**Layout of biometric voice authentication "OWN/ALLIEN" using a passphrase**

The main file for interpreting the layout is called «Voice\_Auth\_With\_Password.py». When the script is launched, the speech-to-text model is initialized and the main program window is launched (Figure 1).

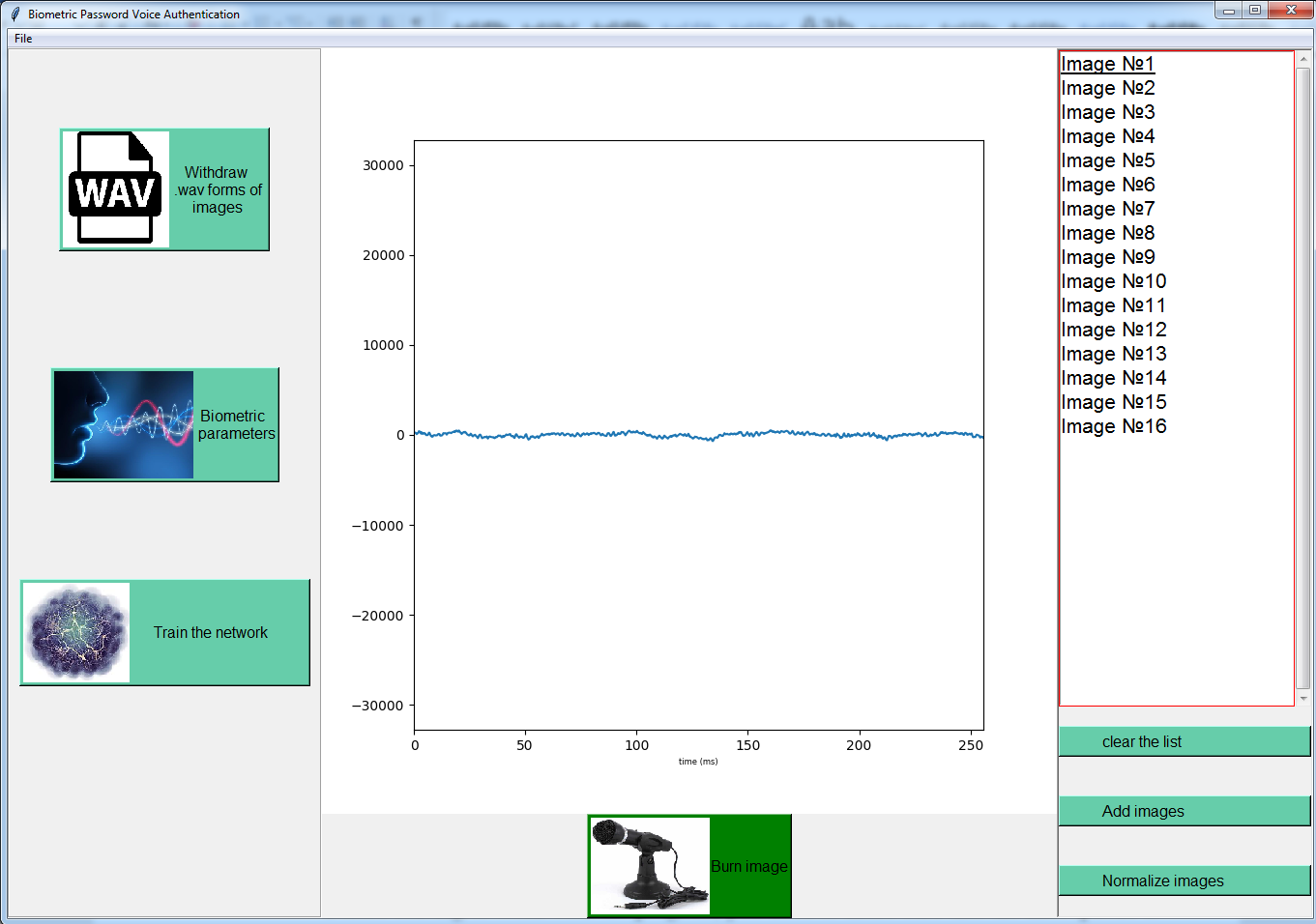


Figure 1 - The main window of the layout

Before starting to work with the program, you need to make sure that the microphone is working and positioned. It is recommended to take images in a quiet room, or from a microphone without an amplifier, so that in silence there is a band that fluctuates around zero. Next, you need to make sure the loudness of the pronunciation so that the final image does not turn out to be too loud or too quiet (Figure 2). If the signal goes beyond the window, you need to move the main microphone away from you, otherwise - move closer to it.

