# LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tác giả luận văn

Hà Quang Tấn

# MỤC LỤC

LỜI CAM ĐOAN 1

MỤC LỤC 2

DANH MỤC THUẬT NGỮ, CHỮ VIẾT TẮT 4

DANH MỤC BẢNG 5

DANH MỤC HÌNH VẼ 6

MỞ ĐẦU 6

1. Lý do chọn đề tài 6

2. Mục đích nghiên cứu 7

3. Đối tượng và phạm vi nghiên cứu 8

4. Phương pháp nghiên cứu 8

Chương 1 – TỔNG QUAN PHƯƠNG PHÁP XÁC THỰC TRÊN ĐIỆN THOẠI DI ĐỘNG 9

1.1. Tại sao cần xác thực cho thiết bị di động? 9

1.2. Các nghiên cứu trước đây 13

1.2.1. Xác thực dựa trên các đặc điểm sinh trắc học 13

1.2.2. Xác thực dựa trên chuyển động 23

1.3. Xác thực trên điện thoại di động bằng nhận dạng cử chỉ người 29

Chương 2 – PHƯƠNG PHÁP NHẬN DẠNG CỬ CHỈ NGƯỜI 29

2.1. Cảm biến gia tốc và dữ liệu cảm biến gia tốc trên điện thoại di động 29

2.2. Khoảng cách và sự tương đồng 31

2.2.1. Khoảng cách giữa hai điểm 31

2.2.2. Khoảng cách và sự tương đồng của các đặc điểm 32

2.2.3. Các loại khoảng cách 34

2.3. Nhận dạng cử chỉ dựa trên kỹ thuật so khớp chuỗi thời gian động 36

2.3.1. Giới thiệu 36

2.3.2. Phát biểu bài toán 38

2.3.3. Thuật toán 39

2.3.4. Độ phức tạp của thuật toán 41

2.3.5. Các ràng buộc của thuật toán DTW 42

2.4. Một số cải tiến kỹ thuật so khớp chuỗi thời gian động cho nhận dạng cử chỉ 45

2.4.1. Thuật toán IDTW 45

2.4.2. Độ phức tạp về thời gian 50

2.4.3. Độ phức tạp về không gian 52

2.5. Xác thực bằng nhận dạng cử chỉ 53

2.5.1. Các yêu cầu đối với cơ chế xác thực người dùng trên thiết bị di động 54

2.5.2. Thuật toán xác thực 55

2.5.3. Quá trình đăng ký và xác thực 59

2.5.4. Tiền xử lý 60

Chương 3 – THỬ NGHIỆM VÀ ĐÁNH GIÁ 61

3.1. Thu thập dữ liệu 61

3.2. Kết quả thực nghiệm DTW 61

3.3. Kết quả thực nghiệm của iDTW 61

3.4. Phân tích và đánh giá 61

3.5. Kết luận 61

KẾT LUẬN 61

HƯỚNG PHÁT TRIỂN TIẾP THEO 64

DANH MỤC TÀI LIỆU THAM KHẢO 65

# DANH MỤC THUẬT NGỮ, CHỮ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| Viết tắt | Tiếng Anh | Tiếng Việt |
| API | Application Program Interface | Giao diện lập trình ứng dụng |
| BXL |  | Bộ xử lý |
| MIMD | Multiple instruction multiple data | Đa lệnh đa dữ liệu |
| MPI | Message Passing Interface | Giao diện truyền thông điệp |
| SIMD | Single instruction multiple data | Đơn lệnh đa dữ liệu |
| SMP | Symmetric MultiProcesor | Đa xử lý đối xứng |
| KPI | Key performance Indicator | Chỉ số đo lường hiệu suất |
| CCBS | Customer Care & Billing System | Hệ thống tính cước và chăm sóc khách hàng |
| POSIX | Portable Operating System Interface | Giao diện hệ điều hành linh động |
| CPU | Central Processing Unit | Bộ xử lý trung tâm |

# DANH MỤC BẢNG

# DANH MỤC HÌNH VẼ

Hình 2.1: Minh họa các chiều của cảm biến gia tốc 18

Hình 3.1. So sánh hai phương pháp đo khoảng cách Euclidean và DTW 63

Hình 3.2. Cách thức “warp” các chuỗi dữ liệu trong DTW 63

Hình 3.3. Khoảng cách giữa hai điểm trên cùng một mặt phẳng 64

Hình 3.4. Khoảng cách giữa hai điểm trong không gian 2-chiều 65

Hình 3.5. Đối tượng A – Toyota Prius 66

Hình 3.6. Đối tượng B – VW Beetle 67

Hình 3.7. Đối tượng C - Cadillac Escalade 67

Hình 3.8. Khoảng cách giữa hai đối tượng dựa trên các thông số của chúng 68

Hình 3.9. Đường warp giữa hai chuỗi 69

Hình 3.10. Ma trận trọng số và đường warp có khoảng cách nhỏ nhất 71

Hình 3.10. Thứ tự điền giá trị cho ma trận chi phí 72

Hình 3.11. Hai ràng buộc Sakoe-Chuba Band (bên trái) và Itakura Parallelogram (bên phải) 74

Hình 3.12. Tăng tốc DTW bằng phương pháp trích rút dữ liệu 75

Hình 4.1. Chiều các trục x, y, z của bộ cảm biến gia tốc được gắn trong iPhone 4. 79

Hình 4.2. Bản ghi mẫu cho các cử chỉ hình tam giác 80

# MỞ ĐẦU

1. Lý do chọn đề tài

Ngày nay, các thiết bị di động cung cấp cho người sử dụng rất nhiều tiện ích và nó đã trở thành một công cụ hỗ trợ đắc lực cho cuộc sống và công việc của chúng ta. Ưu điểm chính của những thiết bị này là chúng ta có thể mang chúng theo và sử dụng chúng ở gần như khắp mọi nơi và vào bất cứ thời điểm nào: chúng ta có thể kiểm tra email, đọc tin tức, trao đổi qua các mạng xã hội và làm rất nhiều việc khác trên đó. Để hỗ trợ người sử dụng, các thiết bị di động cũng có thể tạo ra và lưu trữ rất nhiều dữ liệu cá nhân nhạy cảm trên đó.

Tuy nhiên, bên cạnh các tiện ích không thể phủ nhận thì việc sử dụng các thiết bị di động cũng gắn liền với các nguy cơ về bảo mật. Nếu một người không có quyền, có thể truy nhập tự do vào các thiết bị như vậy thì dữ liệu nhạy cảm của người sử dụng có thể bị đánh cắp và lợi dụng. Vì vậy, các cơ chế xác thực người dùng là rất cần thiết. Hiện nay, các cơ chế xác thực như sử dụng mã PIN và mật khẩu không tính đến những hạn chế về giao diện sử dụng của các thiết bị di động. Vì vậy, cần phải xây dựng và phát triển các cơ chế xác thực mới phù hợp hơn và có khả năng sử dụng trong những điều kiện hạn chế như vậy.

Các công trình nghiên cứu trước đây đã cho thấy rằng các cử chỉ giao tiếp tự nhiên với con người có tiềm năng trở thành các tương tác về mặt cử chỉ. Trong luận văn này, chúng ta sẽ phát triển một cơ chế xác thực người dùng sinh trắc dựa trên các cử chỉ bằng việc sử dụng bộ cảm biến gia tốc 3-chiều được tích hợp sẵn trong các thiết bị di động. Cơ chế xác thực này sẽ được đánh giá trong một nghiên cứu sử dụng bao gồm cả hình thức tấn công thực tế để chứng minh rằng xác thực dựa trên cử chỉ người là khả thi, có khả năng sử dụng cao và đầy hứa hẹn cho các thiết bị di động. Xuất phát từ thực tế và các nhu cầu ở trên tôi chọn đề tài:

**“TỰ ĐỘNG NHẬN DẠNG CỬ CHỈ NGƯỜI VÀ ỨNG DỤNG ĐỂ BẢO MẬT CHO THIẾT BỊ DI ĐỘNG”**

1. Mục đích nghiên cứu

Trong luận văn này một cơ chế xác thực dựa trên cử chỉ cho các thiết bị di động với cảm biến gia tốc 3 chiều được phát triển và đánh giá. Người dùng tiến hành xác thực bằng việc thực hiện một cử chỉ bằng tay trong khi giữ điện thoại di động. Chứng minh phương pháp xác thực dựa trên cử chỉ là khả thi và có một số ưu điểm so với các cơ chế xác dựa trên tri thức đang được sử dụng rộng rãi.

Cơ chế xác thực dựa trên cử chi được thực hiện trong luận văn này sử dụng một bộ cảm biến gia tốc 3 chiều được tích hợp vào trong thiết bị di động. Phương pháp đo của các bộ cảm biến được đánh giá bằng việc sử dụng các thuật toán học máy.

**Luận văn này có hai mục tiêu:**

* + - * Trước tiên, phát triển phương pháp và một hệ thống nhận dạng cử chỉ người và ứng dụng để bảo mật cho các thiết bị di động.
      * Sau đó, đánh giá phương pháp đã đề xuất với dữ liệu được thu thập trên tập hợp 10-20 người dùng khác nhau.

