# **THÔNG TIN CHUNG CỦA BÁO CÁO**

* Link YouTube video của báo cáo (tối đa 5 phút):   
  *(ví dụ: https://www.youtube.com/watch?v=AWq7uw-36Ng)*
* Link slides (dạng .pdf đặt trên Github):   
  *(ví dụ: https://github.com/mynameuit/CS2205.APR2023/TenDeTai.pdf)*
* *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
* *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*

|  |  |
| --- | --- |
| * Họ và Tên: Nguyễn Đại Dương * MSSV: 230202024 | * Lớp: CS2205.MAR2024 * Tự đánh giá (điểm tổng kết môn): 9.0/10 * Số buổi vắng: 0 * Số câu hỏi QT cá nhân: * Link Github: https://github.com/daiduongnguyen68/CS2205.MAR2024/ |

# **ĐỀ CƯƠNG NGHIÊN CỨU**

|  |
| --- |
| **TÊN ĐỀ TÀI (IN HOA)**  BẢO VỆ QUYỀN RIÊNG TƯ TRONG HỆ THỐNG CHỨNG THỰC NGƯỜI DÙNG BẰNG GIỌNG NÓI DÙNG CANCELABLE BIOMETRICS |
| **TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)**  PRIVACY-PRESERVING SPEAKER RECOGNITION WITH CANCELABLE BIOMETRICS |
| **TÓM TẮT** *(Tối đa 400 từ)*  Nhận dạng người nói được sử dụng rộng rãi trong nhiều dịch vụ và ứng dụng như điện thoại thông minh và trợ lý kỹ thuật số thông minh. Trong các hệ thống như vậy, mẫu giọng nói đã đăng ký cần được lưu trữ ở dạng bản rõ để có thể so sánh trong các lần đăng nhập tiếp theo. Tuy nhiên, việc lưu trữ mẫu sinh trắc như vậy sẽ đặt ra một số vấn đề về bảo mật và quyền riêng tư của người dùng. Phương pháp Sinh trắc học có thể hủy bỏ (Cancelable Biometrics, CB) đã nhận được sự quan tâm đáng kể của các nhà nghiên cứu trong những năm gần đây. Trong các mô hình CB, mẫu sinh trắc học được bảo vệ bằng hàm biến đổi một chiều (rất khó để khôi phục lại đặc điểm sinh trắc học ban đầu) và cho phép xác thực trên miền biến đổi này. Tuy nhiên, các mô hình CB hiện tại thường làm giảm hiệu suất nhận dạng và không đáp ứng được các yêu cầu về quyền riêng tư. Trong nghiên cứu này, tôi mong muốn giải quyết những hạn chế này để cải thiện hiệu suất nhận dạng và cũng tăng cường bảo mật hệ thống. Mô hình đề xuất sẽ được đánh giá bằng tập dữ liệu TIMIT để chứng minh hiệu suất nhận dạng so với các mô hình CB hiện tại. Hơn nữa, mô hình đề xuất sẽ được phân tích và đánh giá quyền riêng tự dựa trên tiêu chuẩn ISO/IEC 24745. |
| **GIỚI THIỆU** *(Tối đa 1 trang A4)*  Ngày nay, dữ liệu sinh trắc học được sử dụng rộng rãi trong việc xác thực và định danh người dùng. Bằng cách sử dụng các thiết bị cảm biến kết hợp với mô hình trích xuất đặc trưng thích hợp, đặc điểm sinh trắc học sẽ được trích xuất thành mẫu sinh trắc học (biometric template). Các mẫu sinh trắc học này có thể được lưu lại để xác thực khi người dùng đăng kí vào hệ thống [1]. Dữ liệu giọng nói chứa đựng nhiều thông tin bao gồm về đặc điểm cơ quan sinh học cấu thành giọng nói và ngữ âm của người nói và có thể được dùng để xác thực người dùng.    *Hình 1. Hệ thống xác thực dựa giọng nói truyền thống.