прогнозування кібератак має значний потенціал для підвищення безпеки мережевих систем та своєчасного запобігання інцидентам.

References

1. Столяр А. Л. Аналіз сучасних методів виявлення аномалій в комп'ютерних мережах. 2023, URL: https://doi.org/10.18372/2073-4751.74.17888.
2. Sunanda Gamage, Jagath Samarabandu. Deep learning methods in network intrusion detection: A survey and an objective comparison. 2020, URL: https://doi.org/10.1016/j.jnca.2020.102767
3. Mujaheed Abdullahi, Yahia Baashar, Hitham Alhussian. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. 2022, URL: https://doi.org/10.3390/electronics11020198
4. Nachaat Mohamed. Current trends in AI and ML for cybersecurity: A state-of-the-art survey". 2023, URL: https://doi.org/10.1080/23311916.2023.2272358

APPROACH TO IDENTIFICATION OF ARTIFICIAL INTELLIGENCE-GENERATED PEOPLE IMAGES BY MEANS OF MACHINE LEARNING

Zharnovskyi Oleksandr
Postgraduate student
Mazurets Oleksandr
Ph.D in Engineering Science, Associate Professor
Sobko Olena
Teacher
Computer Science Department
Khmelnytskyi National University, Ukraine

Artificial image generation technology has a wide range of applications, artificial image generators such as Midjourney, StableDiffusion, Adobe FIrefly, FLUX, Runaway can greatly simplify a large number of areas of human activity [1].

Some of the most popular fields of activity using artificial image generation are marketing – where artificial images can replace a photo shoot for a new product and create personalized advertising, medicine – which allows improving image diagnostics by creating clearer images, art and design – artists can use generative AI to create references, base image or less important background elements.

As images become more and more realistic, the creation of deep fakes becomes one of the biggest problems and threats to the existence of open tools [2, 3], which is why the development of methods for identifying generated images is relevant [4, 5].

The proposed method uses a combination of two convolutional neural networks that are excellent for the task of image analysis (Figure 1). The input image is

classified into real and generated, in case the generated image the neural network tries to find matches with known image generators (Figure 2, 3).

Images of people's faces combined with images created by five popular image generators, namely Midjourney, Stable diffusion, Dalle-3, Dreamstudio, Craiyon, will be used as datasets [6].

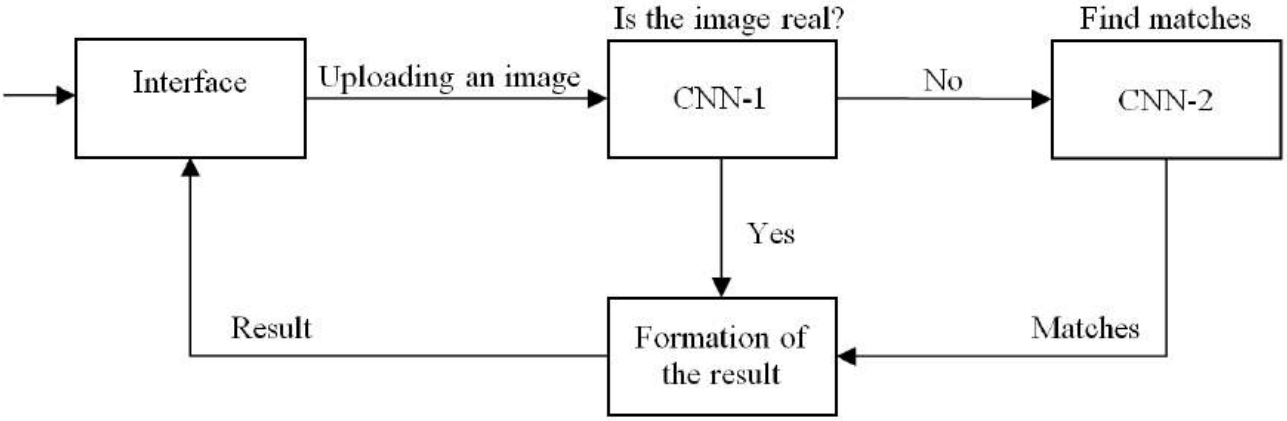

Figure 1. Approach to identification of artificial intelligence-generated people images by means of machine learning.

