INTELLIGENT SYSTEM FOR NEURAL NETWORK DETECTION OF FAKE DOCUMENT IMAGES FOR AUTOMATED PERSONALITY IDENTIFICATION

Oleksandr Zharnovskyi,
student of "Computer Science" specialty
Khmelnytskyi National University,

Olena Sobko,
teacher of Computer Science
Khmelnytskyi National University,

Valeriia Klimenko,
teacher of Computer Science
Khmelnytskyi National University,

In the modern digital world, identity verification through photo images of documents is becoming increasingly crucial. The growing number of online transactions creates new opportunities for fraud. Identity verification helps protect users from these threats.

For example, identity verification based on photo images of documents assists banks and credit companies in preventing fraud related to credit cards, bank accounts, and loans. Additionally, identity verification aids online retailers in safeguarding their customers from fraud such as credit card theft and the compromise of personal data. Citizens can also use document photo images to access social benefits and avail themselves of government services.

The circulation of documents in any format poses potential threats, ranging from the possession of multiple copies of a single document by various official entities to full-fledged forgery. These threats vary from simple alterations, such as erasure (mechanical removal of parts of the document), overprinting (application of new words or printing over existing ones), to sheet replacement (in cases where the document comprises multiple sheets). While traces of rubbing or overprinting in areas with requisites may be detectable without expert examination, complete document replacement or forgery requires more detailed attention.

To prevent forgery, several fundamental types of protection are employed [1]. Any document with bureaucratic value utilizes a combination of these methods, including personal identification documents. The mandatory document for every citizen of Ukraine, the passport, serves as one of the best examples of a widely circulated document with a plethora of protective measures (Figure 1).

Figure 1. Protective measures on the Ukrainian citizen's passport card [2]

Indeed, for the task of developing a neural network method to detect fake images of identification documents for personal identification systems, there are numerous parameters available for identifying forged identification document images.

In general, the methods of generating fake images of documents do not significantly differ from the creation of conventional fake images using graphic editors or similar tools.

When manipulating images of various nature, such as in Photoshop or Paint.net, errors are typically introduced in the editing process and/or in the metadata. Metadata refers to additional information embedded in an image file, including camera type, color profile details, and more.

These errors can be leveraged for image analysis to detect modifications through a combination of Error Level Analysis (ELA) and Convolutional Neural Networks (CNN) in the functional components of a system designed to identify fake document images (Figure 2).

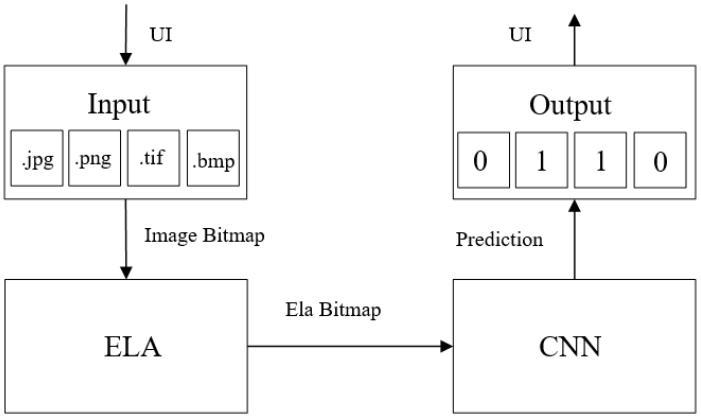

Figure 2. Generalized scheme of the neural network method for detecting fake document images

The input method facilitates user interaction, allowing the uploading of a selected image through the User Interface (UI) and specifying corresponding parameters.

ELA / Error Level Analysis is one of the methods for identifying changes in an image through compression at a specified quality level and comparing it with the

original. If the image has not been edited, the error should be consistent across each individual segment. Otherwise, edited areas will be highlighted (Figure 3).

Figure 3. Example of ELA for a fake image with highlighted splice zone

The task of the functional method is to preserve the input image with a user-specified quality, compare them, and generate an Error Level Analysis (ELA) to be subsequently utilized by the neural network (Figure 4).