*  Tuy nhiên, việc lưu trữ mẫu sinh trắc học trực tiếp và không bảo vệ sẽ đặt ra một số vấn đề về bảo mật và quyền riêng tư của người dùng [1] [2]. Một cách tiếp cận đơn giản là sử dụng hàm băm, đảm bảo không thể khôi phục được dữ liệu sinh trắc học ban đầu. Tuy nhiên, giá trị băm sẽ thay đổi đáng kể và không xác định đối với các thay đổi nhỏ trong đặc điểm sinh trắc học. Một giải pháp đang được nhiều người quan tâm đó là sử dụng phương pháp Sinh trắc học hủy được (Cancelable biometrics, CB). Các mẫu sinh trắc học được bảo vệ bằng hàm biến đổi một chiều (rất khó để khôi phục lại đặc điểm sinh trắc học ban đầu) và cho phép xác thực trên miền biến đổi này. Tuy nhiên, phương pháp này thường làm giảm đi hiệu suất của việc sử dụng dữ liệu sinh trắc học để nhận dạng vì nó làm mất đi nhiều thông tin từ mẫu sinh trắc học thông qua hàm biến đổi. Chính vì vậy, tôi muốn đưa ra một mô hình về CB nhằm nâng cao hiệu năng của việc sử dụng dữ liệu giọng nói để xác thực người dùng trong khi vẫn đảm bảo an toàn đặc điểm sinh trắc học của người dùng.  **Input:** mẫu sinh trắc học được đã được trích xuất từ giọng nói của người dùng, vector .  **Output:** mẫu sinh trắc học có thể hủy được (cancelable biometric template). |
| **MỤC TIÊU**  *(Viết trong vòng 3 mục tiêu, lưu ý về tính khả thi và có thể đánh giá được)*   1. Đề xuất mô hình CB cho bài toán Nhận diện người dùng bằng giọng nói nhằm nâng cao hiệu năng của việc sử dụng dữ liệu sinh trắc học để nhận diện người dùng trong khi vẫn đảm bảo được tính bảo mật của mẫu sinh trắc học. 2. Đảm bảo được quyền riêng tư dữ liệu giọng nói (theo tiêu chuẩn ISO/IEC 24745 [3]):  * *Revocability*: Khi mẫu sinh trắc học được bảo vệ cắp bị đánh cắp thì có thể hủy bỏ mẫu sinh trắc học này và tạo được mẫu sinh trắc học mới dựa trên cùng đặc điểm sinh trắc học của người dùng. Mẫu sinh trắc học mới không liên quan đến mẫu sinh trắc cũ. * *Non-invertibility*: Rất khó để khôi phục các thông tin đặc điểm sinh trắc học của người dùng từ mẫu sinh trắc học được bảo vệ. * *Unlinkability*: Từ 2 mẫu sinh trắc học được bảo vệ, không thể xác định được rằng các mẫu này được sinh ra từ cùng một người hay từ 2 người khác nhau. * *Performance*: Hiệu năng nhận dạng phải được duy trì so với trước khi áp dụng mô hình. |
| **NỘI DUNG VÀ PHƯƠNG PHÁP**  *(Viết nội dung và phương pháp thực hiện để đạt được các mục tiêu đã nêu)*   1. **Nội dung**   Trong đề tài nghiên cứu này, tôi dự kiến sẽ nghiên cứu và tìm hiểu các nội dung chính như sau:   * Khảo sát các mô hình CB được đề xuất gần đây cho bài toán bảo vệ các mẫu sinh trắc học: Có nhiều mô hình khác nhau được đề xuất cho các đặc trưng sinh trắc học khác nhau. * Tìm hiểu thuật toán *Winner-Take-All Hashing* [4]: đây là một thuật toán cơ sở được nhiều mô hình CB dựa trên và cải tiến để áp dụng vào việc bảo vệ mẫu sinh trắc học. * Thử nghiệm các mô hình CB gần đây, tìm ra hạn chế của những mô hình này. Từ đó, đưa ra các giải pháp để cái tiến và tiến hành thực nghiệm, đánh