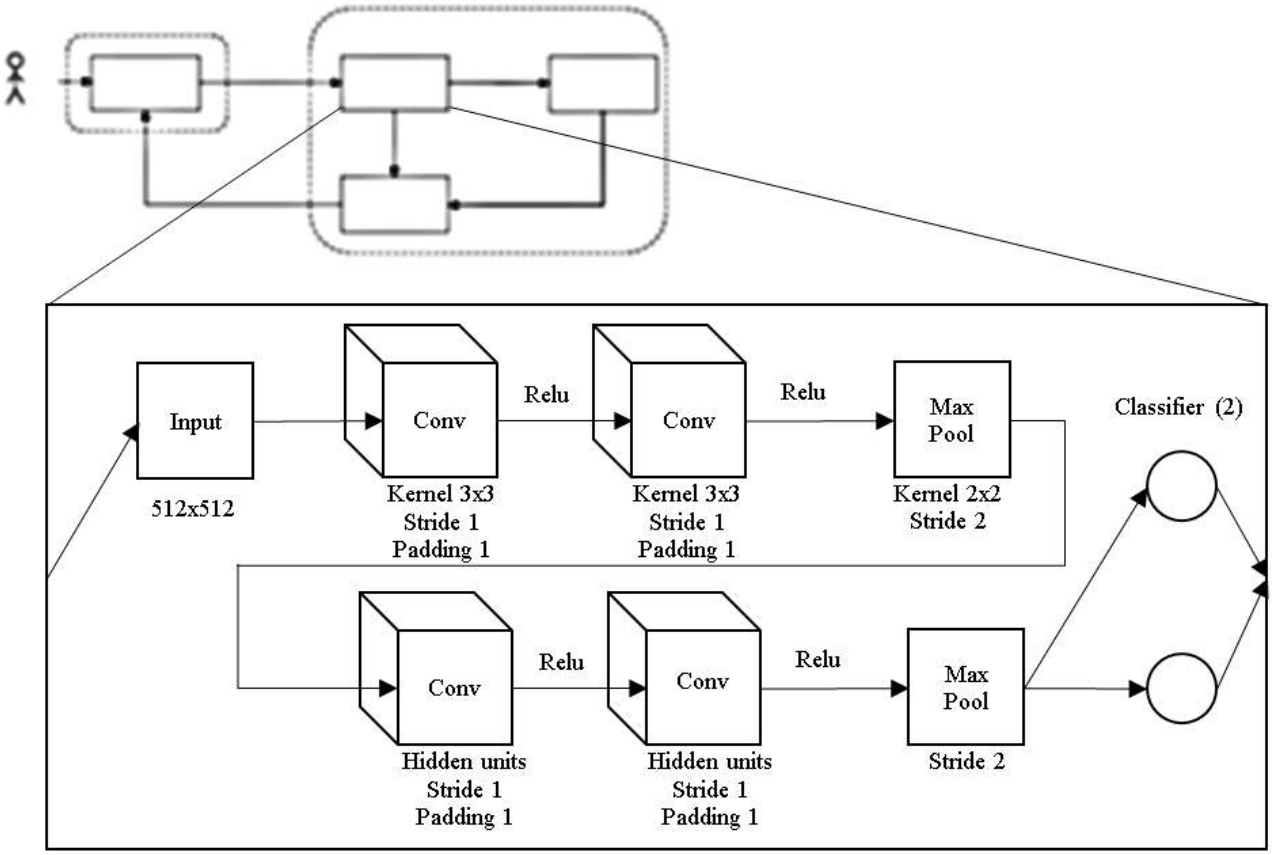

Figure 2. Architecture of CNN neural network model for basic classification of generated images.