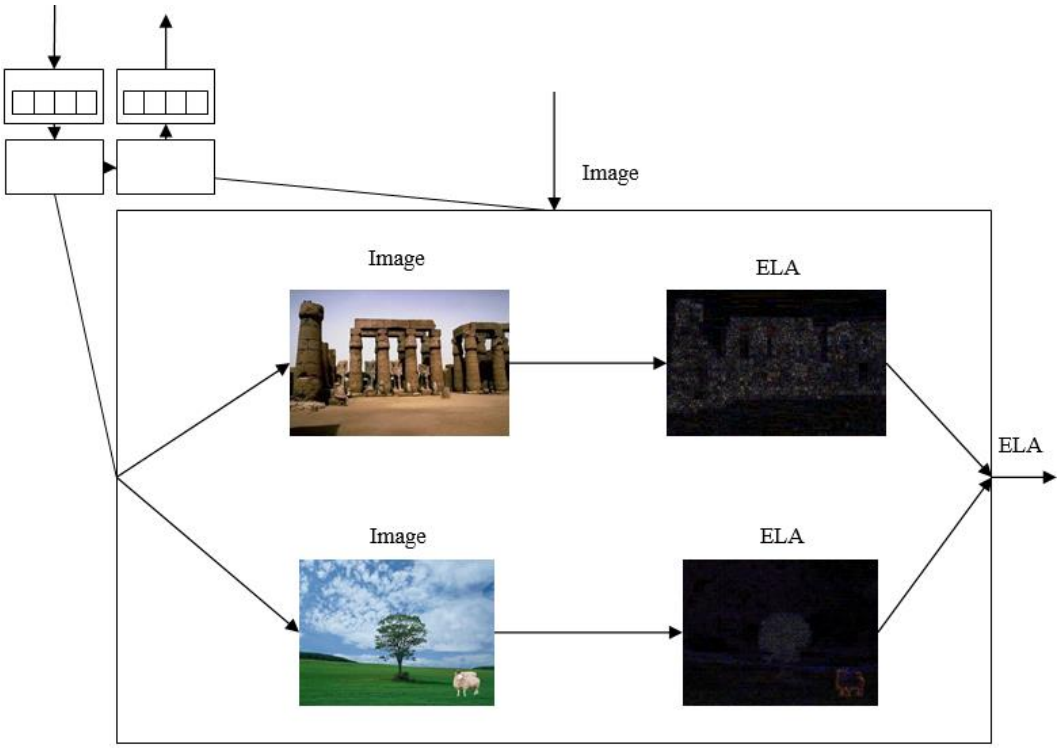

Figure 4. Functionality of the ELA module

Thus, a method for neural network detection of fake document images for personal identification systems has been described.

For the proper functioning of the neural network, training is an obligatory and exceptionally crucial stage. Training enables the network to classify input images

based on the provided examples during the learning process, and depending on the correct configuration of the training process, the network will make accurate or inaccurate conclusions [3].

For the proper functioning of the Neural Network (NM), an important stage in development is the selection of an appropriate dataset on which the network will be trained – the dataset. For the training and testing of the network, the CASSIA2 [4] and MIDV [5] datasets were utilized.

The obtained dataset needs preprocessing – all files have different extensions, formats, and qualities; they need to be standardized and classified for further use by the neural network.

Classification is the process of categorizing the acquired images into classes, which will then be fed into the network. In this case, these classes correspond to "authentic image" and "forged image."

Additionally, the dataset needs to be randomly split into three parts – training, validation, and testing – at each iteration of the model (Figure 5).

Figure 5. Example of dataset splitting

The structure of the network is divided into fundamental functional layers:

Convolution Layer. This is the initial layer used for feature extraction from the image, producing a feature map for further processing by other layers of the network.

Pooling Layer. Typically used after convolution, its function is to reduce the dimensions of the feature map, minimizing computational requirements and accelerating the network's operation while reducing the computer's resource demands.

Fully Connected Layer. Exists to connect different layers of the neural network, where the images are flattened and passed to the next layer, commonly utilized just before the output layer.

Dropout. To prevent overfitting, this layer is employed to randomly remove a portion of neurons from the network, reducing its size.

By combining these layers, an architecture for identifying fake document images has been created (Figure. 6).

For the practical implementation of the fake document image identification method, a class diagram was created according to the expected functionality (Figure. 7).