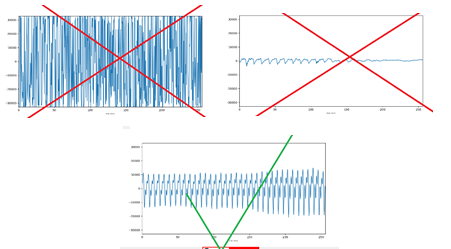


Figure 2 - Checking the microphone volume level

In the middle of the lower part of the window there is a record button with a microphone icon “Record image”. When you click on it, the recording starts. To end the recording, you must click on the same modified button "Stop recording" (Figure 3)



Рисунок 3 – Остановка записи

After the end of the recording, the recorded image will appear on the right side of the layout, which you can listen to, view the .wav-form and delete if the image is unsuccessful for some reason. You can listen to each image and make sure that the passphrase is pronounced correctly and that there is no interference. Also, if the image signal goes beyond the window, it means that the user is speaking too loudly into the microphone.

Having accumulated the training sample (8-16 images), you can visually check all the images on one screen by clicking on the button "Display .wav-forms of images" (example - Figure 4).

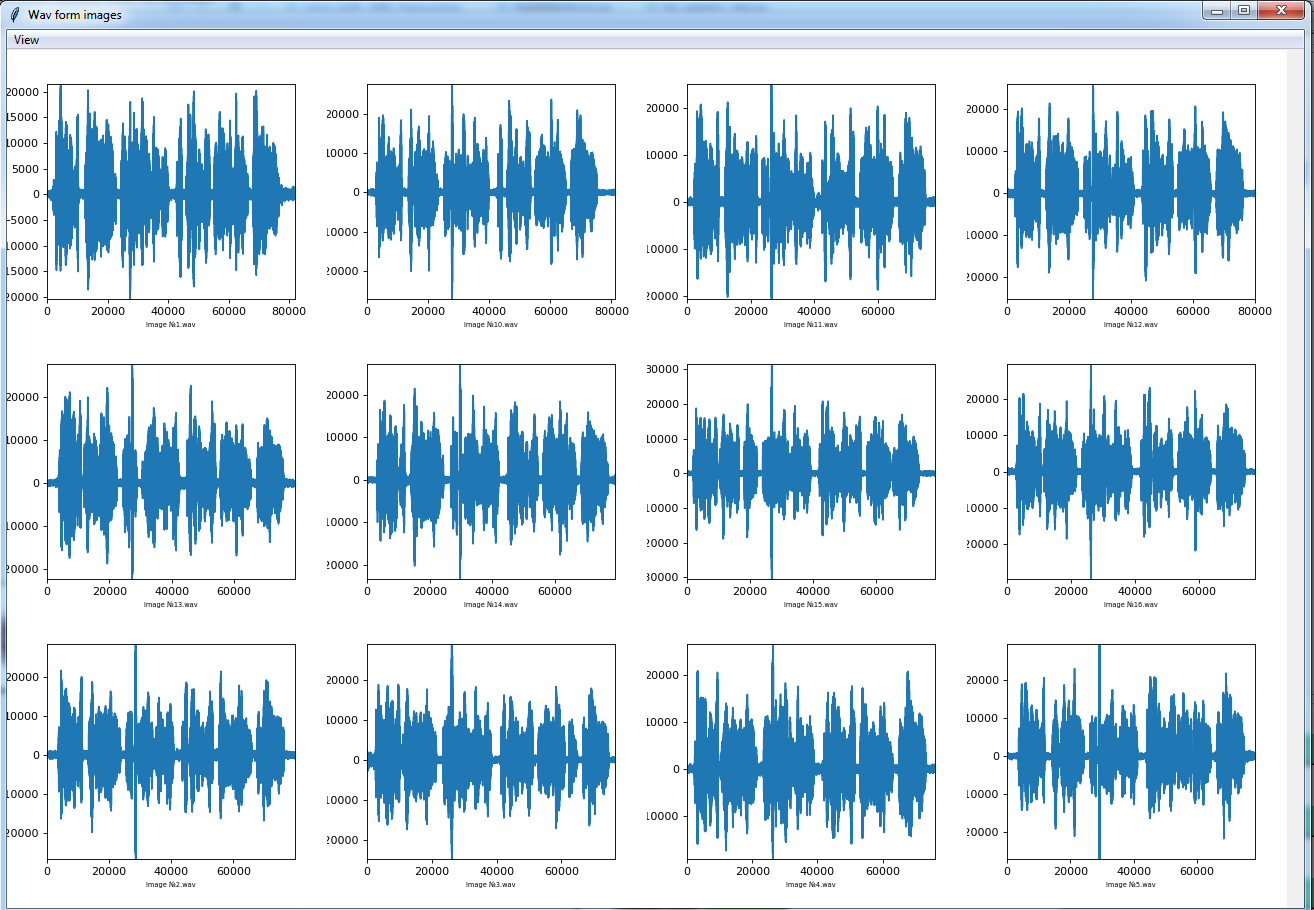


Figure 4 - Examples of .wav-form output of images

By clicking on the "Biometric parameters" button (Figure 5), we go to the graphical view of the biometric parameters extracted from the recorded images.