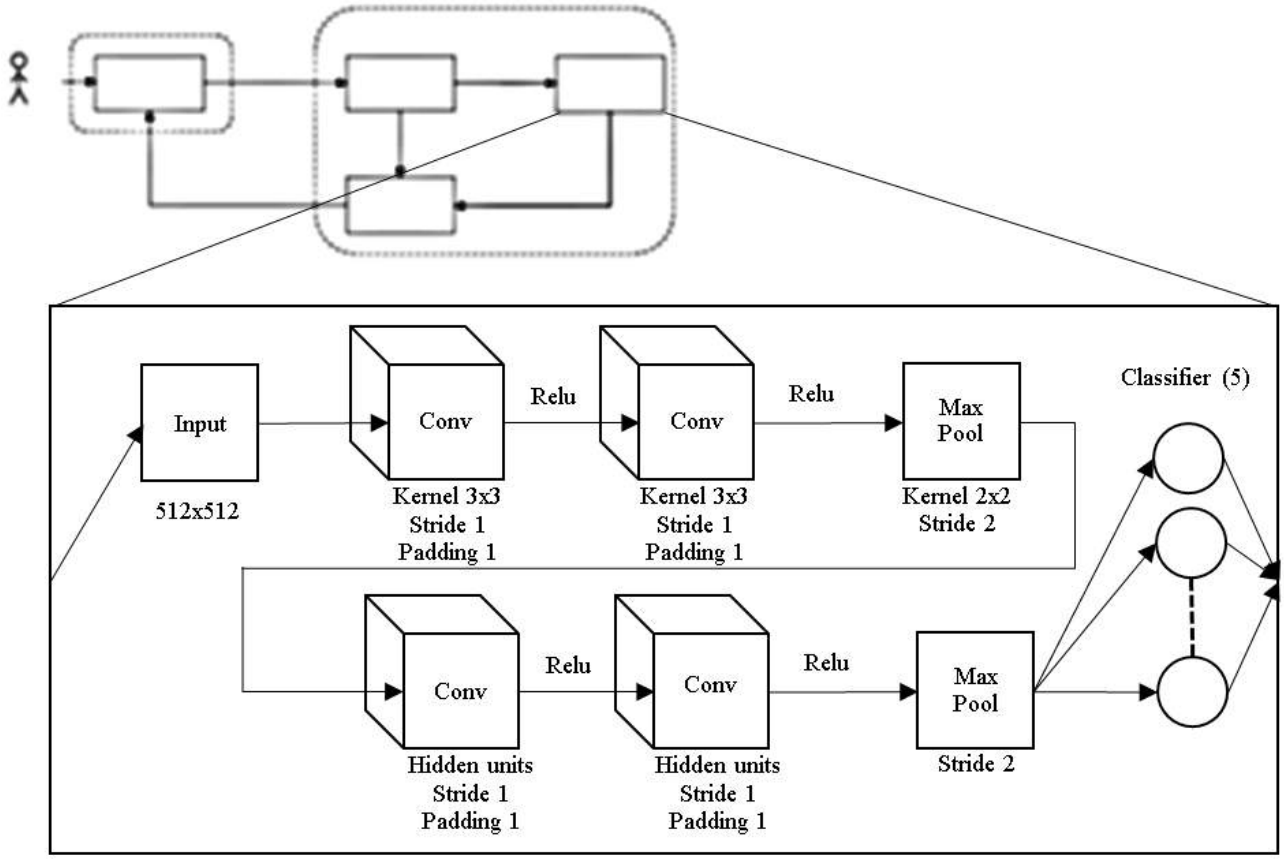

Figure 3. Architecture of CNN neural network model for detailed classification of generated images.

The architecture of convolutional neural networks consists of the following layers:

– activation layer – contains the activation function, usually used after convolution;

– pool layer – reduces image size without significant loss of information, usually used in the middle of the network;

- fully connected layer – perform classification based on features obtained by the previous layer, usually used after convolution and pool layer;

– normalization layer – contains the normalization function, stabilizes training, is used after the activation function;

– screening layer – randomly disconnects artificial neurons from the network, serves to prevent retraining;

– loss layer – determines the level of error between the original result and the expected one;

– output layer – the last layer in the network, the number depends on the number of expected output classes of the network.

The combination of these layers allows creating a functional network architecture for the proposed method [7].

The ready-made TorchVision library was used for the software implementation of the CNN architecture.

TorchVision is a library consisting of popular datasets, model architectures, and image transformation functions for computer vision tasks. It consists of: learning

methods for object detection, image classification, instance segmentation, video classification and semantic segmentation.

Supervised machine learning requires labeled input when training a machine learning model. This training data is labeled by the developer in the training phase before being used to train and test the model. Once the model has learned the relationship between input and output data, it can be used to classify new and unknown data sets and predict outcomes. Unsupervised learning (clustering) – learning on raw and unlabeled training data. It is often used to identify patterns and trends in raw data sets or to cluster similar data into a certain number of groups. Less important parameters for training neural networks are the number of epochs and the group size. The number of epochs is responsible for the training cycles that the network goes through, and the size of the group is how much data it receives in one cycle. If the number of epochs is multiplied by the size of the group more than the taken dataset, part of the data will be reused, which can lead to retraining (Figure 4). Optimal values are determined during training.

