Examination, Handwritten Signatures, Forgery Detection, Image Classification, CNN Architectures*

I. INTRODUCTION

Forensic analysis is the application of scientific methods for the identification and examination of scientific evidence during a criminal investigation. FDE (Forensic Document Examination) is a forensic science that focuses exclusively on examining documents concerning emails, business letters, transactional documents, financial reports, bank signatures, or other criteria. Forgery is the number one crime that is most commonly associated with FDE. It involves the recreation of a false document, signature, or other imitation of an object of value to be used with the intent to deceive another. And it is stated by Interpol that document fraud is considered a form of illegal criminal activity. In this paper, we will be focusing on the identification of handwritten signatures inside documents by using state-of-the-art technologies that utilize artificial intelligence and deep learning techniques.

Handwritten signature forgery can be identified by a set of features and characteristics that most forensic document

examiners are familiar with. However, many of these features can cause confusion for the examiners especially when a forgery is performed by a skilled perpetrator. The proposed system solves this problem by using deep image classification methods that focus on comparing multiple combinations of comprehensive signature features.

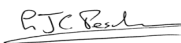



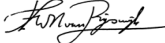

Genuine	Forged
	
	
	

Fig. 1. Genuine Signatures vs Forged Signatures

The handwritten signature samples shown in figure 1 represent the level of challenge encountered by our classification models by showing close similarities between each class. To tackle this problem, we will be using a combination of five different CNN models for the binary image classification of handwritten signatures. With that in mind, the classification models must go through a sufficient amount of training, validating, and testing to reach acceptable results. The dataset used consisted of a sample containing 300 images of handwritten signatures (150 Genuine Signatures + 150 Forged Signatures).

The main contribution of this paper is to explore and compare different CNN models to determine the best-performing model in terms of classification of images containing text data which aims to help forensic examiners with identifying the genuineness of the handwritten signatures. The system uses five different CNN models which are, VGG-16, ResNet50, Inception-v3, Xception models, and our Custom CNN Model.

II. RELATED WORK

Because of the rapid rise of fraudulent activities with fraudsters now taking advantage of contemporary computer software for illegal behaviors and illicit purposes, lots of research efforts were dedicated to this subject for the following topics which are (A) forged document detection, and (B) handwritten signature identification.

A. *forged document detection*

In document forgery detection, Praba et al. [1] has presented a system proposing two methodologies for detecting forged documents, the first is by scanning a QR-code of the document to determine its source, the second way is by using a machine-learning algorithm to train, test, and classify the questioned document to determine whether it is forged or not. Alternatively, James et al. [2] have used a data-driven approach that utilizes OCR (Optical Character Recognition) graph features to detect document manipulations on a constructed dataset of real business documents containing slight forgery imperfections. Yoosuf et al. [3] has proposed a method that applies cognitive techniques to identify and detect document forgery in an information management system by using an automatic document verification model utilizing CNN then applying OCR and LBP (Linear Binary Pattern) to extract textual information and regional edges before using ORB (Oriented fast and Rotated Brief) to extract images from the scanned documents, the MIDV-500 dataset which contains 256 Azerbaijani passport images was used to train the CNN model that uses sliding window operations layers to evaluate authenticity. Roy et al. [4] has presented a system that conducts forensic analysis on handwriting for identifying forgery owing to word alteration. The proposed system uses a Multilayer Perceptron classifier adopted to classify data instances computed by extracting color-based statistical features, the system managed to achieve an accuracy of 83.71% for blue pen data and 78.18% for black pen data.

For copy-move forgery detection and localization, Abdalla et al. [5] has used a deep learning approach that utilizes deep Convolutional learning algorithms, this paper investigates copy-move forgery detection by utilizing a fusion processing model of GANs (General Adversarial Networks) and CNN on four different datasets with an accuracy approximate of 95%. Khan et al. [6] have presented an automated deep learning for forgery detection of ink mismatch in hyperspectral document images using CNN-friendly image format after extracting ink pixels from a hyperspectral document image to be fed to the CNN for classification, the proposed method identifies different inks in hyperspectral document image with an effective accuracy of 98.2% for blue ink and 88% for black ink on the UWA Writing Ink Hyperspectral Images (WIHSI) database.