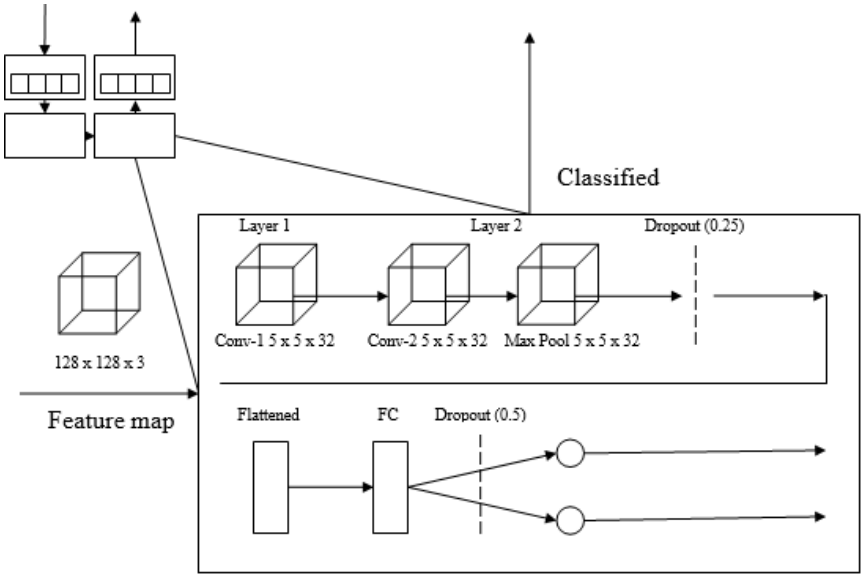

Figure 6. The architecture of a neural network

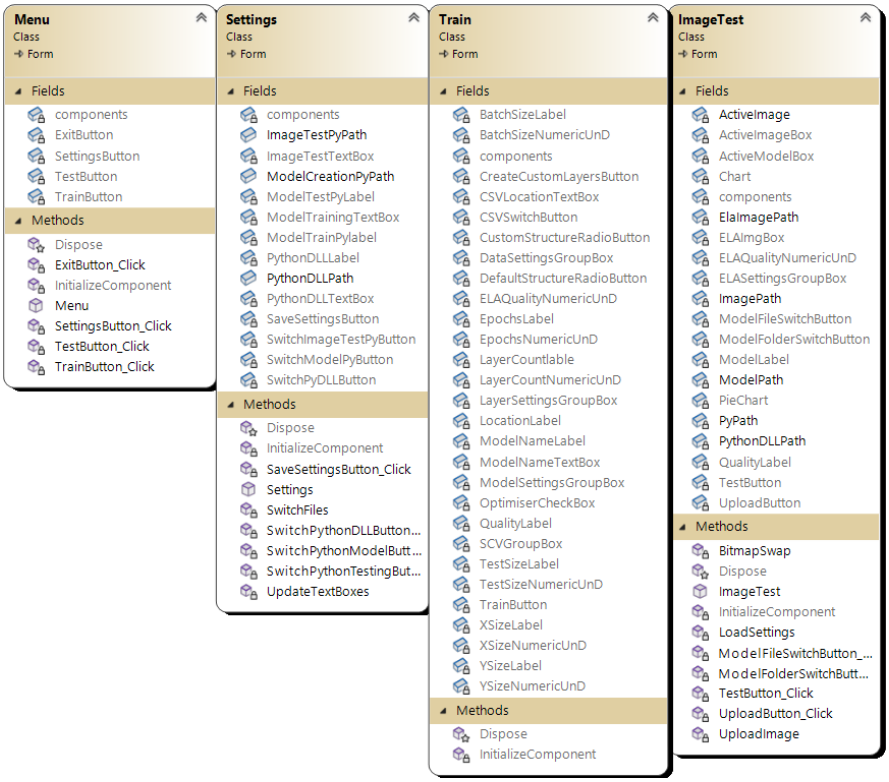

Figure 7. Class diagram

The methods SettingsButton_Click, TestButton_Click, and TrainButton_Click allow transitioning to the selected form upon pressing the respective button.

The Settings class contains methods for modifying the paths to Python classes and the necessary DLL file required for their operation. Changes are stored in a txt file format, which will be subsequently loaded by other modules during further operation and will be preserved in case of program reload (Figure 8).

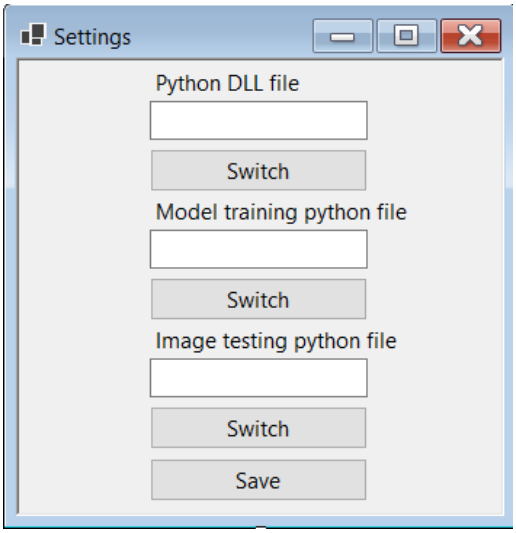

Figure 8. Interface of the Settings class

In the Train class, the logic for configuration, creation, training of the Convolutional Neural Network (CNN), and its preservation for subsequent use is implemented (Figure 9).

