Biometric authorization of Internet services users – Online demo

Offline demo of the project IT "A system for biometric authentication of Internet users based on the fusion of facial and palmprint features" is a web application that enables testing of the biometric verification system in the real-world conditions.
Hardware requirements for the demo are:

- Internet connection
- Color camera with TWAIN-compatible driver
- Scanner with TWAIN- compatible driver and supported resolution of 180dpi

1. Installation

In order to run the demo program, first a client application has to be installed. Installation of the client application demands demands that the .NET framework be installed. If that is not the case, the installation will automatically direct the user to the Web pages where it can be downloaded from. The client application should be installed in the directory where all its users have access rights to write.
Besides the client application, Java Virtual Machine is also required in order to run the demo. It can be installed from
http://java.com/en/download/windows_automatic.jsp

2. Running the demo

The verification or enrollment procedure is initiated from a Web browser, by entering the address of our server
http://balbo.zemris.fer.hr:8080
During the loading of this address, a window will appear, asking the user for access rights necessary in order to run the Web application. The user should allow it, by clicking the 'Yes' button.
After that, a start page opens (Figure 1).

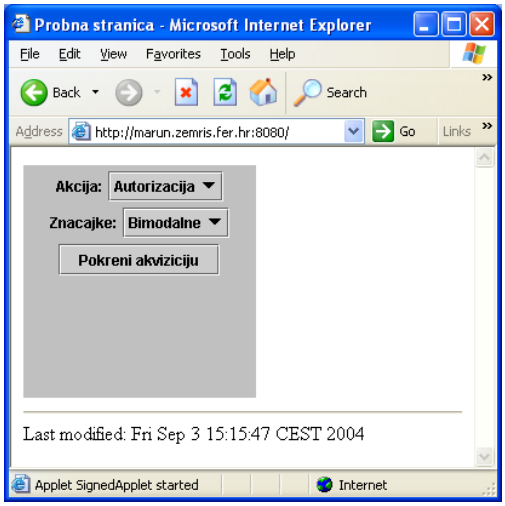

Figure 1: Web page used to run the demo program

On this page, from the 'Akcija' list, it is possible to select two basic actions:

- **Prijava (enrollment)** involves taking several samples (face images, palm images or both) from the user, whose features will then be transferred to the server securely and permanently stored in the feature database of registered users. The user will also have to choose the ID that he/she will use to access the system during the verification. If a user wishes to try to successfully verify himself/herself as a registered user, he/she will first have to enroll this way.
- **Autorizacija (verification)**, involves taking a single sample from the user, whose features will then, together with his/her ID, be securely transmitted to the server and compared with the features of registered users from the database. A part of the system located on the server determines whether the features belong to the same person, and securely sends its reply to the client.

Both actions can be performed using features:

a) Of face only ('lica')
b) Of palm only ('dlana')
c) Bimodal features ('bimodalne')

The above features can be selected from the 'Znacajke' list on the web page used to run the demo.
After the action and the features have been selected, clicking the 'Pokreni akviziciju' (acquisition start) button runs one of the image acquisition applications on the client computer, depending on the selected action and features (options a), b) or c)).
The purpose of this application is the acquisition of facial images using a camera, palm images using a scanner and taking the ID of the user performing the enrollment or verification. The example of the application for the acquisition of face and palm images (run if the user selected bimodal features) is shown on the Figure 2.

Figure 2: The example of the image acquisition application

On first running of each of the image acquisition applications, a window appears where the user should select his/her camera and/or his/her scanner from the list of hardware (Figure 3). In each of the image acquisition applications, near the bottom of the main window, a text can be found, telling the user what he/she should do next. The detailed description of the image acquisition applications can be found in the seminar paper of Želimir Končar, available through the project Web pages.

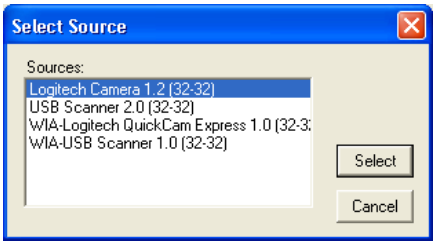

Figure 3: A window for the camera or scanner selection

During the image acquisition, several things should be considered:

- During the face images acquisition, the face should be turned towards the camera. The user should also look in the camera in the moment of acquisition. The whole face should be visible in the image, and the face should be large in the image.
- During the palm images acquisition, the scanner should be set so that the order of the scanning is from the finger-tips toward the wrist of the hand (so that the fingers point upwards in the scanned image). The palm of the right hand

should be placed on the scanner surface, with fingers spread naturally. During the scanning, the hand should be held still. The scanned image should have uniform dark background (the scanner should be shielded from light sources from the above).