1. Đối tượng và phạm vi nghiên cứu

* **Đối tượng nghiên cứu:** Nghiên cứu và phát triển phương pháp nhận dạng cử chỉ người trên các thiết bị di động và ứng dụng phương pháp này để xây dựng hệ thống bảo mật cho các thiết bị di động.
* **Phạm vi nghiên cứu:** 
  + Nghiên cứu và lập trình với bộ cảm biến gia tốc và xử lý dữ liệu cảm biến gia tốc.
  + Nghiên cứu thuật toán nhận dạng cử chỉ của người.
  + Nghiên cứu và ứng dụng phương pháp này để xây dựng một hệ thống xác thực cho các thiết bị di động.
  + Thử nghiệm và đánh giá phương pháp.

1. Phương pháp nghiên cứu

* Nghiên cứu bộ cảm biến gia tốc: xử lý tín hiệu và dữ liệu gia tốc.
* Nghiên cứu phương pháp xác thực người dùng hiện có trên các thiết bị di động để xác định ưu điểm và hạn chế của các phương pháp này.
* Nghiên cứu một số phương pháp nhận dạng và học máy.
* Nghiên cứu phương pháp nhận dạng cử chỉ người sử dụng trên các thiết bị di động dựa trên bộ cảm biến gia tốc 3-chiều.
* Xây dựng cơ chế xác thực dựa trên việc tự động nhận dạng cử chỉ người trên các thiết bị di động.
* Phát triển hệ thống xác thực dựa trên nhận dạng cử chỉ người.
* Thử nghiệm và đánh giá phương pháp.

# – TỔNG QUAN PHƯƠNG PHÁP XÁC THỰC TRÊN ĐIỆN THOẠI DI ĐỘNG

## Tại sao cần xác thực cho thiết bị di động?

Tự do di chuyển là một trong những khái niệm được mô tả bời tính từ “di động”. Do đó, các thiết bị di động như điện thoại di động, điện thoại thông minh hay PDA phải chấp nhận một vài hạn chế để đạt được tiêu chí “tự do” đó.

* Chúng cần phải nhỏ và nhẹ để có thể mang theo một cách dễ dàng. Chúng cần phải luôn luôn hoạt động, ngay cả khi người sử dụng đang di chuyển, để họ có thể tương tác với bất cứ thứ gì mà họ muốn.
* Trong một vài tình huống, người sử dụng có thể tương tác mà không cần phải tập trung hoàn toàn vào thiết bị. Ví dụ họ muốn tương tác với thiết bị trong khi đang đi bộ.
* Trái ngược với máy tính để bàn truyền thống, thông thường người dùng tương tác với các thiết bị di động thường trong khoảng thời gian rất ngắn nhưng lại diễn ra rất thường xuyên.

Những đặc điểm hạn chế này đòi hỏi các giao diện người dụng phải đặc biệt phù hợp, để các thiết bị di động có khả năng sử dụng trong nhiều tình huống khác nhau. Hiện nay, giao diện người dùng chủ yếu bao gồm một màn hình và một bàn phím thông thường hoặc một màn hình cảm ứng. Các bộ cảm biến khác như cảm biến gia tốc, GPS, cảm biến về trạng thái khoảng cách, camera, microphone, la bàn v.v… có thể cung cấp các thông tin về ngữ cảnh, môi trường và có thể được sử dụng như các thiết bị đầu vào khác như bàn phím hay các cổng kết nối đối với thiết bị di động.

Hầu hết các thiết bị di động đều có khả năng kết nối không dây với khoảng cách xa như GSM/UMTS, khoảng cách trung bình như WLAN và khoảng cách ngắn như Bluetooth, ZigBee và NFC. Điều này cho phép thiết bị, và theo đó là người dùng, có thể kết nối tại bất cứ địa điểm nào và vào bất kỳ thời điểm nào. Khả năng này bao gồm cả kết nối Internet di động và kết nối thông qua kênh thoại.

Một thiết bị di động với các khả năng giao tiếp có thể chờ để giao tiếp trong một phạm vi kết nối hoặc bắt đầu tương tác với các thiết bị có khả năng truy cập khác. Để luôn sẵn sàng kết nối trong phạm vi nào đó thì các thiết bị cần phải được bật và duy trì. Rõ ràng, các thiết bị di động cần phải được vận hành bằng pin, chính điều này đã hạn chế thời gian hoạt động của chúng và làm cho việc tiết kiệm năng lượng trở nên cần thiết. Nếu hết pin thì các thiết bị di động gần như vô dụng cho đến khi pin được nạp đầy trở lại. Hơn nữa, yếu tố về hình thức cũng hạn chế sức mạnh xử lý có thể tích hợp vào điện thoại như kích thước và khả năng làm mát.

Ngày nay, các thiết bị di động là các hệ thộng được cá nhân hóa cho một người sử dụng duy nhất (Karlson, 2009; Eren, 2006), được thiết kế để hỗ trợ người sử dụng giải quyết các nhiệm vụ cụ thể (Schmidt, et al., 1999). Các nhiệm cụ thể của người dùng liên quan đến việc lưu trữ và truy vấn thông tin, giao tiếp, tương tác xã hội và giải trí v.v…(Karlson, 2009). Chính điều này yêu cầu các thiết bị cần phải lưu trữ các dữ liệu cụ thể về người dùng như tin nhắn, thông tin liên hệ v.v… Hơn nữa, các chức năng tích hợp sẵn có thể được mở rộng bằng việc cài các ứng dụng nhỏ khác. Chúng được gọi là các ứng dụng cho phép người dùng điều chỉnh các thiết bị cho phù hợp với các yêu cầu riêng biệt của từng người.

Khả năng sử dụng thiết bị di động gần như là ở khắp mọi nơi, từ những nơi riêng tư cho đến những nơi công cộng. Điều này có nghĩa là những người khác xung quanh bạn có thể cũng đang sử dụng. Do đó, việc sử dụng và tương tác với các thiết bị di động cũng dựa trên bối cảnh xã hội (Rico, 2010). Trong một vài trường hợp, có thể là không phù hợp để sử dụng một chức năng nào đó như nói chuyện điện thoại ngay trong lớp học. Ngoài ra, một số đặc điểm về giao diện người dùng có thể được xem là không phù hợp trong một số trường hợp.

Thiết bị di động cung cấp cho người dùng rất nhiều tiện ích. Xét về khía cạnh này thì rõ ràng các thiết bị di động cần phải lưu trữ nhiều thông tin nhạy cảm về người dùng. Do vậy, chỉ có có người dùng “chính chủ” mới có khả năng xem, sửa đổi hoặc xóa những dữ liệu này. Rõ ràng, dữ liệu nhạy cảm nhất được tạo ra khi sử dụng thiết bị là danh bạ điện thoại, lịch làm việc và các ứng dụng quản lý thông tin cá nhân khác. Nếu thiết bị cũng được sử dụng với các dịch vụ như gọi điện, email, internet, mobile banking (Chong, 2009) và cả thanh toán trên điện thoại di động m-payment (Schwiderski-Grosche, 2002) thì lại có càng nhiều dữ liệu nhạy cảm được lưu trữ. Với nhiều dịch vụ, giống như website và email, cơ chế xác thực dựa trên mật khẩu được sử dụng. Thông thường, username và password cho một dịch vụ sẽ được lưu trên thiết bị, do vậy người sử dụng sẽ không bị yêu cầu nhập lại thông tin của mình mỗi khi sử dụng dịch vụ.

Các thiết bị di động cũng tạo ra dữ liệu người dùng cụ thể. Ví dụ, tần xuất và đối tượng mà người dùng gọi điện. Một thiết bị có thể thu thập và lưu trữ dữ liệu về sự tương tác của người dùng và có thể sử dụng dữ liệu này để hỗ trợ người dùng. Ví dụ như cung cấp danh sách các cuộc gọi gần đây. Các thiết bị di động cũng có thể thu thập dữ liệu bằng việc sử dụng các bộ cảm biến được tích hợp trong nó. Ví dụ một GPS tích hợp sẵn trong thiết bị cho phép xác định vị trí hiện tại và cho phép theo dõi thiết bị. Nếu thiết bị được gắn bộ cảm biến gia tốc (**motion sensor**) nó có thể xác định được khi nào người dùng di chuyển và thu thập thông tin về trạng thái hiện tại. Các thiết bị di động cần phải lưu trữ một lượng lớn dữ liệu hữu ích. Hơn thế nữa, các thiết bị này có thể thu thập một lượng lớn dữ liệu nhạy cảm về người dùng, những thứ mà có khả nằng tiết lộ các đặc điểm rất riêng tư của người dùng chủ sở hữu.

Dữ liệu trên thiết bị di động rất riêng tư và nhạy cảm, nhưng lại rất thú vị đối với những người khác, đặc biệt là những kẻ tấn công tiềm năng. Trái với các máy tính đề bàn, các thiết bị di động được thiết kế để di chuyển và do đó nó không bị giới hạn tại một vị trí cụ thể. Trong nhiều trường hợp, các thiết bị di động có thể được truy cập bởi những người dùng trái phép nếu nó không được giám sát bởi chủ sở hữu của nó. Ngoài ra, một kẻ tấn công cũng có thể lấy cắp điện thoại hoặc một người lạ có thể nhặt được thiết bị sau khi chủ sở hữu bị mất nó. Do đó không thể giả định một cách an toàn rằng người dùng hiện tại là hợp lệ và được phép sử dụng thiết bị. Trên thực tế, trường hợp này đòi hỏi sự bảo đảm về mặt an ninh. Quá trình xác minh người sử dụng hiện tại được gọi là **xác thực**. Không có cơ chế xác thực khả quan nào với tất cả mọi người truy cập vật lý đến thiết bị có thể sử dụng nó như người sử dụng chính chủ. Điều này bao gồm việc truy cập dữ liệu đã được lưu trữ và cả các dịch vụ mà không yêu cầu cơ chế xác thực truyền thống.