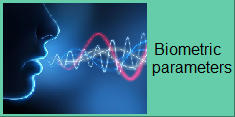


Figure 5 - Button for viewing biometric parameters

This button can be useful for a researcher to compare biometric parameters. An example of the main window is shown in Figure 6.

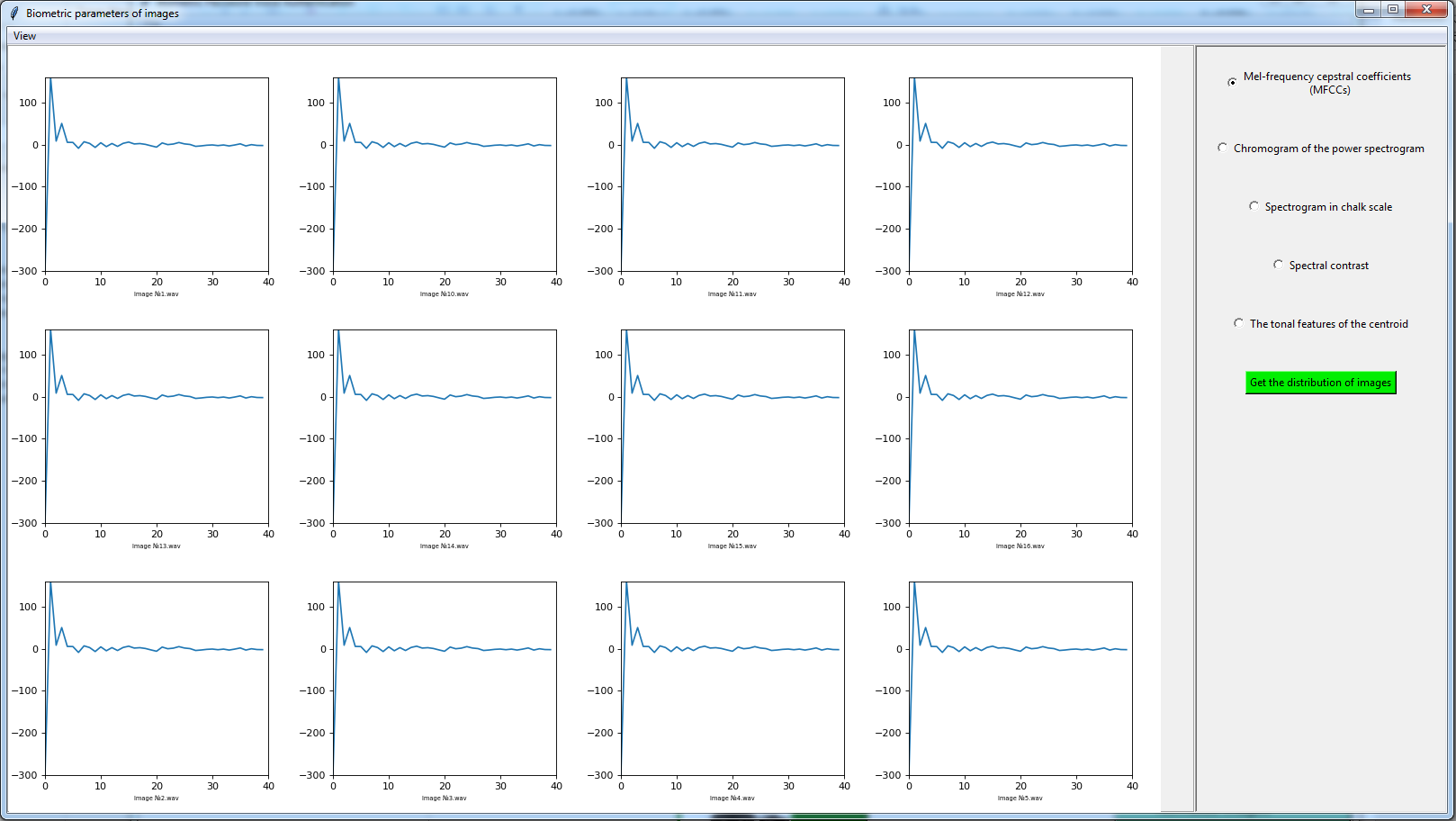


Figure 6 - Main window of graphic demonstration of biometric parameters

The right side offers a choice of "radio buttons", by clicking on which you can view all types of biometric parameters used in the system:

1) chalk frequency coefficients (MFC);

2) spectral power chromogram;

3) spectrogram in chalk scale;

4) spectral contrast;

5) tonal features of the centroid.