Ranjan et al. [7] has proposed a framework for image forgery detection and classification using machine learning,

the paper lays a foundation for the investigation of digitally manipulated images by providing a solution to distinguish between such images with an accuracy of 96.4%. Adi et al. [8] has presented a system for combining perceptual hash and OCR for securing and authenticating printed documents from forgery attacks. Bunk et al. [9] has presented a system that uses two deep learning methods for detection and localization of image forgeries by utilizing resampling features. The first method uses overlapping image patches to compute the radon transform of resampling features before using deep learning classifiers and Gaussian conditional random field model to create a heatmap to then identify tempered regions using the Random Walker segmentation method. In the second method, what differs is that the computed resampling features on overlapping image patches pass through an LSTM (Long Short Term Memory) network for classification purposes. Vieira et al. [10] has proposed an information system for automation management of counterfeited document images using a two-fold approach that utilizes the OpenCV framework which is used to compare images, match patterns, and analyze textures/colors tested on a Portuguese citizen card. Ghosh et al. [11] has presented a system for detection and localization of image and document forgery using CNN classifier.

Shang et al. [12] has presented a document print and copy forgery detection by analyzing different printer types (laser printers, inkjet printers, and electrostatic copiers), the proposed method can distinguish between each type based on features extracted from characters in the documents which was able to achieve an accuracy of 90% that also works with JPEG compression. Bertrand et al. [13] has presented a system that is based on finding intrinsic features for detection of fraudulent documents by proposing a method which is based on detecting outlier characters in a discriminant feature space and the detection of strictly similar characters, each character then is classified as a genuine one or a fake one.

B. *handwritten signature identification*

Other than checking for document authenticity, forged handwritten signatures is one of the most common things that would be found on a document, must not be overlooked. Poddar et al. [14] has presented a system that uses a deep learning approach to recognize and detect forged handwritten signatures using CNN, Crest-Trough method, SURF algorithm, and Harris Corner detection algorithm, the proposed system managed to attain an accuracy of 90%-94% for recognizing a valid signature and an accuracy of 85%-89% for detecting forged signatures. Kao et al. [15] has proposed a method based on a single known sample for offline signature verification and forgery detection using an explainable deep learning approach that utilizes DCNN (Deep Convolutional Neural Network) backed by a unique local feature extraction method, this system was capable of achieving an accuracy between 94.37% add 99.96% with false rejection rate (FRR)

between 5.88% and 0% and a false acceptance rate (FAR) between 0.22% and 5.34% when used on the Document Analysis and Recognition (ICDAR) 2011 SigComp dataset. Wei et al. [16] has presented IDN (Inverse Discriminative Network) for verification of handwritten signatures that aims to differentiate between genuine signatures and forged signatures, this model was used on a Chinese signature dataset of 29,000 images from 749 individuals to test on different datasets of different languages as well which are: CEDAR, BHSig-B, and BHSig-H. Pokharel et al. [17] has proposed a deep learning system for handwritten signature recognition that uses a CNN architecture, they used a transfer learning method to retrain the GoogleNet model on 25 classes of a signature image dataset where each class contains 85 signatures to achieve a mean testing precision of 95.2%.

III. PROPOSED METHODOLOGY

We proposed a binary image classification system that uses a combination of different CNN models to classify these images of handwritten signatures. The goal of this system is to find the most effective classification method that works best with text-based images by testing each method separately and comparing the attained outcome. This system works by taking an input of a scanned image containing the signature and using binary image classification models in order to validate the processed image.

