BẢO VỆ QUYỀN RIÊNG TƯ TRONG HỆ THỐNG CHỨNG THỰC NGƯỜI DÙNG BẰNG GIỌNG NÓI DÙNG CANCELABLE BIOMETRICS

Nguyễn Đại Dương - 230202024

Tóm tắt

- Lớp: CS2205.MAR2024
- Link Github: https://github.com/daiduongnguyen68/CS2205.MAR2024
- Link YouTube video:
- Ảnh + Họ và Tên: Nguyễn Đại Dương
- Tổng số slides không vượt quá 10

Giới thiệu

Speaker Recognition:

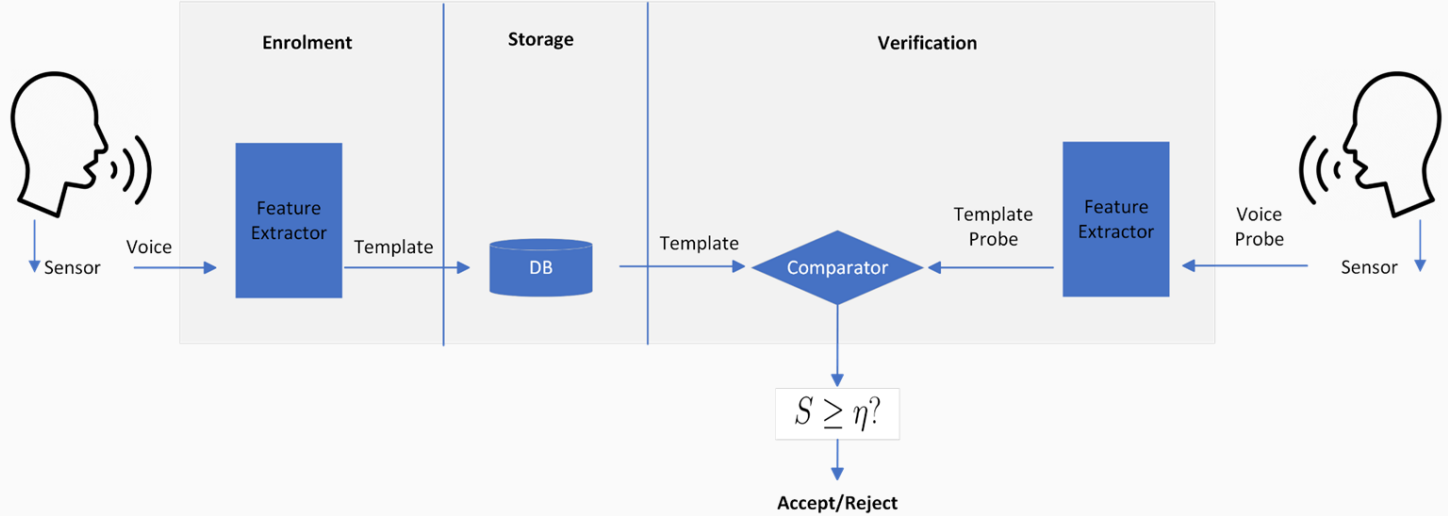
- Nhận diện một người bằng cách phân tích giọng điệu, cao độ giọng nói và giọng điệu của họ[1].
- Có thể dễ dàng triển khai trên các thiết bị thông dụng (vd: máy tính, thiết bị di động) có micro.

Hình 1. Sinh trắc học giọng nói

[1]Andreas Nautsch et al. “Preserving privacy in speaker and speech characterisation”. In: Computer Speech & Language 58 (2019), pp. 441–480.

Speaker Recognition System

- Gồm có 2 pha: *đăng ký* và *xác thực*.



