# First paragraph

The authentication system is a system that involves verifying the identity that the one is claiming. The main difference between a system for authentication and identification is that the first require confirming, that given credentials of the subject corresponds to the template of proposed identity, and therefore a task of binary classification in such system is presumed. At the same time, in identification system the goal is to recognize the person from some dataset of subjects, so multiclass classification in such system is presumed. It is obvious that the identification approach would be too complex to use in a real-world system with many users. First of all, usage of machine learning is a popular approach for users’ classification. Therefore, it narrows the opportunities of using such technologies of machine learning as neural networks, since multiclass classification increases the computational cost, while performing the worse results than binary classification. It was proven in [10] that identification system performs lower accuracy than authentication system, even though the same input data was used. Moreover, usually identification systems are not intended for adding new users easily to the system, since it would require to change an output of the whole system and retrain it from scratch.

Authentication systems, in which different biometric, i.e. person’s anatomical features (fingerprints, face, palm veins, hand geometry, iris, voice) or behavioral traits (signatures, gaits, etc.), are used as credentials, are called biometric authentication systems. Because such type of data is physically user-related and is hard to steal, biometric authentication systems are claimed to be one of the most reliable ones. However, all aforementioned biometrics are could be faked. One of the perspective types of biometrics recently has proved to be electroencephalogram (EEG) of brain activity. As long as it is recorded from a human head, it is hard to reproduce such signal.

The reliability of biometric authentication system could be judged by False Accepted Rate (FAR) - the rate of successful authentications of impostors, and False Rejected Rate (FRR) - the rate of denied accesses for registered users. As long as the wrong person should never be authenticated, FAR is the most important for authentication system, and should be as low as possible.

# Second paragraph

In the last 20 years, in numerous studies different approaches of using EEG data as biometrics for authentication of the subjects were proposed.

Poulos et al. [] proposed the first authentication system in 1999. They collected a 3-minutes recording of a resting state with closed eyes (REC) from 4 subjects with 45 recording for each, and 75 imposters with 1 recording for each. Auto-Regression and Moving Average model (ARMA) was used for feature extraction, and the Kohonen’s Linear Vector Quantizer model of neural network was trained for binary classification. However, they obtained pretty high average FRR of 0.22 and extremely high for authentication FAR of 0.2, and therefore this system is inappropriate for a real-world authentication system.

Marcel et al. [] collected EEG data from 9 subjects during 12 sessions over 3 days. During the recording, subjects performed different mental tasks: imagining left and right hand movement, and generating the word that starts with same random letter. For forming a feature vector, PSD was extracted from 12 frequency bands for 8 chosen channels. For classification, Maximum A Posteriori model (MAP) was used. They obtained a lot of results from different experimental protocols, with the approximate average FRR and FAR of the best protocols at the level of 0.08 and 0.1 respectively. Interestingly, the task of imagining left hand moving performed the best results.

Hu et al. also used recordings of different imaginary tasks, but collected data only from 3 subjects. Feature vector was extracted from an ARMA linear model, as in [Poulos], and neural network with 5 hidden layers was used to classify the subjects. The FRR varied from 0.15 to 0.25, however, the results FAR were not presented in this paper, so it is hard to judge on reliability of the built systems.

Yeom et al. collected data from 10 users, where self-face and non-self-face images were used as a stimulus. Interestingly, that 2 twins were among these subjects. For input vector, they extracted so-called ‘temporal’ and ‘dynamic’ features from 18 selected channels, and used Support Vector Machine for classification. The average FAR and FRR of 13.9 was obtained.

The most recent work was presented by Wu et al. They collected EEG and EOG signals from 40 persons (15 as users and 30 as impostors), and used rapid serial visual presentation of faces (face-RSVP) as a stimulus. They then compared systems based on EEG only and the combination of EEG and EOG. However, we are interested in using the EEG signal only, and therefore the above explanation applies only for this system. In the Wu et al. system, unlike aforementioned systems, feature matrix, not a vector, was former for classification. As features, the average ERPs were used for specifically chosen channels. For classification, the convolution neural network was used. However, for this purposed feature matrix was expanded into a square matrix by the sparse method, which is an arguable method to use when forming an input for neural network. The average FAR was around 0.062 and FRR around 8.49.

# Third paragraph

It is well known that authentication require the more consistent data, and in works [citations] it has been proven that one of the most consistent types of recorded EEG data is recordings during motor activity. Therefore, we proposed to use motor activity stimulus in order to achieve better accuracy and create more reliable system in terms of consistency of the input data.

We did not do any channels’ selection for information safety reasons. One of the methods of avoiding leaving the information that could be important is to use all channels and as much as possible features. However, we got a high dimensional matrix of features. As long as neural network has proven to deal with classifying a high dimensional data with a high accuracy and low computational cost (comparing to other machine learning algorithms) [10][11], in this work it was proposed to use it as a classifier.

Moreover, in a lot of studies (for example [13], [14]), a method of improving the accuracy of classification by using the combination of neural network and Support Vector Machine (SVM) was proposed. Thus, this method was used in our work as well.

Furthermore, a Principal Component Analysis (PCA), just as neural network, could be used for convoluting correlated set of variables into the new, smaller set of variables [15]. Therefore, in this work a PCA was used in a combination with SVM for classification as well.