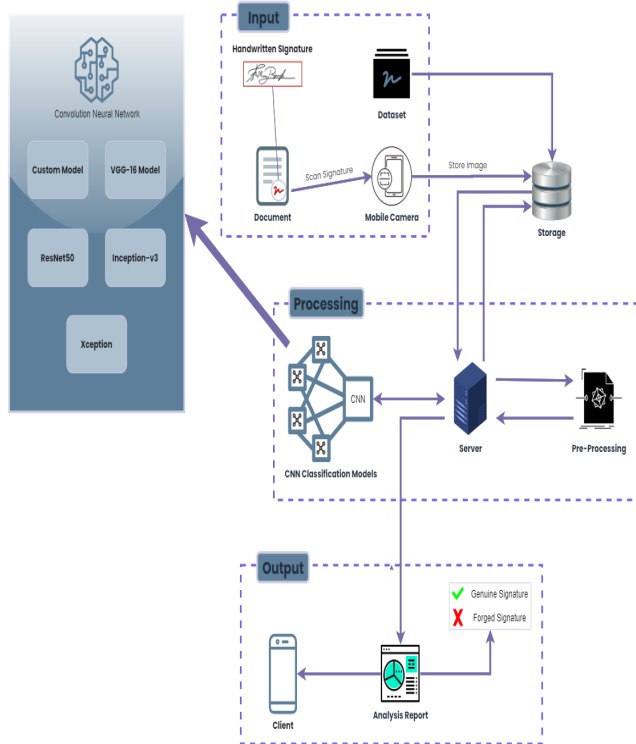


Fig. 2. Overview

A. Convolutional Neural Network

A CNN is a type of artificial deep learning neural network that is used most in image recognition/classification and is commonly associated with computer vision. It contains multiple layers called convolutional layers which are based on the convolution operation that works by combining two functions (input image, image filter) to produce a third function.

Convolution Operation:

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t - \tau)d\tau$$

$(f * g)(t)$ = functions that are being convoluted

t = real number variable of functions f and g

$g(t)$ = convolution of the function $f(t)$

$d\tau$ = first derivative of $g(\tau)$ function

An image consists of a set of arrays of different numbers representing squares of pixels arranged in rows and columns, which is called an Image Matrix. The CNN works by taking an input image in the form of an image matrix to extract features from the image and classify them based on learned features.

B. Pre-Processing

Before introducing the classification models, a pre-processing phase must take place. The methods used in this phase are simple but rather very important in order to allow the classification models to perform most effectively on the signature images. Each image matrix is rescaled to grayscale and resized to a default resolution of 320 X 240, which is going to be the same as the input layer (first layer of the classification model in Fig. 3) for all the different classifiers.

C. CNN Models

The proposed system uses the following 5 CNN image classification models, which consist of our Custom CNN model and four other pre-trained models (VGG-16 model, ResNet50 model, Inception-v3 model, and Xception model).

First, the Custom CNN classification model is of type sequential, which consists of 3 convolutional layers that use RELU (Rectified Linear Activation Function), three max-pooling layers, and two dense layers with the output layer using SOFTMAX activation function for binary classification.

Second, to configure the proposed pre-trained models which were trained on the ImageNet dataset through a process of Transfer Learning, we were able to fine-tune each model by removing its current input and output layers so that we can replace them with our own inputs and outputs. For the input, we added a new layer with our desired input data. As for the

output, we added a new flatten layer to flatten the pre-trained model into a 1 Dimension followed by a dense layer of 512 neurons that uses RELU activation function before adding the final output dense layer for binary classification that consists of the Softmax activation function and 2 categorical classes which are later defined as either a forged signature or a genuine signature.