Một kẻ tấn công cũng có thể thay đổi phần cứng và phần mềm của thiết bị, do vậy chức năng của thiết bị được toan tính theo ý định của kẻ tấn công và trả nó lại cho chủ sở hữu (Baumgarten, 2001). Ví dụ một thiết bị có thể bị sửa đổi để nó gửi vị trí hiện tại của thiết bị một cách thường xuyên (Dworschak, 2011). Bằng việc sử dụng dữ liệu này, kẻ tấn công có thể theo dõi chủ sở hữu của thiết bị. Ngoài ra, kẻ tấn công có thể thay thế thiết bị chính hãng bằng một thiết bị tương tự có chứa dữ liệu được lưu trữ trên thiết bị chính hãng. Vì vậy, về mặt lý thuyết cần phải xác định thiết bị hiện tại có phải là thiết bị chính hãng hay không. Việc này thường không được thực hiện vì những lý do khách quan. Các thiết bị di động được thiết kế hướng đến người sử dụng thiết bị duy nhất, nhưng đôi khi chủ sở hữu chia sẻ thiết bị với các người khác một cách thoải mái (Karlson, et al., 2009). Trong trường hợp này, một cơ chế xác thực sẽ là vô ích khi chủ sở hữu thiết bị mở khóa thiết bị và đưa nó cho người khác.

Để đạt được mục đích, kẻ tấn công không cần thiết phải truy cập vật lý đến một thiết bị di động. Một cuộc tấn công có thể được thực hiện thông qua các giao tiếp truyền thông. Nếu việc truyền thông không được bảo vệ, một kẻ tấn công có thể nghe lén, sửa đổi, duy trì và giả mạo thông tin (Bishop, 2002). Kiểu tấn công này không mới đối với các thiết bị di động và đã tồn tại từ khi xuất hiện mạng máy tính. Tuy nhiên, ngày càng có nhiều vấn đề bởi vì các thiết bị di động có thể giao tiếp với các thiết bị điện tử xung quanh nó (Bichler, 2005). Một kẻ tấn công có thể tấn công một thiết bị, nếu anh ta có được khoảng cách đủ gần và có thể giao tiếp với thiết bị đó. Trong luận văn này chúng ta sẽ bỏ qua kiểu tấn công này vì nó không liên quan đến việc xác thực người dùng. Tuy nhiên, chúng là những mối đe dọa an ninh thực sự.

## Các nghiên cứu trước đây

### Xác thực dựa trên các đặc điểm sinh trắc học

Tiếp theo, chúng ta sẽ tìm hiểu về phương pháp xác thực người dùng dựa trên sinh trắc học đã được nhắc đến ở các phần trên. Phần này bắt đầu bằng việc giới thiệu tóm tắt tính bảo mật và biện pháp xác thực người dùng nói chung. Sau đó, thảo luận về các cơ chế xác thực và giới thiệu về các hình thức tấn công xác thực người dùng dựa trên sinh trắc học. Sinh trắc học (**biometrics**) là lĩnh vực nghiên cứu các phương pháp toán học và thống kê áp dụng trên các bài toán phân tích dữ liệu sinh học. Cụm từ “biometrics” xuất phát từ chữ “bio” (life) và “metrics” (measure) trong tiếng Hy Lạp.

Sinh trắc học gồm các phương pháp nhận diện một người dựa trên các đặc điểm sinh lý học (physiological) hay các đặc điểm hành vi (behavioral) của người đó. Các hệ thống sinh trắc đã và đang được phát triển trong các ứng dụng thực tế như hệ thống bảo mật giao tác, quản lý truy xuất, các hệ thống điều phối. Sinh trắc học đem lại một số ưu điểm so với các phương pháp bảo mật truyền thống (card, password...) như: không thể hoặc rất khó giả mạo, không bị đánh cắp hay bị mất... Tuy nhiên, kết quả của các công trình nghiên cứu trên lĩnh vực này vẫn chưa đủ hoàn thiện để có thể thay thế hẳn các phương pháp truyền thống. Hiện nay, kỹ thuật sinh trắc thường được sử dụng kết hợp với password hay card để tăng cường khả năng bảo mật cũng như tính an toàn của dữ liệu.

Sinh trắc học được sử dụng theo hai hình thức chính là định danh (**identification**) và xác minh (**verification**):

* Định danh: xác định cụ thể mẫu sinh trắc thuộc về ai. Cơ chế định danh thông qua việc tìm một bộ khớp nhất trong database so với mẫu test. Phương pháp này đòi hỏi rất nhiều chi phí tính toán nếu kích thước database lớn.
* Xác minh: xác định xem mẫu sinh trắc có phải thuộc về một chủ thể cho trước hay không. Cơ chế xác minh thông qua việc so khớp giữa mẫu test với các mẫu thuộc chủ thể đó trong database. Do vậy, phương pháp này đòi hỏi ít năng lực xử lý và thời gian tính toán hơn phương pháp định danh.

#### Bảo mật và xác thực người dùng

Một hệ thống có thể được mô tả như một máy trạng thái với các trạng thái an toàn, trạng thái không an toàn và các quá trình chuyển trạng thái. Định nghĩa hệ thống bao gồm tất cả các đối tượng tương tác – người và máy - và các kênh giao tiếp tiềm năng. Nếu không tồn tại trường hợp chuyển trạng thái từ một trạng thái bất kỳ sang trạng thái không an toàn, thì hệ thống được gọi là an toàn. Mục tiêu của bảo mật là phát hiện và ngăn chặn các trường hợp chuyển trạng thái không an toàn và hơn thế nữa là để khôi phục các quá trình chuyển trạng thái không an toàn. Một hệ thống cẩn phải đảm bảo được tiêu chí này trong hầu hết các trường hợp có thể xảy ra trên thực tế. Do vậy, các cơ chế và chính sách bảo mật được áp dụng. Các chính sách bảo mật chỉ ra những gì được phép và không được phép trong một hệ thống và được thực thi bởi các cơ chế bảo mật. Các chính sách và cơ chế bảo mật được giả định là rõ ràng và chính xác. Trong thực tế, nếu giả định này không được duy trì thì hệ thống trở nên không an toàn. Liên quan đến dữ liệu, bảo mật dẫn đến tính toàn vẹn, tin cậy, sẵn có, xác thực và không thể chối bỏ.

* Tính toàn vẹn đạt được khi và chỉ khi chỉ có các bên đã được xác nhận mới được phép sửa đổi dữ liệu.
* Tính tin cậy có nghĩa là chỉ có các bên đã được xác nhận mới được phép truy cập dữ liệu. Trên thực tế, tính tin cậy liên quan đến tính bí mật.
* Tính sẵn có đảm bảo rằng dữ liệu luôn ở trạng thái sẵn sàng khi các bên truy cập đến nó.
* Tính xác thực và tính không thể chối bỏ có ý nghĩa gần giống nhau. Trong khi tính xác thực có nghĩa là thông tin để nhận dạng của một bên nào đó là có thể kiểm chứng được thì tính không thể chối bỏ là có thể kiểm chứng được bên nào phải chịu trách nhiệm cho một hành động nào đó.

Tính bảo mật cũng chỉ ra rằng người dùng hiện tại chỉ được phép truy cập các chức năng và dữ liệu mà anh ta đã được xác nhận. Trong lần sử dụng đầu tiên, thông tin nhận dạng về người dùng được tạo ra. Thông tin nhận dạng chỉ ra những gì người dùng được phép làm và cách thức người dùng đó chứng minh anh ta là một người dùng hợp lệ. Việc tạo ra một mối quan hệ tin tưởng được gọi là quá trình ghi danh (***enrollment process***). Giả định được tạo ra mà chỉ có người dùng hợp lệ mới có thể cung cấp bằng chứng để nhận dạng trong quá trình xác thực. Quá trình xác thực bao gồm 2 bước. Ở bước nhận dạng, người dùng hiện hành phải truyền vào thông tin nhận dạng mà anh ta định sử dụng. Ở bước tiếp theo, bước xác nhận, người dùng cần cung cấp bằng chứng cho thông tin nhận dạng đã chọn ở bước trước. Nếu bằng chứng hợp lệ, thông tin nhận dạng được chấp nhận. Quá trình nhận dạng có thể được bỏ qua nếu bằng chứng là duy nhất trong hệ thống. Trong trường hợp này, quá trình xác thực được gọi là nhận dạng. Trên thực tế, quá trình xác thực được thực hiện thường xuyên hơn quá trình ghi danh.

Việc xác thực có thể là rời rạc hoặc liên tục. Nó được gọi là rời rạc nếu sau khi xác thực thành công, việc truy cập được cho phép trong một khoảng thời gian nhất định hoặc cho đến khi người dùng đăng xuất. Các cơ chế xác thực liên tục xác minh người dùng trong toàn bộ quá trình tương tác. Điều này thường được thực hiện ngầm định (chế độ nền), vì nếu không nó sẽ yêu cầu người dùng phải tập trung và thao tác quá nhiều và ảnh hưởng đến thao tác chính của mình.