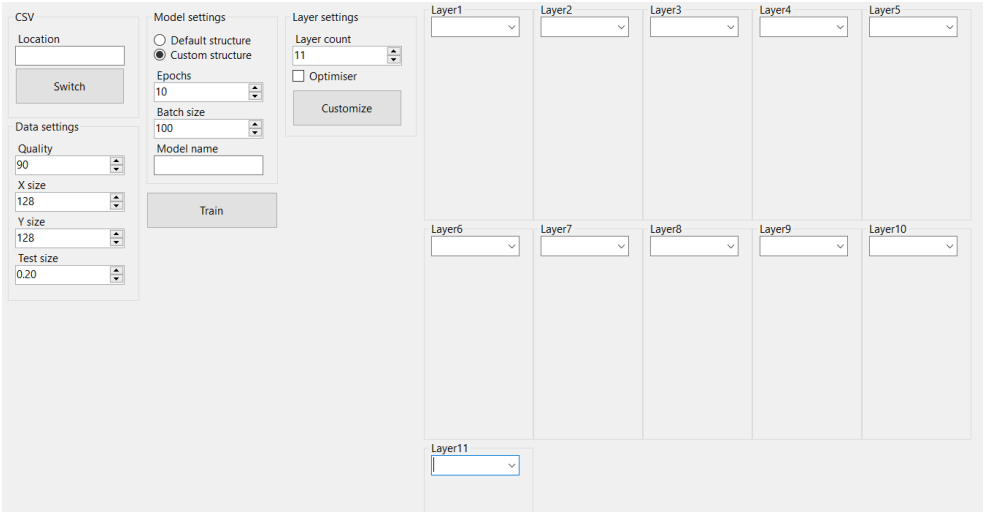

Figure 9. Interface of the Train class

The class ImageTest serves to verify the authenticity of a selected document image using the trained neural network.

To investigate the effectiveness of the developed neural network method for detecting document images, a neural network was trained and tested with a chosen structure and modification of its key parameters before the training process.

Testing the model with the following input parameters:

Number of epochs – 20.

Batch size – 150.

Test-validation data split 65:35.

Training results (Fig. 19).

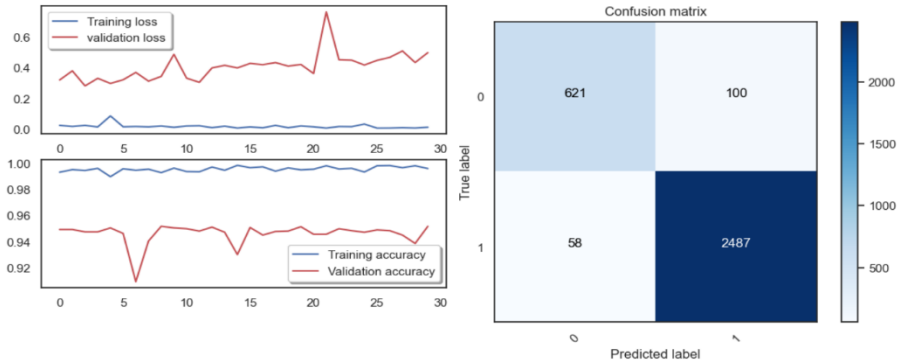

Figure 9. Graphs and confusion matrix of the obtained network

Therefore, the effectiveness of CNN models was examined with variations in size parameters, the number of epochs, and the proportion of image distribution. It was determined that with the parameters: number of epochs – 20, batch size – 150, and a 65:35 split of test and validation data, favorable results were obtained.

The outcome of the work is the developed method for neural network detection of fake document images and an information system for personal identification. The system utilizes the developed method and allows for the automated assessment of the authenticity level of a photographed identity document image using the developed approach.

The research has demonstrated that the method achieves an accuracy of 95.16%. The developed information system for detecting fake document images can be an effective means of preventing fraud in personal identification systems. It can aid in identifying forged document images that may be used for identity theft, credit card fraud, or other criminal activities.

References:

1. Core.ac.uk. Document types and protection methods. URL: https://core.ac.uk/download/pdf/12241561.pdf

2. Dmsu. Ukraine ID card protection layers. URL: https://dmsu.gov.ua/faq/biometrichni-dokumenti-v-ukrajni/yaka-stupin-zaxistu-u-biometrichnix-dokumentiv.html

3. Slobodzian V., Molchanova M., Kovalchuk O., Sobko O., Mazurets O., Barmak O., Krak I. An Approach Based on the Visualization Model for the Ukrainian Web Content Classification. 2022 12th International Conference on Advanced Computer Information Technologies, ACIT 2022. 2022. pp. 400-405. DOI: 10.1109/ACIT54803.2022.9913162. URL: https://ieeexplore.ieee.org/document/9913162

4. Kaggle. Cassia2 dataset. URL: https://www.kaggle.com/datasets/sophatvathana/casia-dataset

5.PapersWithCode. MIDV-500 dataset. URL: https://paperswithcode.com/dataset/midv-500