An example of changing biometric parameters - Figure 7.

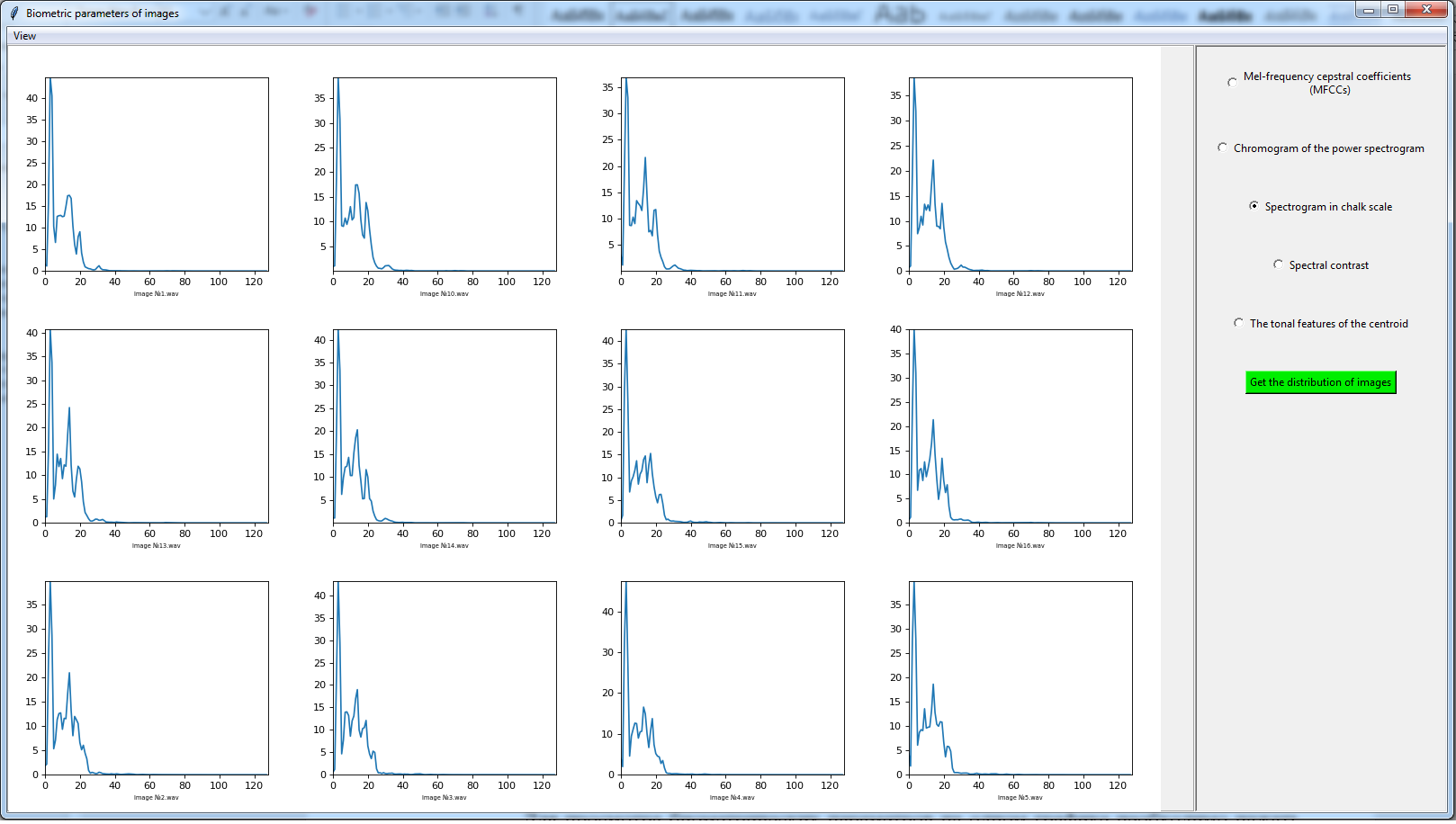


Figure 7 - Examples of coefficients in chalk-scale

To view biometric parameters on one chart, click on the "View" tab and select "On one chart" (Figure 8)

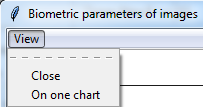


Figure 8 - View of viewing biometric parameters on one graph

When you click on the button, a graph will be displayed (example Figure 9). In this graph, each image is marked with a different color.