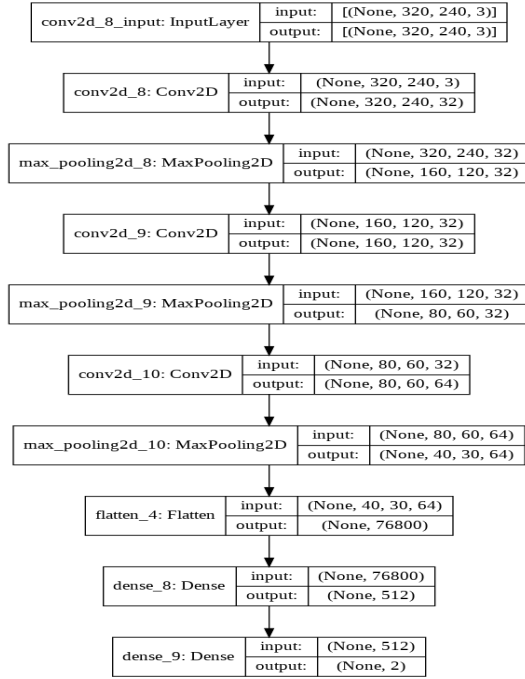


Fig. 3. Our CNN Model

IV. EXPERIMENT

We conducted a total of two experiments. The purpose of the first experiment is to test all of our CNN models to determine which model has the best results of the classification task on a dataset of 300 images of handwritten signatures. As for the second experiment, the objective is to use the model that achieved the highest score from the first experiment to test it on a newly collected dataset that contained 130 images of handwritten signatures.

A. experiment 1

In this experiment, we set up each of our five models for training and testing on a dataset of 300 images¹ for handwritten signature samples that consisted of 150 genuine signatures and 150 forged signatures. The main objective of this experiment is to compare the outcome of the different models and determine which model is best at classifying text-based images.

¹ Handwritten Signatures Dataset 1: <https://www.kaggle.com/divyanshrai/handwritten-signatures>

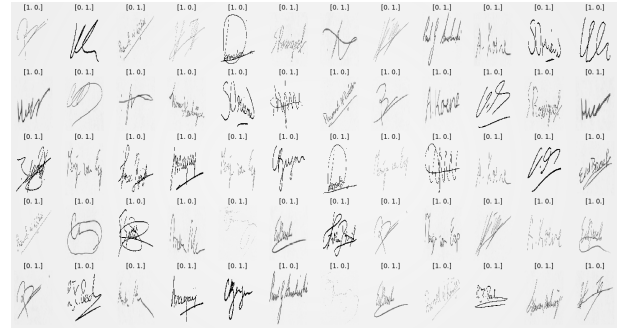


Fig. 4. Handwritten Signature Dataset 1

B. experiment 2

The experiment objective is to test the model that achieved the highest score from the first experiment on a new dataset of 140 images² to see if it can deliver better results. First, we worked on creating a new dataset by gathering new handwritten signature samples from different individuals, each individual providing five samples of their handwritten signature. Then we attempted to forge the gathered signatures to best resemble their genuine signature as a skilled perpetrator would likely do in an event of a forgery.

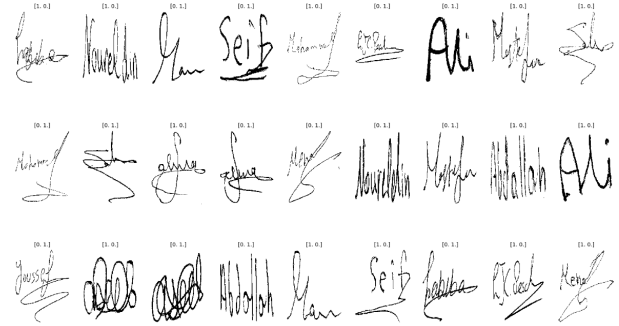


Fig. 5. Handwritten Signature Dataset 2

For the experiment, we used our created dataset which provides the input data of 140 handwritten signature samples belonging to 14 different individuals where half of them are forged. Both of the forged and genuine signatures are then introduced to the classification model to being the training phase. We obtained 10 signature samples per individual where the used dataset ratio of training to testing was 6 : 4. For each 10 signature samples, we used only 6 samples for training the model and the remaining 4 samples for testing the trained model. In the training phase, the 6 samples are categorized into 3 genuine signatures and 3 forged signatures. As for the testing phase, the 4 samples were categorized into 2 genuine signatures and 2 forged signatures.