Bằng chứng để nhận dạng có thể dựa trên cái mà người dùng biết, sở hữu, thông tin nhận dạng anh ta là ai hoặc hành vi của anh ta. Các cách tiếp cận dựa trên tri thức sử dụng một mã bí mật được biết bởi người dùng và chỉ có cơ chế xác thực. Các cơ chế xác thực dựa trên tính sở hữu cho rằng chỉ có người dùng hợp lệ mới có thể cung cấp một mã bí mật nhận tạo duy nhất. Nếu có thể giả định một cách an toàn rằng mật mã không thể bị sao chép và người dùng chính thống sở hữu nó thì chỉ anh ta mới có khả năng tiến hành xác thực thành công. Do đó, các cơ chế bảo mật này là có thể kiểm chứng được.

Các đặc điểm sinh trắc học đánh giá được các đặc tính của con người. Điều này cho phép xác minh người dùng dựa trên tiêu chí anh ta là ai hoặc cách thức thực hiện hành vi của anh ta như thế nào. Cắc đặc điểm mà sử dụng các thuộc tính có thể đo lường được của cơ thể người dùng được gọi là các đặc điểm sinh học. Trên thực tế, các bộ phận trên cơ thể được sử dụng như các mật mã sinh học như dấu vân tay hoặc mống mắt. Thông thường, các đặc điểm về sinh trắc học không thể thay đổi một cách dễ dàng. Đôi khi, các đặc trưng về đặc điểm sinh học được sử dụng của người dùng tiếp xúc với kẻ tấn công và do đó hắn ta có thể tạo ra các thông tin giả mạo. Trong trường hợp này các thuộc tính khác cần được sử dụng để đạt được tính bảo mật. Hơn nữa, các đặc điểm sinh học có thể để lộ ra thông tin về cơ thể của người sử dụng mà đó có thể là những thông tin riêng tư. Các đặc trưng sinh trắc học dựa trên hành vi đánh giá cách thức người sử dụng thực hiện hành vi. Các đặc trưng này phụ thuộc vào các đặc điểm sinh học, dựa trên kiến thức và thói quen của người sử dụng. Các cơ chế dựa trên các đặc trưng về sinh trắc học để chứng minh người sử dụng hợp lệ là thật, trong khi đó các cơ chế dựa trên mật mã và tri thức cần phải giả định nó.

Cơ chế xác thực dựa trên sinh trắc học sử dụng một hoặc nhiều bộ cảm biến để lấy được các đặc điểm cần thiết của người dùng hiện tại. Trái với các cơ chế xác thực dựa trên tri thức, việc đo lường và đánh giá các đặc trưng sinh trắc là rất khó khăn, bởi vì con người không phải là một thực thể tĩnh mà thay đổi theo thời gian. Ngoài ra, việc xác thực có thể được yêu cầu trong các tình huống khác nhau. Do đó, các phép đo khác nhau của các đặc trưng được sử dụng rất khó để xác định giống nhau một cách chính xác. Chính vì vậy, sự không giống nhau cần phải được xem xét khi so sáng phép đo hiện tại với các phép đo đăng ký để quyết định xem người dùng hiện tại hợp lệ hay không.

#### Các yêu đầu đối với đặc điểm sinh trắc học

Không phải tất cả các đặc trưng về sinh trắc học đều hữu ích. Một đặc trưng hữu ích cần phải có mức độ dao đông biến đổi thấp, trong khi các đặc trưng khác lại có khoảng cách biến đổi lớn. Điều này có nghĩa là các mẫu thử nghiệm trên một người chỉ có một chút sự khác nhau, trong khi đó các mẫu thử trên những người khác nhau sẽ có sự khác nhau rõ rệt. Khi mức độ dao động tăng lên thì xác suất chấp nhận các mẫu thử không chính xác cũng tăng lên và việc giả mạo trở nên dễ dàng hơn. Đễ xác nhận dạng được thì các đặc trưng phải là duy nhất cho từng người dùng.

Nhìn chung, một đặc trưng sinh học bao giờ cũng có tính ổn định dù ít hay nhiều vì nó chị bị thay đổi chậm theo thời gian. Trong khi đó, người dùng điện thoại sẽ được yêu cầu lặp lại quá trình đăng ký mỗi khi các đặc điểm về sinh trắc của anh ta thay đổi quá nhiều. Một yêu cầu thêm nữa cho các tính năng sinh trắc học là tất cả người dùng tiềm năng cần tham gia thực hiện từng tính năng. Ngoài ra, một điều quan trọng đó là một tính năng sinh trắc học cần phải được đo một cách đáng tin cậy và quá trình đo này phải nhanh và thuận tiện cho người sử dụng.

#### Các mối nguy hai đối với cơ chế xác thực người dùng dựa trên sinh trắc học

Các cơ chế xác thực người dùng được sử dụng để xác minh tính hợp lệ của người dùng hiện tại, nhưng chúng không phải là hoàn hảo. Bất kỳ một cơ chế xác thực nào cũng yêu cầu người dùng đưa cấp bằng chứng trong quá trình xử lý xác thực, chính điều này có thể giúp cho các kẻ tấn công có thể có được thông tin về bằng chứng để xác thực. Thông tin này có thể làm tăng khả năng thành công của các cuộc tấn công. Đây thực sự là một vấn đề đặc biệt đối với các cơ chế xác thực dựa trên tri thức, bởi vì để xác thực chỉ cần yêu cầu thông tin về mã bí mật. Để đảm bảo tính bảo mật một cách chắc chắn, thì hoặc là thông tin nhập vào phải được giấu kín trong quá trình xác thực hoặc là việc giả mạo phải không thể được thực hiện bởi những kẻ tấn công thông thường.

Một vấn đề khác là các cơ chế xác thực người dùng là chỉ chứng minh được tính hợp lệ của người dùng mà không thể xác minh được động cơ của người dùng. Việc xác thực thành công của một người dùng hợp lệ không đảm bảo rằng anh ta sẽ không phá vỡ hệ thống bảo mật. Ví dụ một người dùng có thể bị ép buộc hoặc bị lừa để xác thực bởi một kẻ tấn công nào đó, để hắn có thể truy cập lại hệ thống và tấn công từ bên trong.

Hơn nữa, mục tiêu của bảo mật và mục tiêu của khả năng sử dụng lại xung đột với nhau. Mục tiêu của bảo mật từ quan điểm sử dụng là “làm cho những hành động không mong muốn trở nên khó khăn hơn”, trong khi đó mục tiêu của khả năng sử dụng là làm cho mọi thứ trở nên dễ dàng hơn. Từ khía cạnh của người sử dụng, các cơ chế xác thực thường được xem là trở ngại gây phiền toái nên tránh, vì người dùng thường phải tương tác với các cơ chế này và làm gián đoạn công việc của họ.

“*Nếu tính bảo mật và/hoặc tính riêng tư và khả năng sử dụng xung đột với nhau, thì khả năng sử dụng luôn giành phần thắng!*”

Người sử dụng có thể vô hiệu hóa các cơ chế gây phiên nhiều nếu họ được phép. Họ cũng có thể không kích hoạt các cơ chế này. Thường là không đủ nếu chỉ thêm một lớp xác thực vào tầng giao diện, mà hơn thế các cơ chế cần tích hợp một cách kỹ lưỡng và nhất quán trong quá trình thiết kế hệ thống. Trên thực tế, người dùng thường không nhận ra hoặc đánh giá thấp các nguy cơ mà các cơ chế xác thực phải đối phó. Người sử dụng cũng có xu hướng vô hiệu hóa các cơ chế xác thực. Một cơ chế xác thực người dùng yếu cũng có thể làm suy giảm hệ thống bảo mật. Người sử dụng có thể cảm thấy cảm giác không an toàn, mặc dù nó không được đảm bảo. Người dùng cảm thấy an toàn sẽ tương tác với hệ thống theo một cách mà đòi hỏi các chuẩn bảo mật cao hơn. Hơn nữa, người sử dụng cũng có thể hủy hoại tính bảo mật bởi một hành vi không an toàn như viết ra mật khẩu. Bảo mật không chỉ đơn thuần là vấn đề kỹ thuật mà còn là vấn đề tổ chức, bởi vì người sử dụng là một phần của hệ thống.

“*Người dùng đầu cuối đóng vai trò quan trong trong việc đạt được bảo mật hệ thống. Nếu các hệ thống bảo mật được thiết kế để đáp ứng các yêu cầu và hạn chế của người dùng thông thường thì nhiều khả năng hệ thống bảo mật sẽ thành công.*”

#### Hiệu quả của các cơ chế xác thực người dùng dựa trên sinh trắc học

Việc thực thi các cơ chế xác thực người dùng rất đa dạng và tùy thuộc vào từng trường hợp cụ thể. Để đánh giá các đặc điểm và các kết luận trong quá trình thực thi, Renaud đã phát triển ra 4 loại: khả năng tiếp cận, khả năng ghi nhớ, tính bảo mật và chi phí.