giá các giải pháp đã đề xuất để chọn ra giải pháp tốt nhất. * Phân tích tính bảo mật và quyền riêng tư của mô hình đã đề xuất.  1. **Phương pháp**  * Khảo sát các mô hình CB được đề xuất để bảo vệ mẫu sinh trắc học người nói: tìm hiểu xem các mô hình này có gì khác so với các mô hình để bảo vệ các mẫu sinh trắc hoc khác hay không? Các mô hình này có đi sâu vào khai thác các đặc trưng cụ thể nào của mẫu sinh trắc học hay không? Điểm mạnh và điểm yếu của những mô hình này là gì? Hiểu được cách đánh giá và phân tích về tính bảo mật và quyền riêng tư của một mô hình CB. * Xây dựng nền tảng lý thuyết mà các mô hình CB thường dựa trên: Ví dụ: các mô hình dựa trên hàm băm theo phương pháp *Locality-sensitive hashing (LSH)* để tạo ra các mẫu sinh trắc học hủy được. *Winner-Take-All Hashing* (hay còn gọi là *Index-of-Max Hashing*) là một ví dụ cho phương pháp LSH, dựa trên *rank correlation* để đánh giá sự tương đồng giữa các đối tượng và được các nghiên cứu gần đây áp dụng để bảo vệ mẫu sinh trắc học như đặc trưng người nói [5] và đặc trưng vân tay [6]. * Thực nghiệm các mô hình, chọn ra mô hình để cải tiến: Kiểm tra các kết quả của các công trình đã có, chọn làm baseline để so sánh. * Đề ra các giải pháp cải tiến, sau đó tiến hành thực nghiệm, đánh giá các giải pháp đã đưa ra, so sánh kết quả của mô hình đề xuất với baseline. Từ đó, chọn ra giải pháp tốt nhất. |
| **KẾT QUẢ MONG ĐỢI**  *(Viết kết quả phù hợp với mục tiêu đặt ra, trên cơ sở nội dung nghiên cứu ở trên)*   * Về hiệu năng: Đạt được chỉ số Equal-Error-Rate (EER) khoảng 5% hoặc nhỏ hơn trên tập dữ liệu: TIMIT [7]. * 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 xác thực sinh trắc học khác nhau. * *Unlinkability*: , nghĩa là mô hình đề xuất đảm bảo yêu cầu về unlinkability. |
| **TÀI LIỆU THAM KHẢO** *(Định dạng DBLP)*  [1]. Christian Rathgeb, Andreas Uhl:  A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. 2011: 3 (2011)  [2] Vishal M. Patel, Nalini K. Ratha, Rama Chellappa:  Cancelable Biometrics: A review, IEEE Signal Process, Mag. 32(5): 54-65 (2015)  [3] ISO/IEC 24745:2011 Information technology - Security techniques - Biometric information protection (2011)  [4] Jay Yagnik, Dennis Strelow, David A. Ross, Ruei-Sung Lin:  The power of comparative reasoning. ICCV 2011: 2431-2438  [5] Kong-Yik Chee, Zhe Jin, Danwei Cai, Ming Li, Wun-She Yap, Yen-Lung Lai, Bok-Min Goi:  Cancellable speech template via random binary orthogonal matrices projection hashing. Pattern Recognit. 76: 273-287 (2018).  [6] Zhe Jin, Jung Yeon Hwang, Yen-Lung Lai, Soohyung Kim, Andrew Beng Jin Teoh:  Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing. IEEE Trans. Inf. Forensics Secur. 13(2): 393-407 (2018)  [7] John S. Garofolo, Lori F. Lamel, William M. Fisher, Jonathan G. Fiscus, David S. Pallett, Nancy L. Dahlgren, Victor Zue:  Timit acoustic phonetic continuous speech corpus (1993) |