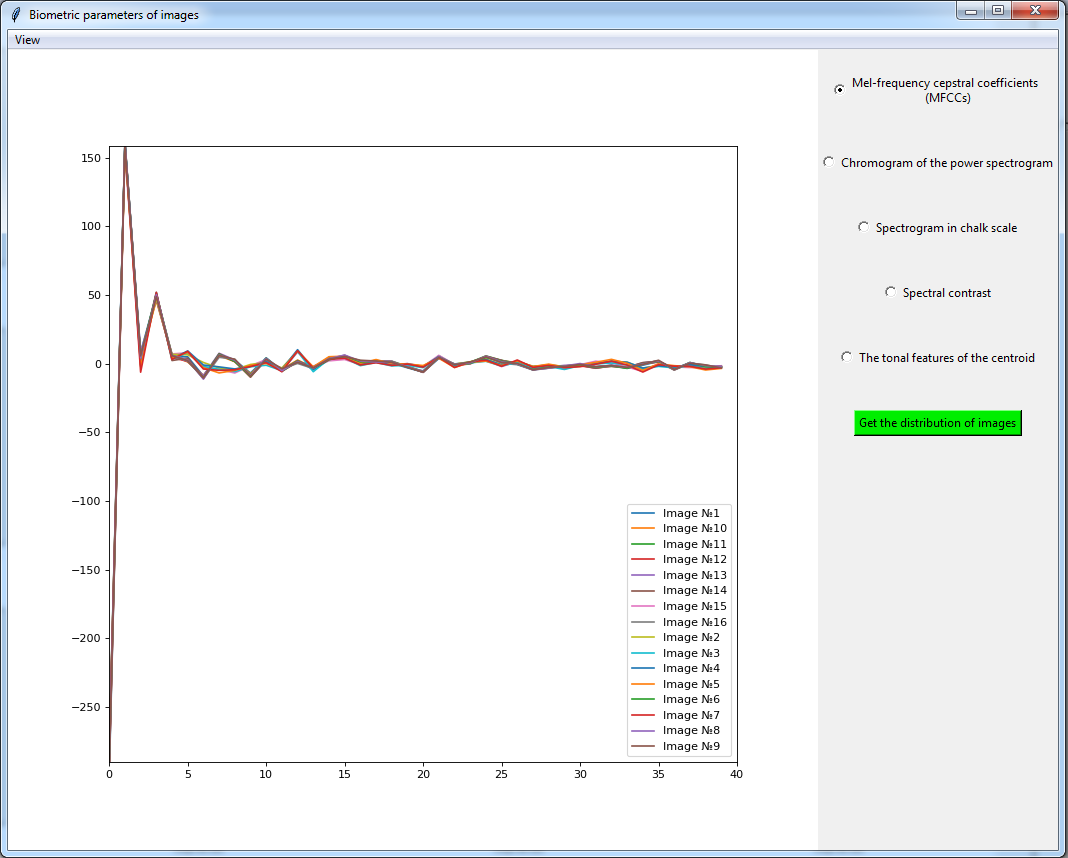


Figure 9 - An example of displaying "on one chart"

Using this view, you can conduct research on environmental influences, microphone variations, illness, atmospheric pressure on biometric parameters.

When you click on the "Get the distribution of images" button, a window appears with a view of the following distributions variations:

1) One's OWN relative to all one's own;

2) One's OWN relative to each other;

3) ALL ALLIENCES relative to each other;

4) One's OWN relative to ALL ALLIENCES;