* ***Khả năng tiếp cận:*** bao gồm các yêu cầu cho từng cơ chế xác thực, tính thuận tiện trong sử dụng và cả các yêu cầu về phía người sử dụng. Các yêu cầu là phần cứng, phần mềm và kiến thức về kỹ thuật của người dùng tiềm năng. Sự thuận tiện trong quá trình sử dụng liên quan đến khả năng sử dụng của cơ chế bao gồm việc đăng ký, xác thực và thay thế bằng chứng. Các yêu cầu về phía người sử dụng mô tả các yêu cầu của một cơ chế xác thực mà người dùng tiềm năng cần phải đáp ứng. Cơ chế xác thực chỉ có thể được sử dụng bởi người dùng, người mà có tất cả các khả năng về vật lý, cảm giác và nhận thức.
* ***Khả năng ghi nhớ:*** bao hàm độ sâu xử lý khi đăng ký, chiến lược phục hồi khi xác thực, và tính gợi nhớ của thông tin. Nhớ lại mà không cần tín hiệu, nhớ lại có tin hiệu hoặc nhận dạng có thể được sử dụng như các chiến lược phục hồi. Xuất phát từ quan điểm sử dụng thì cả hai cách, nhận dạng hoặc hỗ trợ người dùng gắn ý nghĩa vào thông tin mà anh ta phải nghi nhớ, tốt hơn so với việc nhớ lại với tín hiệu.
* ***Bảo mật:*** được cấu thành bởi các tiêu chí như: tiết lộ, khả năng tiên đoán và bí mật, khả năng xâm nhập và độ hội tụ, và tính riêng tư.
  + Tiết lộ có nghĩa là bằng chứng hợp lệ có thể đệ lộ ra cho người khác một cách vô tình hoặc cố ý. Điều này cũng bao gồm việc tiết lộ trong quá trình xác thực.
  + Khả năng tiên đoán có nghĩa là nếu một kẻ tấn công có đủ thông tin về người dùng, thì anh ta có thể đoán ra được chứng cứ để tiến hành xác thực.
  + Khả năng giữ bí mật mô tả cách thức chứng cứ được bảo vệ trong quá trình xác thực.
  + Khả năng xâm nhập chính là khả năng phá vỡ một cơ chế mà không cần bất cứ thông tin trợ giúp trước đó.
  + Độ hội tụ nói về khoảng thời gian cần thiết để phá vỡ hệ thống bảo mật.
  + Tính riêng tư về thông tin người dùng cần phải cung cấp trong quá trình xác thực.

Trên thực tế thì không chỉ những tiêu chí ở trên mới quan trọng mà còn có tiêu chí về chi phí. Tổng chi phí của một cơ chế bao gồm phát triển, triển khai và vận hành. Ngoài ra, chi phí còn bao gồm những phát sinh trong trường hợp hệ thống bảo mật bị phá hỏng.

Tiêu chí đo hiệu năng đã trình bầy ở phần trên là rất tổng quát và có thể được sử dụng để đánh giá và so sánh các cơ chế xác thực khác nhau, do vậy cách phù hợp nhất là chọn một trường hợp cụ thể nào đó. Tuy nhiên, việc đánh giá hiệu năng ban đầu của một cơ chế xác thực sinh trắc học thường được thực hiện một cách thực tế hơn là chỉ dựa trên tính khả thi.

Các tiêu chí đo được sử dụng rộng rãi sẽ được giới thiệu bao gồm: Failure-to-Enroll (FTE), Failure-to-Acquire (FTA), False-Rejection-Rate (FRR) và False-Acceptance-Rate (FAR).

* FTE đo tỷ lệ người dùng không thể sử dụng cơ chế bởi vì họ không cần đến cơ chế xác thực.
* FTA đo số lần người dùng không thể xác thực do hệ thống không thể lấy được các đặc tính tạm thời.
* FRR đo tần suất các chứng cứ hợp lệ bị từ chối và do đó quá trình xác thực một người dùng hợp lệ không thành công.
* FAR đo tần xuất cơ chế xác thực chấp nhận các chứng cứ giả là hợp lệ. Trong trường hợp này quá trình xác thực thành công mặc dù người dùng hiện tại không hợp lệ.

Hai tiêu chí FAR và FRR liên quan chặt chẽ đến nhau, bởi vì cả hai đều phụ thuộc vào độ dao động được cho phép. Để hình dung sự cân bằng giữa FRR và FAR, bộ tiếp nhận đặc điểm hoạt động (Receiver Operating Characteristic - ROC) được sử dụng. Để chọn ra các tham số cho cơ chế xác thực, tức là các biến thể cho phép, thường là EER được chọn (Equal-Error-Rate – EER), tức là cả FAR và FRR đều bình đẳng.

Các tiêu chí đo cho cơ chế xác thực người dùng sinh trắc học đã trình bày ở trên chỉ có thể được xấp xỉ hóa trong các nghiêu cứu người dùng, bởi loại thông tin này không sẵn có trong các tình huống thực tế. Chính vì lý do này, các kết luận về một cơ chế xác thực phụ thuộc rất nhiều vào việc thiết lập và các tình huống của một trường hợp nghiên cứu được thực hiện. Do các chỉ số hiệu năng cho các cơ chế sinh trắc FAR và FRR thường được sử dụng mà không tính đến các nỗ lực giả mạo phức tạp và tinh vi. Bỏ qua các chỉ số đo ở trên trong việc đánh ra sẽ cho ra kết quả tốt hơn, nhưng sẽ dẫn đến các kết luận sai về hiệu suất bảo mật. Để đánh giá hiệu suất bảo mật một cách kỹ lưỡng, điều cần thiết là phải đánh giá các tài nguyên, khả năng và kỹ năng của kẻ tấn công tiềm năng và nghiên cứu các cuộc tấn công mở và có thể sử dụng các kết quả này trong các nghiên cứu sử dụng.

#### Các kiểu tấn công đối với cơ chế xác thực dựa trên sinh trắc học

Các cơ chế xác thực người dùng cần bảo vệ hệ thống khỏi các kẻ tấn công tiềm năng. Sau đây sẽ nói về một hệ thống phân loại các cuộc tấn công dựa trên hiểu biết về kẻ tấn công. Với một cuộc tấn công thành công với cơ chế xác thực sinh trắc học, kẻ tấn công cần phải có khả năng tạo ra một sự giả mạo, để các bộ cảm ứng tạo ra các số đo tương tự như chứng cứ thật. Cường độ của các mối đe dọa có thể khác nhau tùy thuộc vào các kỹ năng, động cơ và thời gian để chuẩn bị của một kẻ tấn công tiềm năng. Mỗi mối đe dọa sẽ làm tăng thêm một kẻ tấn công biết về chức năng của cơ chế và tăng thêm tài nguyên bị xâm nhập. Đông cơ có thể là đủ để có được các kỹ năng và và kiến thức, nhưng thời gian và tài nguyên luôn luôn là các yếu tố bị hạn chế.

Bất kỳ kiến thức nào về chứng cứ hợp lệ cho việc xác thực đều làm gia tăng các mối nguy hại. Nếu tất cả các thông tin này đều được biết bởi kẻ tấn công thì anh ta có thể vượt qua cơ chế xác thực thành công.

Các cuộc tấn công được gọi “ngây thơ”(naïve) nếu một kẻ tấn công có một động cơ nhất định, nhưng lại rất hạn chế để tấn công một hệ thống và do đó cần phá vỡ cơ chế xác thực tại chỗ, nhưng lại không có thông tin về chứng cứ để giả mạo và không có khả năng để lấy được thông tin này. Kiểu tấn công này thường được sử dụng trong việc đánh giá chứng cứ của các cơ chế xác thực, ở đó tất cả người tham gia đều được coi là các người dùng hợp lệ. Tất cả các mẫu không hợp hệ chỉ đơn giản được sử dụng như các sử giả mạo. Tuy nhiên, các bằng chứng giả mạo được tạo ra không nhằm mục đích tấn công. Trên thực thế, cần nhấn mạnh rằng việc xác minh này không thể được sử dụng để đánh giá hiệu suất bảo mật thực tế, bởi vì một kẻ tấn công thực sự sẽ có nhiều khả năng kiến thức về các chứng cứ hợp lệ. Do đó, việc giả mạo một cách “ngây thơ” chỉ cho phép đánh giá một cách rất hạn chế các cuộc tấn công ở thế giới thực. Một sự giả mạo từ một kẻ tấn công, người mà có thông tin, tài nguyên và động cơ để tấn công, được gọi là giả mạo lão luyện hoặc có tay nghề cao. Một sự giả mạo có tay nghề cao luôn luôn có nhiều khả năng được chấp nhận trong quá trình xác thực hơn so với sự giả mạo ngây thơ. Một kiểu tấn công không thể ngăn chặn bởi xác thực sinh trắc học là tấn công cưỡng chế. Những kẻ tấn công đe doạ người dùng hợp lệ xác thực và cấp quyền truy cập cho chúng. Một trường hợp tấn công cưỡng chế là tấn công để tống tiền.

Để đánh giá mức độ bảo mật có thể đạt được trên thực tế của một cơ chế xác thực sinh trắc học, đầu tiên phải xác định được các kịch bản sử dụng chính, sau đó phải xác định các kiểu tấn công tiềm năng và khả năng của chúng. Việc sử dụng kiến thức này có thể đánh giá được sức đề kháng của cơ chế đối với các cuộc tấn công trong các điều kiện thực tế hơn. Các tiêu chí FAR và FRR của các cơ chế xác thực khác nhau chỉ có thể so sánh nếu các cuộc tấn công được nghiên cứu cũng được so sánh.