² Handwritten Signatures Dataset 2: <https://github.com/OmarTibraheem/FDE/tree/main/Datasets/Handwritten%20Signature%20Dataset%202>

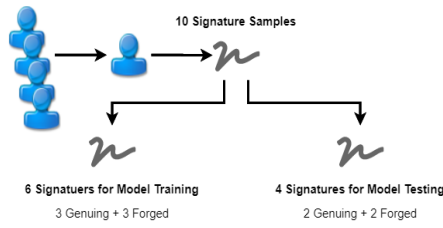


Fig. 6. Breakdown of Collected Signature Samples

V. RESULTS AND DISCUSSION

Concerning the first experiment, we were able to reach the following scores for each model as shown in table 1. The ResNet-50 model was capable to perform the most accurate of the 5 models by reaching an accuracy of 82.3%.

Model	Accuracy	Precision	Recall	F1 Score
CNN	0.75	0.80	0.67	0.73
VGG-16	0.75	0.70	0.87	0.78
ResNet50	0.82	0.81	0.83	0.82
Inception-v3	0.77	0.72	0.87	0.79
Xception	0.70	0.64	0.93	0.76

Table 1. Classification Models Report

We used the following mathematical relations to calculate each of the Accuracy, Precision, Recall, and F1 Score. It is also worth knowing that: TP = True Positive, TN = True Negative, FP = False Positive, and FN = False Negative. Keeping in mind that we will be using our CNN model result values as an example.

$$\begin{aligned} TN &= 0.83 & FN &= 0.33 \\ FP &= 0.17 & TP &= 0.67 \end{aligned}$$

Precision:

$$P = \frac{TP}{TP + FP} = \frac{0.67}{0.67 + 0.17} = 0.80$$

Recall:

$$R = \frac{TP}{TP + FN} = \frac{0.67}{0.67 + 0.33} = 0.67$$

F1 Score:

$$F1 = 2 \times \frac{Precision \times recall}{Precision + recall} = 0.73$$

The following figures show the classification results through visual representations of the confusion matrix and reveal where the confusion occurs between both false positive and false negative predictions for each model. The reason for these false predictions is due to the not having enough

images of the same type of signature as it is expected to have much lower false predictions if provided.

