Birzeit University

Computer Science Department

Information Security (Comp 432)

Assignment One

Due Date: 5/5/2024. By11:59 PM Over ITC Meta-Course

The students were required to design a Biometric Authentication system using one of the following biometric authentication methods (Fingerprint, Face Recognition, Iris). Each student must work individual, and not share any of used techniques with others, since the assignment required the students to go through different steps as follows:

- Each student must define the authentication method used through this assignment.
- Research paper must be submitted as guidance for the authentication process; it must be one of recent research in the selected field (such as reading a research paper regarding face recognition, or fingerprint for the purpose of authentication).
- Implement the designed system using a programming language of your choice (e.g., Python, Java, C++).
- The student can use one of the public data sets (Publicly available benchmark datasets like FVC (Fingerprint Verification Competition) or UTIris (University of Toronto Iris Recognition) for the purpose of testing, instead of data acquisition process due to privacy concerns. Students can also explore libraries or tools for generating biometric data that statistically resemble real data (PyFprint (Python) or BioGen (Java) can be used for fingerprint data generation).
- Select the matching algorithm and one of the known distance metrics for authentication.
- Define the method used to select the threshold value for authentication purpose (machine learning and heuristic algorithm can be used here).
- The student must divide the dataset into two main groups (Training and testing).

    - Training Set: Used to train the matching algorithm that compares features for authentication. This set should include features from both genuine users (enrolled users) and imposters (non-enrolled users).
    - Testing Set: Used to evaluate the performance of the system. This set should also contain features from genuine users and imposters, independent of the training data.
- Evaluation using the following metrics:
    - False Match Rate (FMR): Rate at which an imposter is incorrectly classified as a genuine user.
    - False Non-Match Rate (FNMR): Rate at which a genuine user is incorrectly classified as an imposter.
    - Plot the Receiver Operating Characteristic (ROC) curve, which shows the trade-off between FMR and FNMR.
    - Determine the Equal Error Rate (EER), the point on the ROC curve where FMR and FNMR are equal.
- Report, each student is required to submit will structured report that includes:
    - A detailed description of your system design, including the chosen modality, algorithms used in the steps of matching and selecting the thresholds value, and system architecture.
    - The source code of your program with clear comments explaining each part.
    - The results of the evaluation, including the calculated FMR, FNMR, ROC curve, and EER.
    - Discussion on factors that can affect the performance of your system and potential improvements.

Late Assignment (even one minute late) will NOT be accepted for any reason.

Assignment Files not compressed correctly or cannot be opened will not be graded and will receive a zero grade.