### Xác thực dựa trên chuyển động

Trong phần tiếp theo, các kỹ thuật nhận dạng và xác thực người dùng dựa trên chuyển động được giới thiệu. Người sử dụng hợp lệ chứng minh danh tính của mình bằng một chuyển động có thể đo được với giả định rằng chỉ có người sử dụng hợp lệ mới có khả năng cung cấp các mẫu của một chuyển động hợp lệ. Sau đó, các cách tiếp cận dựa trên chuyển động sẽ được trình bày, cách tiếp cận này yêu cầu người sử dụng ghi nhớ một chuyển động mà anh ta có thể lặp lại một cách tương tự sau này và người sử dụng có khả năng quyết định khi nào thực hiện chuyển động. Phương pháp này không bao gồm các cơ chế như nhận dạng dáng đi.

Trước khi trình bày các cơ chế xác thực người dùng dựa trên chuyển động, chúng ta sẽ tìm hiều về các cơ chế chuyển động của các thiết bị ghép cặp (pairing). Trong phần 2.3.4, chúng ta sẽ tìm hiều về cơ chế xác thực dựa trên cử chỉ người – một lớp con của xác thực dựa trên chuyển động.

#### Ghép cặp thiết bị dựa trên chuyển động

Các thiết bị điện tử thường giao tiếp với nhau thông qua các kênh nặc danh và do đó không thể phân biệt được nguồn gốc của thông điệp. Để tích hợp các mục tiêu về an toàn thông tin, cần phải thiết lập một mối quan hệ đáng tin cậy giữa hai hoặc nhiều thiết bị ở lần kết nối đầu tiên. Điều này được gọi là ghép cặp (pairing). Nó tương đương với quá trình đăng ký ở cơ chế xác thực người dùng. Đầu tiên, người sử dụng cần chọn ra các thiết bị muốn ghép cặp. Tiếp theo, anh ta sẽ thiết lập một kênh giao tiếp an toàn giữa các thiết bị để bảo vệ thông tin liên lạc ban đầu được sử dụng để trao đổi các mã bí mật trên từng thiết bị hoặc anh ta sẽ tạo ra một mã bí mật cho tất cả các thiết bị. Bằng việc sử dụng các mã bí mật, các mối quan hệ đáng tin cậy được thiết lập. Một ví dụ về ghép cặp đó là quá trình ghép cặp dựa trên Bluetooth. Cách tiếp cận này đòi hỏi các thiết bị có một giao diện người dùng với các khả năng tương tác đầy đủ để nhập vào một mã bí mật. Đối với một số loại thiết bị, yêu cầu này có thể không phù hợp hoặc thậm chí là không thể. Ví dụ các tai nghe Bluetooth thường sử dụng một mã bí mật cố định – thường là 0000 – bởi vì chúng có một giao diện sử dụng rất hạn chế. Do một mã bí mật cố định là không an toàn nên nó không thích hợp cho một quá trình ghép cặp.

Tiếp theo, các cách tiếp cận khác sử dụng chuyển động của người dùng như là các mã bí mật cho việc ghép cặp được giới thiệu. Để ghép cặp hai thiết bị, người dùng cầm chúng và tiến hành di chuyển trong cùng một khoảng thời gian theo cùng một cách, ví dụ người dùng cầm cả hai thiết bị trên cùng một tay và di chuyển chúng. Giả sử chỉ những thiết bị cần ghép cặp được di chuyển, việc di chuyển được coi là mã bí mật. Trên thực tế, các thiết bị cần phải có khả năng để đo được các chuyển động và tạo ra các chỉ số có thể so sánh được. Người ta đã sử dụng các chỉ số về gia tốc được nhúng trong các thiết bị. Việc lựa chọn các thiết bị để ghép cặp là hoàn toàn tự nhiên, bởi vì người dùng chỉ đơn giản là cầm các thiết bị lên. Người dùng không cần ghi nhớ chuyển động, bởi vì nó được sử dụng như mã bí mật một lần và việc sử dụng các chuyển động tương tự nhau cho nhiều quá trình ghép cặp có thể làm cho chúng có khả năng bị tấn công.

Patel đã tạo ra kỹ thuật ghép cặp dựa trên chuyển động để ghép cặp một thiết bị di động với một thiết bị đầu cuối phổ thông/công cộng trong một khoảng thời gian nào đó. Kiểu ghép cặp có thể là cần thiết, nếu thiết bị đầu cuối được sử dụng như thiết bị đầu vào cho thiết bị di động hoặc để gán quyền truy cập đến dữ liệu được lưu trữ trên thiết bị đầu cuối. Cách tiếp cận này đòi hỏi các các thiết bị di động và thiết bị đầu cuối có thể giao tiếp trực tiếp với nhau. Thiết bị di động thông báo sự có mặt của nó với thiết bị đầu cuối và người dùng chọn thiết bị di động của mình trên các thiết bị đầu cuối công cộng mà yêu cầu người dùng di chuyển thiết bị theo một cách cụ thể nào đó. Sau đó, thiết bị đầu cuối kết nối với thiết bị di động và yêu cầu thiết bị di động gửi các thông số đo được của chuyển động. Quá trình ghép cặp theo thời gian thành công nếu các thông số đo được chấp nhận là tương tự với chuyển động được yêu cầu.

Một kẻ tấn công cần phải xác định được chuyển động, chuyển động này được sử dụng như một mã bí mật. Tiếp theo anh ta có thể có khả năng sử dụng mã bí mật để can thiệp vào quá trình ghép cặp và thiết lập một mối quan hệ giả mạo để lấy được thông tin nhạy cảm.

#### Chuyển động người dùng cho tương tác máy

Trong phần sau, các cơ chế xác thực dựa trên các chuyển động người dùng cho tương tác máy được trình bầy. Tất cả các giao diện người dụng được thiết lập sử dụng các chuyển động của người dùng như là cách thức nhập liệu. Các ví dụ điển hình là các nút bấm, bàn phím, con trỏ và màn hình cảm ứng. Thông thường chỉ một phần nhỏ thông tin có sẵn được sử dụng cho tương tác người-máy giống như là nút nào được ấn và nơi nào người dùng nhấp vào. Trên thực tế, phần thông tin chưa được sử dụng lại rất đáng chú ý cho việc xác thực như là cách thức người dùng sử dụng các thiết bị nhập liệu.

Wobbrock đề suất một cơ chế xác thực được gọi là TapSong sử dụng một nút duy nhất. Người sử dụng tiến hành xác thực bằng cách ấn vào nút đó một cách nhịp nhàng tương tự như nhịp điệu đã chọn trong quá trình đăng ký. Các nhịp điệu được sử dụng dựa trên các bài hát để giúp người dùng dễ dàng hơn trong việc ghi nhớ. Cách tiếp cận này rất thích hợp cho các thiết bị di động vì nó chỉ yêu cầu một nút duy nhất và người dùng có thể tiến hành xác thực mà không cần nhìn vào điện thoại của mình. Hơn nữa, chuyển động cho việc xác thực có thể là rất nhỏ và rất khó quan sát bởi người khác. Người dùng cũng có thể tiến hành xác thực trong khi thiết bị đang nằm trong túi của anh ta và do đó các bằng chứng có thể được che dấu hoàn toàn.

Các cách tiếp cận khả thi khác là sử dụng tổ hợp phím động. Các cơ chế này không sử dụng nội dung người dùng nhập vào mà lại nhận dạng bằng cách thức người dùng tương tác với bàn phím. Ví dụ về các đặc trưng hữu ích như thời giàn bấm phím và thời gian giữ các phím. Các đặc trưng về tổ hợp phím động có thể được đo bằng cách cho phép người dùng nhập vào một đoạn văn bản cho trước hoặc một đoạn văn bản do người dùng cung cấp trong quá trình tương tác bình thường. Trong trường hợp thứ hai, quá trình xác thực có thể được thực hiện một cách liên tục một cách ngầm định. Các tổ hợp phím động có thể được sử dụng trên tất cả các thiết bị mà có sử dụng bàn phím như các thiết bị đầu vào.

Một cách tiếp cận khác thực chất là sự mở rộng của cơ chế xác thực dựa trên mã PIN cho các thiết bị di động bằng việc sử dụng một màn hình cảm ứng điện dung như thiết bị đầu vào được trình bầy bởi Saevanee. Thông thường một nút chỉ cung cấp thông tin về trạng thái hiện tại của nó mà thôi, nó được ấn hay không. Tuy nhiên khái niệm về nút có thể được mở rộng, do đó điện dung được đưa vào.

#### Chữ ký tay

Chữ ký tay là một trong những cách phổ biến nhất để chứng minh danh tính của một người. Chữ viết và các chữ ký trên văn bản được coi là các đặc điểm riêng của từng người. Trên thực tế, chữ ký bằng văn bản được sử dụng để ký kết hợp đồng. Khi một người nào đó ký vào văn bản, điều này có nghĩa là anh ta biết, hiểu và chấp nhận các điểu khoản nội dung. Chữ ký màng tính ràng buộc và pháp luật cấm việc giả mạo chữ ký.