After the image acquisition application finishes, the user should **wait** while the features are being extracted from the acquired images and transferred to the server, where the selected action will take place. This procedure lasts somewhat longer for the enrollment than for the verification, because during enrollment more than one sample must be processed. At the end of the enrollment procedure, the user receives a message in a Web browser stating that the enrollment was successful. That reply is shown in Figure 4.

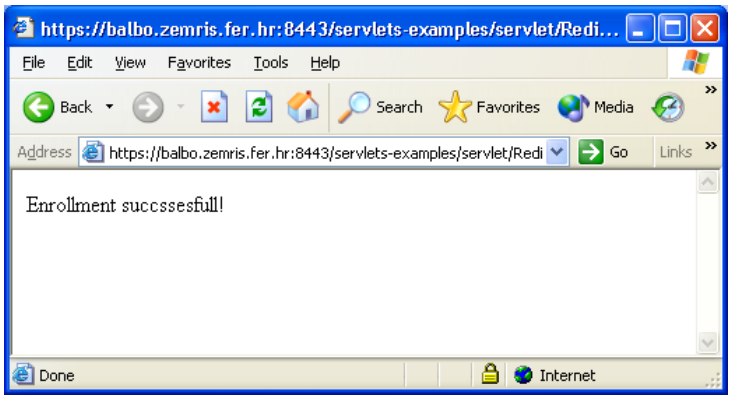

Figure 4: Server reply after enrollment procedure

At the end of the verification procedure, the user receives the reply in a Web browser, stating whether the verification was successful or not. The example of the reply sent to client in the case of successful verification is shown in Figure 5.

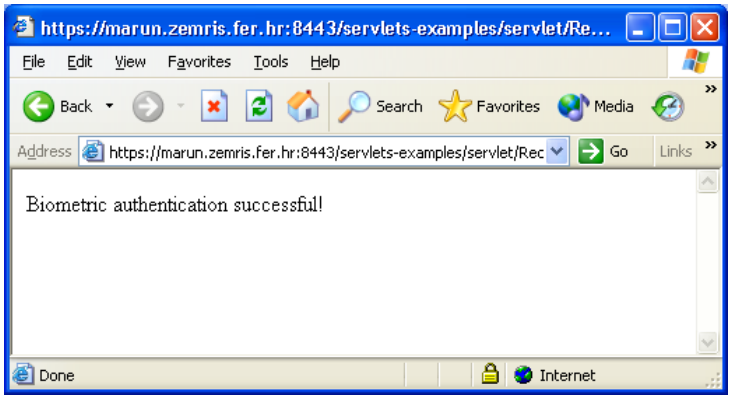

Figure 5: The example of reply from the server (in the case of successful verification)

Using the online demo, the two main experiments can be carried out, during which the user plays the role of the client or the role of the impostor.

- A **client** is a person enrolled in the system, whose features are stored in the registered user database on the server. In order to carry out this experiment, the user should first pass through the enrollment procedure. During each of the verification attempts, a client provides biometric samples (using camera and/or scanner) and his/her ID, the one entered during the enrollment procedure. In this case the verification should be successful.

- **An impostor** is a person not registered as a user in the registered user database, trying to verify his/her identity using one of the registered users' ID, or he/she is registered, but is trying to verify his/her identity using ID of some other user. In this case, the verification result should be a failure. To enable such experiment, several users have already been enrolled in the registered user database with Ids 'ifratric', 'ssegvic', 'jkrapac', 'jsnajder', 'zkalafatic', 'thrkac', 'bdalbelo'.

EXAMPLES:

1. Case: The person is not enrolled and his/her features can't be found in the registered user database on the server. The person (impostor) provides his/her biometric samples (using scanner and/or camera) and uses 'stolen' ID, for example 'ifratric'.
   Expected result: Server reply 'Biometric authentication failed'.
2. Case: The person carries out the enrolment procedure. His/her ID and biometric features are sent to the server and stored in the database. Afterwards, the person tries to verify his/her identity. The person again provides his/her biometric samples (using scanner and/or camera) and uses his/her own ID (selected during the enrollment procedure).
   Expected result: Server reply 'Biometric authentication successful'.