The malefactor in relation to all OWN Window example - Figure 10

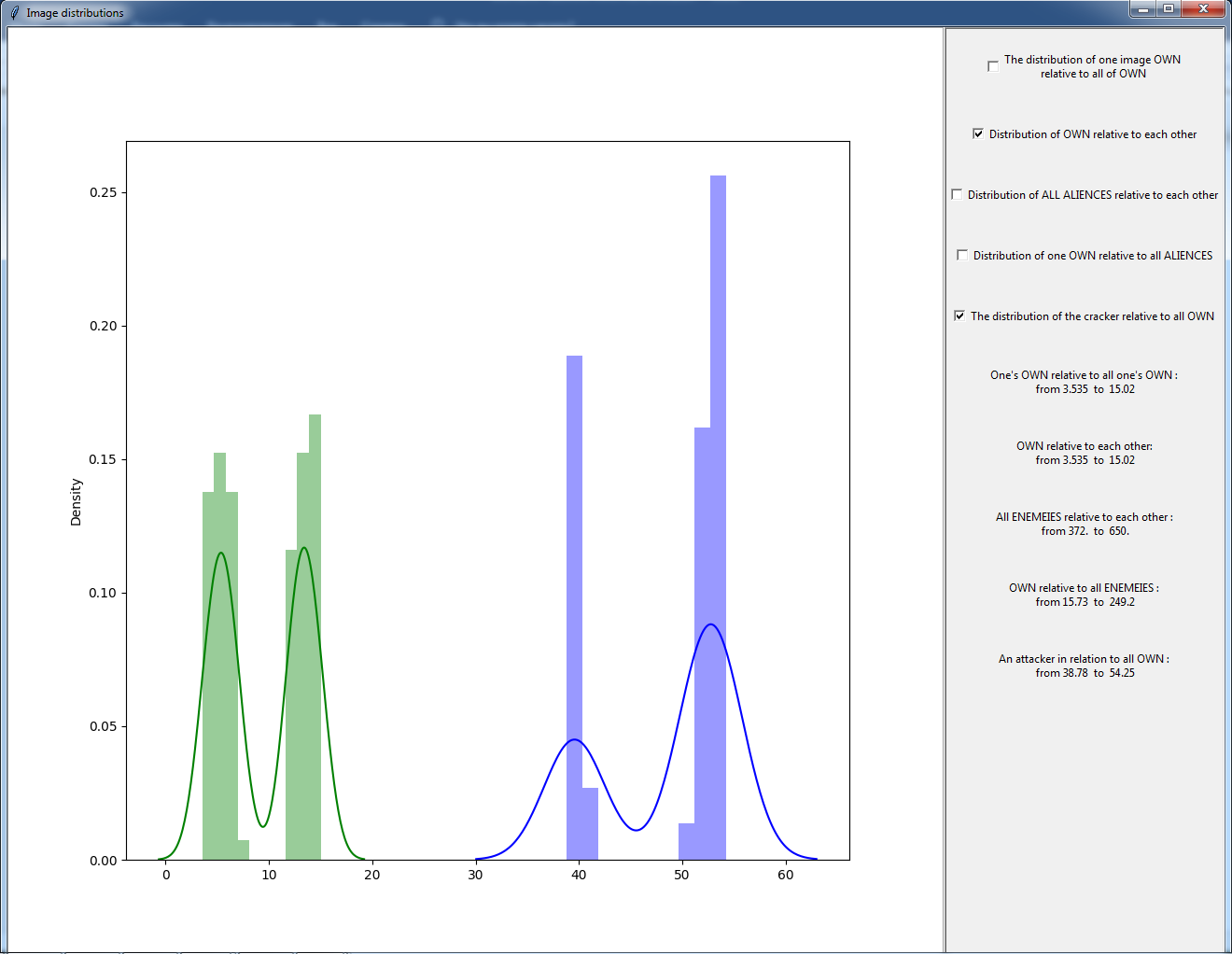


Figure 10 - An example of a window for viewing the distribution of images

Using this window, you can determine whether there are “bad” images in the training sample (records with interference, excess noise). You can also be convinced of the normal distribution of "Own" and its remoteness from the images of "All ENEMIES". Also, when choosing the fifth item, the images are compared with the images of an outsider, which are located in the internal directory in the "ENEMY" folder.

The "Add Images" button at the bottom right of the main menu allows you to download images from any source in the ".wav" format.

Below, the button “Normalize images” is intended for normalizing the added images by volume level.

By clicking on the "Train the network" button, go to the demo user authentication window - Figure 11.