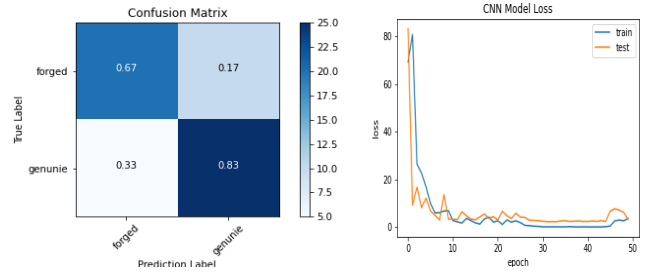


Fig. 7. Our CNN Model Confusion Matrix and Loss Curve

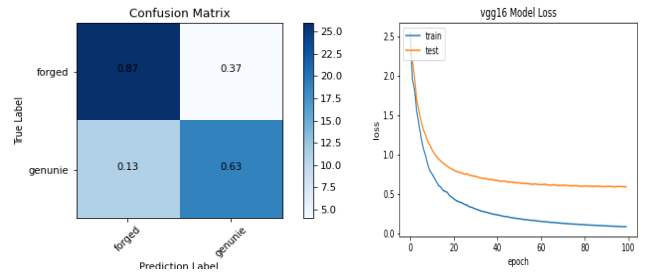


Fig. 8. VGG16 Confusion Matrix and Loss Curve

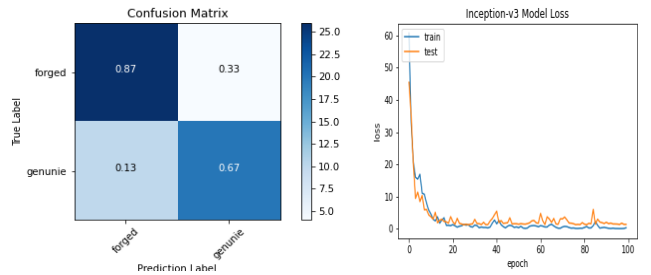


Fig. 9. Inception-v3 Confusion Matrix and Loss Curve

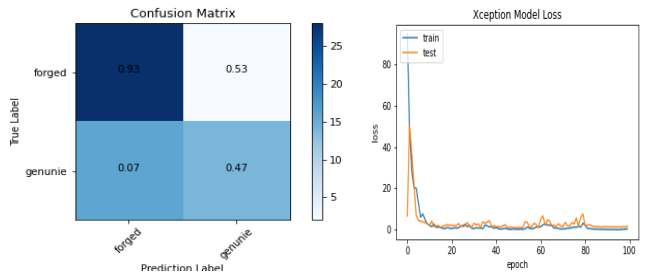


Fig. 10. Xception Confusion Matrix and Loss Curve

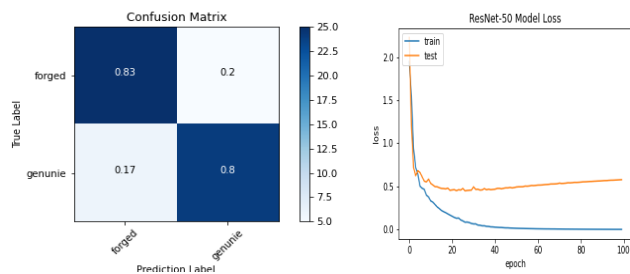


Fig. 11. ResNet50 Confusion Matrix and Loss Curve for **Experiment 1**

As for the second experiment, we used the model with the highest rating from the first experiment, which is the ResNet50 model. After testing the ResNet50 model on the newly collected dataset, which was able to reach a higher precision score since the model is performing on a lower number of signature images from the second dataset. The accuracy reached by this model is 86% which is relatively close compared to a recent work presented by Poddara et al. [14] on using CNN combined with Crest-Trough method, SURF algorithm, and Harris Corner detection algorithms to achieve an accuracy of 85% - 89% for forgery detection of offline signatures.

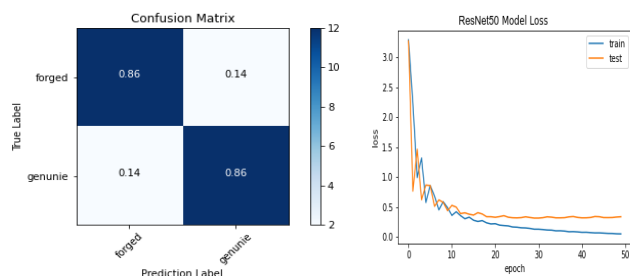


Fig. 12. ResNet50 Confusion Matrix and Loss Curve for **Experiment 2**

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed five different CNN classification models to determine which is the best-performing model for binary image classification of handwritten signatures inside documents. After testing each model, we concluded that the ResNet50 model has achieved the best results compared to the other CNN models regarding the classification of text-based images where it was able to reach an accuracy of 82.3% and 86% conducted on two datasets which contained samples of 300 and 140 handwritten signature images respectively.

Regarding future work, this paper provides useful information for suggesting the ResNet50 model and encourages further analysis that includes not binary but categorical classifications of handwritten signatures by utilizing different signature aspects and characteristics.