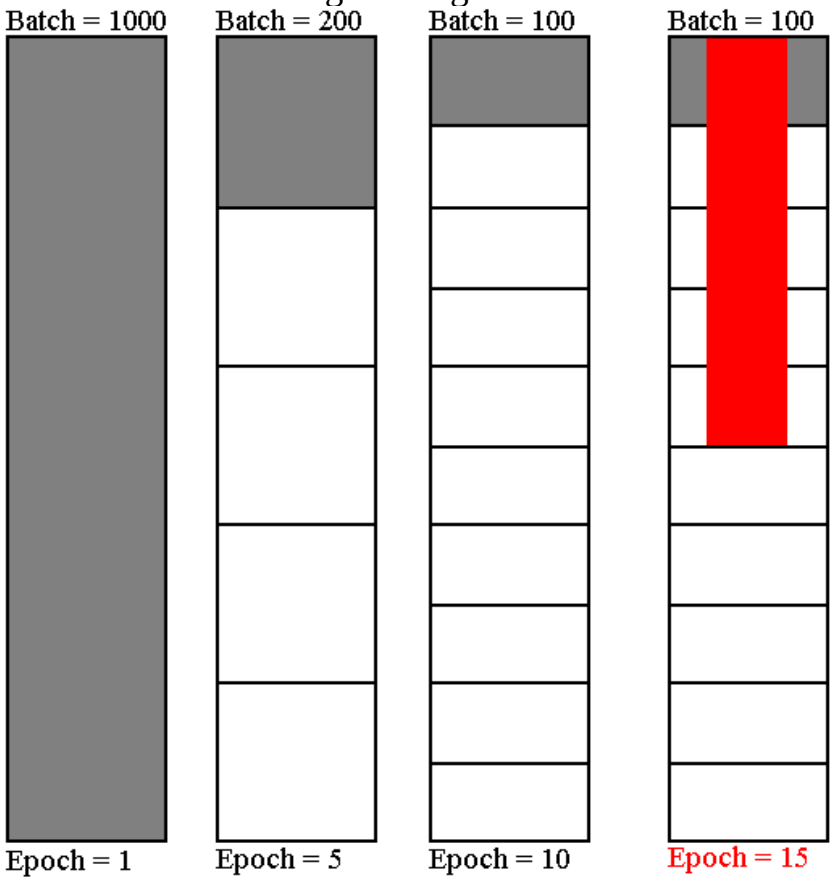

Figure 4. Dependence on the number of epochs and the size of the group.

For the CNN-1 network, whose task is to classify images into real and generated ones, the data needs to be grouped into two classes. In turn, CNN-2 will try to assign the input image to one of them.

So, the result of the work is the development of a method of identification of images of people generated by artificial intelligence by means of machine learning. The developed method allows for efficient image identification and can be integrated into mass media and social networks for automatic verification of image authenticity.

In addition, the network can be constantly improved and adapted to new methods of image generation to prevent the spread of false information.

References

1. Zharnovskyi O., Sobko O., Klimenko V. Intelligent System for Neural Network Detection of Fake Document Images for Automated Personality Identification. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 337-343.
2. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
3. Mazurets O., Molchanova M., Klimenko V., Klopotivskyi D. Datalogic Model for Image Recognition by Convolutional Neural Network Using Cloud Services. Proceedings of XXII International Scientific and Practical Conference «Modern Scientific Research: Theoretical and Practical Aspects». May 8-10, 2024. Oslo, Norway. 2024. Pp. 64-68.
4. Molchanova M., Mazurets O., Klimenko V., Kuflevsky Ev. Object-oriented model for neural network damage detection of mail packages. Proceedings of XIV International Scientific and Practical Conference «Solving Scientific Problems Using Innovative Concepts». March 13-15, 2024. Copenhagen, Denmark. 2024. Pp. 58-62.
5. Novak Y., Mazurets O. Practical Application of Method of Automated Personal Identification by Fingerprints Using Convolution Neural Networks. Proceedings of V International Scientific and Practical Conference «Modern strategies of global scientific solutions». December 27-29, 2023. Stockholm, Sweden, International Scientific Unity. 2023. Pp. 136-140.
6. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
7. Mazurets O., Zalutska O., Tyschenko O., Bohdanova A. An Approach to Using MobileNet CNN-model for Gesture Recognition. Proceedings of XXIII International Scientific and Practical Conference «Problems of Science and Technology: the Search for Innovative Solutions». May 15-17, 2024. Munich, Germany. 2024. Pp. 59-64.