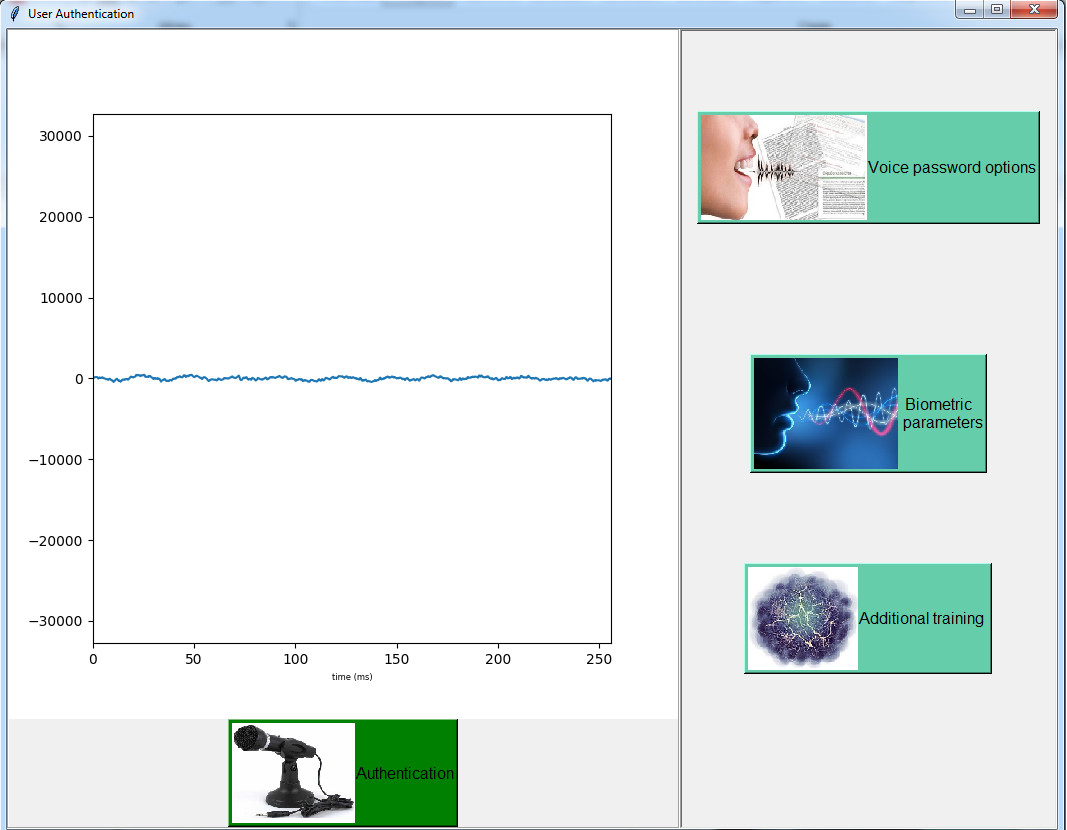


Figure 11 - User authentication window

In this window, when you click on the "Authentication" button, recording will start from the microphone, at which point the user must say a passphrase. Next, a message box will appear with the result of authentication "OWN" - in case of success, and "ALIEN" - if the program did not recognize the user, or the user is different, or an incorrect passphrase is named. Also, the message will display the value of the weighted Euclidean distance and the translated text of the phrase. The decision threshold is configured in the "bio\_params\_view.py" file in the get\_porog function. The threshold depends on the length of the phrase, the nature of the person himself, the environment at the time of authentication. An example of a message output is shown in Figure 12.

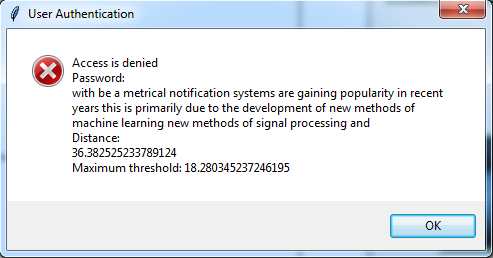


Figure 12 - An example of the authentication result

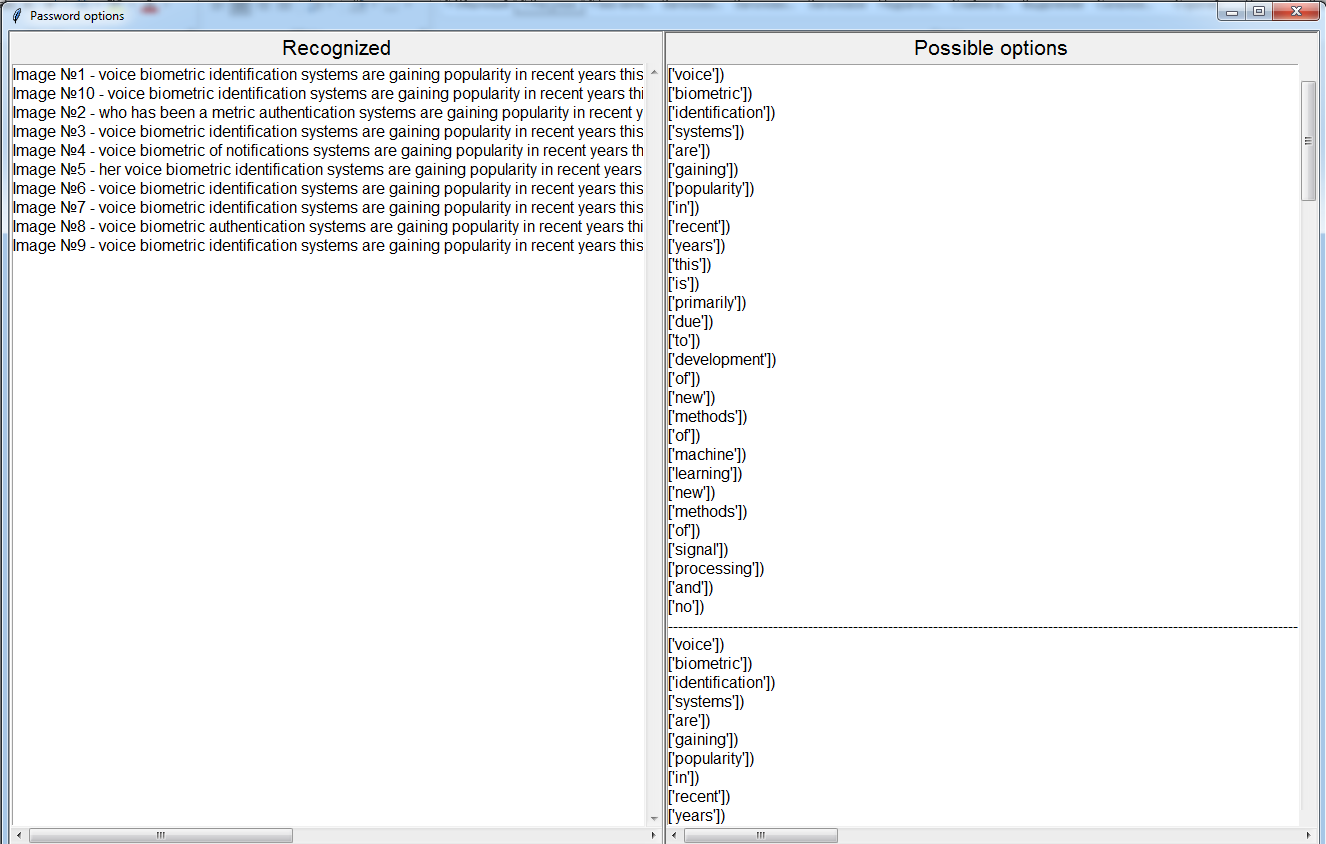
When you click on the "Voice password options" button, a window will be displayed with the source phrases translated into the text and possible tokens for each word (example - Figure 13).