REFERENCES

- [1] G. C. Praba, E. Jeevitha, A. Abitha, A. Shalini, and B. Swetha, "Fake education document detection using image processing and deep learning," *International Journal of Engineering Research Technology*, vol. 9, no. 5, Mar 2021. [Online]. Available: <https://www.ijert.org/research/fake-education-document-detection-using-image-processing-and-deep-learning-IJERTCONV9IS05018.pdf>, <https://www.ijert.org/fake-education-document-detection-using-image-processing-and-deep-learning>
- [2] H. James, O. Gupta, and D. Raviv, "OCR graph features for manipulation detection in documents," *CoRR*, vol. abs/2009.05158, 2020. [Online]. Available: <https://arxiv.org/abs/2009.05158>
- [3] M. Yoosuf and R. Anitha, "Forgery document detection in information management system using cognitive techniques," *Journal of Intelligent Fuzzy Systems*, vol. 39, pp. 8057–8068, 12 2020.
- [4] P. Roy and S. Bag, "Forensic performance on handwriting to identify forgery owing to word alteration," 01 2019, pp. 1–9.
- [5] Y. Abdalla, M. T. Iqbal, and M. Shehata, "Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network," *Information*, vol. 10, no. 9, 2019. [Online]. Available: <https://www.mdpi.com/2078-2489/10/9/286>
- [6] M. Khan, A. Yousaf, A. Abbas, and K. Khurshid, "Deep learning for automated forgery detection in hyperspectral document images," *Journal of Electronic Imaging*, vol. 27, p. 053001, 09 2018.
- [7] S. Ranjan, P. Garhwal, A. Bhan, M. Arora, and A. Mehra, "Framework for image forgery detection and classification using machine learning," 06 2018, pp. 1872–1877.
- [8] P. Adi and M. Luthfi, "An authentic and secure printed document from forgery attack by combining perceptual hash and optical character recognition," 10 2019, pp. 157–162.
- [9] J. Bunk, J. H. Bappy, T. M. Mohammed, L. Nataraj, A. Flenner, B. Manjunath, S. Chandrasekaran, A. K. Roy-Chowdhury, and L. Peterson, "Detection and localization of image forgeries using resampling features and deep learning," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, Jul 2017, p. 1881–1889. [Online]. Available: <http://ieeexplore.ieee.org/document/8014969/>
- [10] R. Vieira, C. Silva, M. Antunes, and A. Assis, "Information system for automation of counterfeited documents images correlation," *Procedia Computer Science*, vol. 100, pp. 421–428, 2016, international Conference on ENTERprise Information Systems/International Conference on Project MANagement/International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN / HCist 2016. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050916323468>
- [11] A. Ghosh, D. Zou, M. Singh, and Verisk, "Detection and localization of image and document forgery : Survey and benchmarking," 2016.
- [12] S. Shang, N. Memon, and X. Kong, "Detecting documents forged by printing and copying," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, p. 140, Sep 2014. [Online]. Available: <https://doi.org/10.1186/1687-6180-2014-140>
- [13] R. Bertrand, P. Gomez-Krämer, O. R. Terrades, P. Franco, and J.-M. Ogier, "A system based on intrinsic features for fraudulent document detection," in *2013 12th International Conference on Document Analysis and Recognition*, 2013, pp. 106–110.
- [14] J. Poddar, V. Parikh, and D. Bharti, "Offline signature recognition and forgery detection using deep learning," *Procedia Computer Science*, vol. 170, pp. 610–617, 01 2020.
- [15] H.-H. Kao and C.-Y. Wen, "An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach," *Applied Sciences*, vol. 10, no. 11, 2020. [Online]. Available: <https://www.mdpi.com/2076-3417/10/11/3716>
- [16] P. Wei, H. Li, and P. Hu, "Inverse discriminative networks for handwritten signature verification," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 5757–5765.
- [17] S. Pokharell, S. Giri, and S. Shakya, "Deep learning based handwritten signature recognition," 02 2020.