Một chữ ký có thể được xác nhận bằng việc sử dụng thông tin online hoặc offline. Cơ chế xác minh offline chỉ sử dụng hình ảnh kết quả của chữ ký. Hình ảnh này có thể được so sánh với một mẫu hợp lệ nào đó để đánh giá mức độ tương đồng. Các cơ chế xác minh trực tuyến cũng sử dụng thông tin về cách thức hình ảnh được tạo ra. Thông tin này có thể bao gồm tốc độ, các thay đổi của chuyện động và áp lực. Các thông tin này có thể có được bằng cách sử dụng các bảng đồ họa như là các thiết bị đầu vào chứ không phải là bút chì và giấy.

#### Các cử chỉ tay

Trong phần tiếp theo, chúng ta sẽ tìm hiểu về các cơ chế sử dụng cử chỉ tay cho việc xác thực với các bộ cảm biến gia tốc được nhúng trong các thiết bị cầm tay.

Một cơ chế sử dụng các cử chỉ rời rạc để ánh xạ đến các con số của mã PIN trên các thiết bị di động được giới thiệu bởi Chong Chong, 2009; Chong, et al., 2010). Người dùng nhập vào từng số của mã PIN bằng cách áp dụng các cử chỉ tương ứng trên thiết bị di động. Các cử chỉ được sử dụng là các chuyển động trên một tay và trong thời gian ngắn, bắt đầu và kết thúc tại cùng một vị trí. Người dùng cần thực hiện từng cử chỉ một cách chính xác đê việc nhận dạng thành công. Trên thực thế, trong quá trình xác thực người dùng sẽ tiết lộ cử chỉ bí mật được sử dụng như mã PIN và do vậy một kẻ tấn công có thể biết được tập hợp các cử chỉ rời rạc này. Điều này có thể cho phép kẻ tấn công dò được mã PIN bằng cách quan sát các cử chỉ một cách dễ dàng. Anh ta cũng có thể sử dụng thông tin này để bắt chước thứ tự của các cử chỉ hợp lệ vì anh ta không cần phải giả mạo một cách chính xác các chuyển động của người dùng hợp lệ mà chỉ cần thực hiện các cử chỉ rời rạc.

Trong phần tiếp theo, các cơ chế xác thực sử dụng các cử chỉ cá nhân để khắc phục các nhược điểm của các cử chỉ rời rạc sẽ được giới thiệu. Một chữ ký văn bản có thể được coi là một cử chỉ tay mang tính cá nhân, nó được chiếu trên một không gian hai chiều. Trên thực tế, việc xác thực người dùng dựa trên cử chỉ đôi khi còn được gọi là cử chỉ chữ ký.

Okumura đã đề xuất một cơ chế xác thực người dùng bằng cách lắc thiết bị trên một tay. Cơ chế này đòi hỏi thiết bị phải được trang bị bộ cảm biến gia tốc 3 chiều. Trong một nghiên cứu sử dụng với 22 ứng cử viên thì tỷ lệ cân bằng lỗi đạt được là 5%. Phương pháp này được tinh chế bằng cách thêm vào một thủ tục cập nhật các mẫu đăng ký để tăng hiệu suất theo thời gian. Điều này là cần thiết bởi vì theo thời gian người sử dụng cũng tinh chỉnh các chuyển động. Liu đã tạo ra một cơ chế xác thực dựa trên cử chỉ bằng việc sử dụng Nintendo Wii Controller. Cơ chế phân biệt giữa xác thực quan trọng và xác thực không quan trọng. Xác thực quan trọng là cần thiết, nếu cơ chế xác thực được sử dụng để bảo vệ các hệ thống quan trọng. Trên thực tế, điều này đặt ra các yêu cầu cao hơn về bảo mật và do đó độ phức tạp của cử chỉ bị giới hạn bởi các ràng buộc nào đó. Để nghiên cứu giả mạo đối với cơ chế xác thực quan trọng, các video ghi hình quá trình xác thực được sử dụng. Các tấn công tiềm năng có thể xem cách tiếp cận này đầy hứa hẹn, bởi vì các cử chỉ dường như tương đối dễ dàng quan sát. Nhìn chung, một tỉ lệ loại bỏ sai FRR với một tỉ lệ chấp nhận sai FAR 10% đã đạt được cho cơ chế xác thực quan trọng. Với xác thực không quan trọng, không có giả mạo kỹ thuật cao, tỉ lệ loại bỏ sai nằm trong khoảng 1% - 11% tùy thuộc vào từng người dùng. Guerra Casano đã phát triển một cơ chế bằng việc sử dụng điện thoại iPhone 3GS. Họ cũng thực hiện các cuộc tấn công giả lập thông qua các file ghi hình và đạt được kết quả tỷ lệ cân bằng lỗi là 2.5%. Cho đến nay, tất cả các cơ chế đã trình bầy được đánh giá với các nghiên cứu sử dụng khác nhau để những người tham gia được phép lựa chọn những cử chỉ riêng của họ. Farella trình bầy một cơ chế xác định người dùng bằng việc sử dụng các kỹ thuật trích rút các đặc điếm. Kỹ thuật này đạt được độ chính xác 95% bằng việc sử dụng các cử chỉ được định nghĩa trước.

Một cách tiếp cận rất khác trong việc xác thực và nhận dạng người dùng dựa trên cử chỉ được giới thiệu Ketabdar vào năm 2010. Nó có tên là MagiSign và không sử dụng các bộ cảm biến gia tốc gắn trên các thiết bị, mà sử dụng la bàn và nam châm. MagiSign sử dụng một la bàn 3 chiều được tích hợp sẵn trên điện thoại iPhone 3GS để đo sự thay đổi của từ trường được tao ra bởi một thanh từ nhỏ mà người dùng cầm nó như một cây bút. Với cây bút này, người dùng xác thực bằng việc viết bằng chứng của anh ta lên không khí. Cách tiếp cận này tương tự với phương pháp dùng chữ ký văn bản, nhưng các chuyển động 3 chiều là có thể. Trong một nghiên cứu sử dụng, một tỉ lệ loại bỏ lỗi FRR 4.8% và tỉ lệ chấp nhận lỗi 0.3% đã đạt được.

Tất cả các cơ chế đã trình bầy với các bộ cảm biến gia tốc được sử dụng nhưg một bộ cảm biến gia tốc 3 chiều. Do đó, một cơ chế sử dụng sự kết hợp của bộ cảm biến gia tốc và con quay hồi chuyển để đo các chuyển động để cho ra kết quả tốt hơn sẽ được trình bầy trong luận văn này.

## Xác thực trên điện thoại di động bằng nhận dạng cử chỉ người

Các nghiên cứu trước đây đã chỉ ra rằng xác thực dựa trên cử chỉ với các cử chỉ tay và bộ cảm biến gia tốc là khả thi. Xác thực dựa trên cử chỉ tỏ ra đầy hứa hẹn các thiết bị di động, bởi vì các khả năng về giao diện sử dụng bị giới hạn. Các cử chỉ tay là các đặc điểm sinh trắc của từng người và có một số đặc điểm đầy hứa hẹn. Người dùng không nhất thiết phải nhớ một mã bí mật. Thay vào đó, anh ta huấn luyện một cử chỉ và nó sẽ được lưu một cách ngầm định trên vỏ não. Do đó, bằng chứng xác thực không thể được chuyển qua cho người khác một cách dễ dàng. Xác thực dựa trên cử chỉ có thể là một lựa chọn hữu ích thay thế cho các cơ chế xác thực dựa trên tri thức cho các thiết bị di động.

Để có được đánh giá bước đầu cho cơ chế xác thực dựa trên cử chỉ, có 4 câu hỏi được xem là quan trọng cần được nghiên cứu một cách chi tiết:

1. Các đặc trưng về sinh trắc học của mỗi người liệu có đủ để tiến hành xác thực?
2. Cơ chế xác thực dựa trên cử chỉ yêu cầu những gì từ các người dùng tiềm năng?
3. Làm thế nào có thể sử dụng cơ chế xác thực dựa trên cử chỉ đừng từ quan điểm của người sử dụng?
4. Các thể loại tấn công có thể và thực sự đối với cơ chế xác thực này?

Những câu hỏi này đã được sử dụng như những hướng dẫn trong luận văn này. Câu hỏi 1 là về tính khả thi. Các gợi ý cho câu hỏi này đã được đưa ra bởi nghiên cứu trước đây về xác thực người dùng dựa trên cử chỉ người bằng việc sử dụng các bộ cảm biến gia tốc được trình bầy ở phần 2.3.4. Luận văn này nhằm mục đích chứng minh xác thực dựa trên cử chỉ người là khả thi trên các thiết bị di động bằng việc sử dung các bộ cảm biến gia tốc tích hợp sẵn. Trước khi thảo luận chi tiết về câu hỏi 2 và câu hỏi 3, các yêu cầu cho cơ chế xác thực trên thiết bị di động cần được phân tích. Điều này rất quan trọng vì quan điểm người dùng có thể phát hiện ra các yêu cầu, có thể là không nhìn thấy trực tiếp nhưng nó rất liên quan. Sau đó, cơ chế xác thực dựa trên cử chỉ người sẽ được trình bầy trong luận văn này. Phần này cũng trả lời câu hỏi 2 và câu hỏi 3. Đến cuối chương này, chúng ta sẽ thảo luận về các cuộc tấn công tiềm năng.