Figure 13 - Examples of variations of passphrases

Pressing the button "Biometric parameters" will display the already described window for graphical viewing of biometric parameters with the last added image submitted for authentication (example - Figure 14).

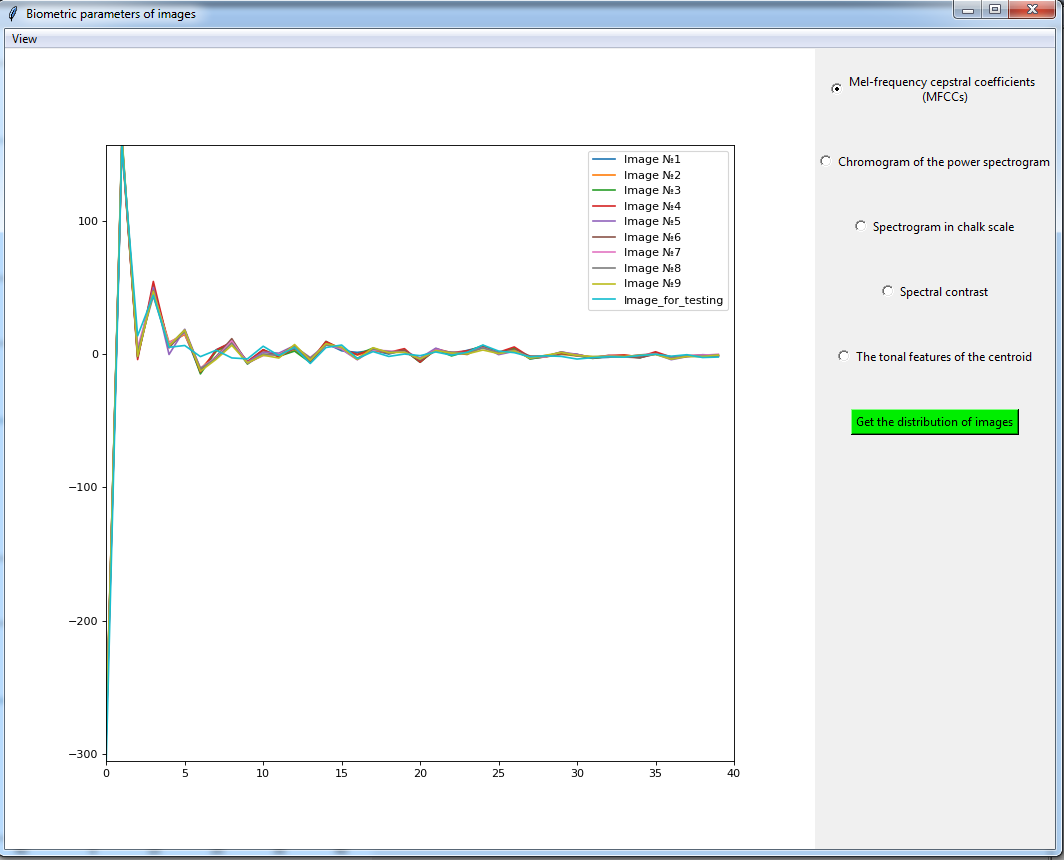


Figure 14 - An example of training images and image submitted for authentication

Using this item, you can see in what types of biometric parameters the new image differs / converges with the images submitted for training.

If the image has not passed authentication (has too great a distance) - there is a button "additional training", when you click on which, the statistics of the training sample will be updated taking into account the last image.