Case #1 “Who took this photo?”

It has been a long time that neural networks learned to generate high-quality photo and even video images. Will you be able to distinguish an existing person from one generated by a neural network? Most likely, you will have a hard time doing it. Will your neural network be able to identify a fake? Let’s check it!

Below you will find data sets containing thousands of faces: some of them are real, while others are fake, that is, generated by artificial intelligence. **You are invited to resolve a problem of binary classification of images: identify pictures that show real people, and those that do not.**

The fake recognition technology is very useful for security solutions, for checking media publications, for verification of user of various services and social media, and, paradoxical as it may sound, for improving the performance of neural networks that generate the images. They, in turn, have a huge potential to be used in cinema, games, social media and other spheres.

By the way, there are numerous resources allowing you to test your natural intelligence capacities in terms of distinguishing real and artificial faces, for example, here.

> The face is a mirror of the soul
>
> **Marcus Tullius Cicero**

Data

In order to resolve your problem, we offer the following materials:

1. The **data256faces.tar.gz** image archive, where you will find two data sets:
   - **train** is the training sample, which you will use to train your model (the sample size is 8,000 images);
   - **test** is the testing sample, for which you will need to make a prediction and upload it to the platform for verification (12,000 images).
2. The **train.csv** file for model training and parameter setup, which contains the right answer for every image from the ‘train’ (1 - fake image, 0 - real image).
3. The solution upload example file **submit.csv** (you will have to upload a file with the same number of rows and columns to the platform, when it becomes possible to upload solutions).
4. In addition to that, you have access to the basic solution by the problem developers.

Download the data

Solution format

For verification, you will need to upload the **submit.csv** file containing the columns **'name'** and **'pred'**:

1. The **"name"** column should specify the image ID.

2. The **"pred"** (abbreviated from «prediction») column should specify the probability of the image being a fake one (the higher the probability, the higher the confidence that the image is fake: 1 - maximum, 0- minimum).

The file should be sorted by the **'name'** column.

The predictions must be made for all test (from the test data set) images (see submit.csv for example).

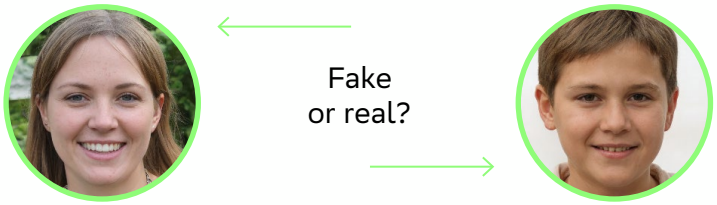
The solution quality shall be determined by the 'accuracy' metric:

Acc = (# number of images the class of which was guessed correctly) /
(# total number of images for which the prediction was made)

The image class (by probability p in the 'pred' column) shall be determined as follows:

1. if 0 <= p <0.5, then 0 (the image is real);

2. if 0.5<= p <=1, then 1 (the image is fake)



Please note: to pass to the next stage, you will have to improve the basic solution or suggest your own, which resolves the problem with the required result or better.

Supplementary materials

To learn basics of ML you can try Stanford's course on Coursera.

We also recommend you to study the basics of PyTorch in more depth.