Hình 2. Hệ thống nhận dạng người nói truyền thống

Speaker Recognition System Problems

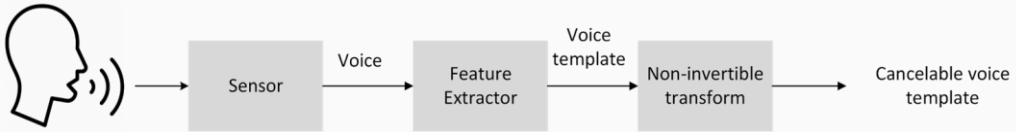
Lưu trữ sinh trắc học giọng nói (dưới dạng bản rõ) mà không có biện pháp bảo vệ sẽ gây ra những lo ngại về quyền riêng tư:

- Mô hình giọng nói (cùng với các mẫu giọng nói được trích xuất) có thể được sử dụng để tạo ra các giọng nói đại diện cho người nói ban đầu[2].
- Đặc điểm giọng nói không thể bị hủy bỏ hoặc thu hồi.
- Các mẫu giọng nói từ cùng một giọng của người dùng cho các ứng dụng khác nhau có độ tương đồng cao. Nếu một mẫu bị lộ, các ứng dụng còn lại sử dụng sinh trắc học giọng nói sẽ dễ bị khai thác.

[2]Nautsch et al., “Preserving privacy in speaker and speech characterisation”.

Cancelable Biometrics (CB)

- Phương pháp này sử dụng hàm một chiều để làm biến dạng mẫu giọng nói gốc[3].
- CB cho phép thực hiện nhận dạng trên miền đã được biến đổi.
- CB băm các mục đầu vào tương tự thành cùng một giá trị với xác suất rất cao.



Hình 3. Minh họa mô hình CB để bảo vệ mẫu sinh trắc học

[3]Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. “Enhancing security and privacy in biometrics-based authentication systems”. In: IBM systems Journal 40.3 (2001), pp. 614–634.

Mục tiêu

Đề xuất mô hình CB cho bài toán Nhận diện người dùng bằng giọng nói đảm bảo các yêu cầu về quyền riêng tư dữ liệu giọng nói (theo tiêu chuẩn ISO/IEC 24745[4]):

- *Revocability*
- *Non-invertibility*
- *Unlinkability*
- *Performance*

[4]ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection. 2011

Nội dung và Phương pháp

- Xây dựng nền tảng lý thuyết:
  - Locality-sensitive hashing (LSH).
  - Winner-Take-All Hashing[5] áp dụng cho sinh trắc học.
- Khảo sát các mô hình CB:
  - Đánh giá điểm mạnh, yếu của cá mô hình bảo vệ mẫu sinh trắc học.
- Cài đặt, thực nghiệm và chọn mô hình để cải tiến:
  - Kiểm tra kết quả, chọn baseline để so sánh.
- Đề ra và thực nghiệm các giải pháp cải tiến:
  - Đánh giá và so sánh kết quả với baseline.
  - Chọn giải pháp tốt nhất.

[5]Jay Yagnik et al. “The power of comparative reasoning”. In: 2011 International Conference on Computer Vision. IEEE. 2011, pp. 2431–2438.

Kết quả dự kiến

- Về hiệu năng: Đạt được chỉ số Equal-Error-Rate (EER) khoảng 5% hoặc nhỏ hơn trên tập dữ liệu: TIMIT[6].
- Về quyền riêng tư và bảo mật:
  - *Irreversibility:* Rất khó để có thể khôi phục được mẫu sinh trắc học ban đầu từ các mẫu sinh trắc học có thể hủy bỏ sinh ra từ mô hình CB.
  - *Revocability*: Mô hình đề xuất có số lượng mẫu sinh trắc học có thể hủy bỏ phải đủ lớn để có thể đáp ứng cho việc sử dụng trên nhiều hệ thống khác nhau.
  - *Unlinkability*: chỉ số *D_sys* xấp xỉ 0, nghĩa là mô hình đề xuất đảm bảo yêu cầu về tính unlinkability.

[6]Garofolo, John S. “Timit acoustic phonetic continuous speech corpus”. In: Linguistic Data Consortium, 1993 (1993).

Tài liệu tham khảo

[1] Andreas Nautsch et al. “Preserving privacy in speaker and speech characterisation”. In: Computer Speech & Language 58 (2019), pp. 441–480.

[2] Nautsch et al., “Preserving privacy in speaker and speech characterisation”.

[3] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. “Enhancing security and privacy in biometrics-based authentication systems”. In: IBM systems Journal 40.3 (2001), pp. 614–634.

[4]ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection. 2011

[5] Jay Yagnik et al. “The power of comparative reasoning”. In: 2011 International Conference on Computer Vision. IEEE. 2011, pp. 2431–2438.

[6] Garofolo, John S. “Timit acoustic phonetic continuous speech corpus”. In: Linguistic Data Consortium, 1993 (1993).