Cơ chế xác thực dựa trên cử chỉ trong luận văn này được thiết kế cho các thiết bị di động cầm tay và được tích hợp các bộ cảm biến gia tốc 3 chiều. Để tiến hành xác thực, người dùng nhập vào cử chỉ của mình bằng việc di chuyển thiết bị cầm trên tay. Do vậy, về cơ bản các cử chị bị giới hạn bởi chuyển động của cánh tay và ban tay. Một thiết bị cầm tay chỉ phù hợp với cơ chế này nếu nó đủ nhỏ và nhẹ để việc di chuyển không gây mệt mỏi cho người sử dụng.

Thiết bị cảm biến gia tốc 3 chiều đo được toàn bộ gia tốc trọng trường bao gồm trọng lực, gia tốc trọng trường tác động lên người sử dụng và tất cả các loại gia tốc khác. Một bộ cảm biến gia tốc không thể phân biệt chính xác các nguồn gia tốc khác nhau. Mặc dù vậy, nó có thể được sử dụng để đoán được điệu bộ cử chỉ ở một mức độ chính xác nhất định, nếu có thể phân biệt được hướng của lực hấp dẫn. Điều này là có thể nếu trọng lực là lực tác động lớn nhất. Tuy nhiên, các bộ cảm biến chỉ đo sự chuyển động của thiết bị, điều này có nghĩa là chúng đo chuyển động của người dùng một cách gián tiếp. Hơn nữa, chúng ta không thể có được hướng di chuyển chính xác vì dữ liệu của các bộ cảm biến bị nhiễu và chúng chỉ đo đạo hàm bậc nhất và bậc hai của các thuộc tính. Tuy nhiện, các chuyển động tương tự nhau thì sẽ dẫn đến các số đo tương tự nhau.

Cách tiếp cận phân đoạn tự động bị loại bỏ bởi vì nó quá phức tạp trong việc tính toán. Nó sẽ tiêu tốn nhiều năng lượng và làm chậm quá trình xác thực. Thay vì phân đoạn cử chỉ bằng việc nhần vào một nút nào đó rồi thực hiện từng cử chỉ. Để nhập vào một cử chỉ, người sử dụng nhấn nút liên tục trong quá trình di chuyển. Do đó, điểm đầu và điểm kết thúc của cử chỉ được người dùng nhập vào một cách tương đối chính xác. Quá trình xác thực được thực hiện chủ yếu dựa trên các chỉ số đo. Hơn nữa, tương tác của người dùng với nút bấm trở thành một phần của cử chỉ. Chính điều này vô tình đã đưa vào thêm một số thông tin và làm cho việc giả mạo khó khăn hơn, vì một kẻ tấn công cần phải tương tác với đúng nút đã được thiết lập trước và phải theo cách tương tự.

Quá trình đăng ký của cơ chế xác thực dựa trên cử chỉ ở phía trước. Ban đầu, người dùng chọn hoặc tạo ra một cử chỉ mà anh ta muốn sử dụng cho việc xác thực. Sau khi huấn luyện một cách đầy đủ theo cách riêng của mình, người dùng cung cấp các mẫu chính thức cho thiết bị di động. Điều này cho phép xác định phương sai riêng cho từng người dùng. Các mẫu được sử dụng bởi cơ chế xác thực để học cử chỉ bằng các thuật toán học máy, các thuật toán này sẽ tạo ra một mô hình dưới giả định rằng các mẫu được cung cấp là tiêu biểu. Ở bước xác thực, mô hình này được sử dụng để quyết định xem mẫu thử do người dùng nhập vào để xác thực có giống với mẫu chính thức đã được thiết lập trong quá trình đăng ký hay không, nếu giống thì quá trình xác thực thành công. Ngược lại, người dùng không thể xác thực thành công và truy cập vào thiết bị. Quá trình xác thực và đăng ký của cơ chế xác thực dựa trên cử chỉ sẽ được trình bầy chi tiết trong phần tiếp theo.

#### Một số ưu điểm

Xác thực người dùng dựa trên cử chỉ có một số ưu điểm so với các cơ chế xác thực dựa trên tri thức cho các thiết bị di động hiện nay. Các cơ chế dựa trên tri thức yêu cầu người sử dụng phải ghi nhớ và bảo vệ một mã bí mật tùy ý nào đó. Để đảm bảo tính bảo mật, mã bí mật đó cần phải đủ phức tạp để nó không thể đoán được bởi các kẻ tấn công tiềm năng. Nhưng điều này cũng kiến cho nó khó có thể nhớ được một cách dễ dàng. Trong khi đó, người dùng ghi nhớ các cử chỉ thông qua việc đào tạo những cử chỉ trên vỏ não của họ. Đặc điểm này giúp người dùng tránh được việc phải nhớ một mã bí mật phức tạp. Ngoài ra, một cử chỉ không chỉ đơn giản là viết ra và việc huấn luận ngăn cản việc truyền cử chỉ đến người khác một cách dễ dàng. Ưu điểm khác đó là việc nhập cử chỉ có thể được thực hiện mà không cần dùng mắt bởi vì người sử dụng không cần nhìn vào thiết bị.

Cơ chế xác thực dựa trên cử chỉ sử dụng các đặc trưng về hành vi sinh trắc học để xác thực. Một cơ chế xác thực dựa trên các đặc điểm sinh trắc học cần phải lưu lại các đặc điểm của bằng chứng thật sự, các đặc điểm này sẽ được sử dụng trong quá trình xác thực. Tuy nhiên, thông tin về người dùng thật sự có thể là rất riêng tư và không được để lộ ra. Các đặc điểm được sử dụng bởi cơ chế xác thực dựa trên cử chỉ chỉ liên quan đến chuyển động của tay trong một khoảng thời gian ngắn. Thông tin này không cho phép kẻ tấn công rút ra được các kết luận cụ thể về chủ sở hữu. Hơn nữa, bằng chứng cho cơ chế xác thực dựa trên cử chỉ là đặc điểm sinh trắc học và có thể được thay đổi một cách dễ dàng bằng cách huấn luận một cử chỉ khác và lặp lại quá trình đăng ký. Điều nay là cần thiết.

Xác thực dựa trên cử chỉ có hai yêu cầu quan trọng mà sẽ trả lời cho câu hỏi 2 ở phần trước “Xác thực dựa trên cử chỉ yêu cầu những điều gì từ phía người dùng?”. Trước hết, nó đòi hỏi người sử dụng có thể thực hiện ít nhật một cử chỉ phức tạp và riêng biệt nào đó. Cử chỉ cần phải đủ phức tạp để nó không thể bị bắt chước một cách dễ dàng bởi người khác. Do đó, người sử dụng hoặc là bị hạn chế trong việc thực hiện các cử chỉ bất kỳ hoặc là bạn chế trong việc thực hiện các cử chỉ phức tạp sẽ không có khả năng sử dụng cơ chế xác thực dựa trên cử chỉ, chẳng hạn như những người tàn tật hoặc người già. Ngoài ra, người ốm cũng khó có thể sử dụng được cơ chế này trong thời gian điều trị và phục hồi. Thứ hai, xác thực dựa trên cử chỉ đòi hỏi người dùng thật sự có khả năng lặp lại cử chỉ theo cách tương tự. Tuy nhiên, rất khó để người dùng lặp lại các cử chỉ một cách chính xác. Các chuyển động khác nhau dựa trên cùng một cử chỉ có thể thay đổi theo thời gian và phương hướng.

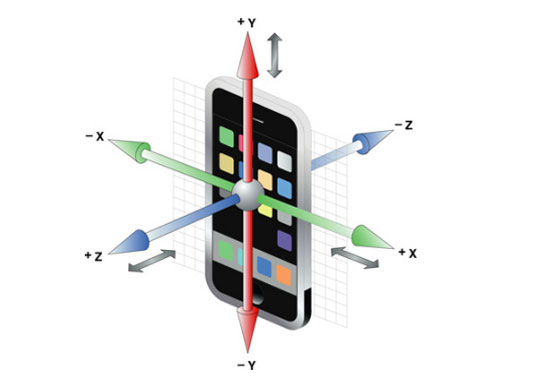
Ngoài ra, một cử chỉ cần phải phức tạp, vì vậy nó có thể được coi là an toàn. Độ phức tạp không chỉ thể hiện ở hướng di chuyển, mà còn bao gồm tốc độ thay đổi và tốc độ xoay. Điều này thậm chí còn gây ra nhiều khó khăn hơn cho người sử dụng trong việc lặp lại chuyển động một cách chính xác hoàn toàn. Trên thực thế, người dùng có thể lặp lại cử chỉ càng chính xác thì phương sai càng nhỏ, phương sai càng nhỏ thì việc giả mạo lại càng khó khăn hơn.

# – PHƯƠNG PHÁP NHẬN DẠNG CỬ CHỈ NGƯỜI

## Cảm biến gia tốc và dữ liệu cảm biến gia tốc trên điện thoại di động

Cảm biến gia tốc (**Accelerometer**) là một thiết bị có thể cảm nhận được sự thay đổi của gia tốc và đo được sự thay đổi đó. Cảm biến gia tốc được chế tạo dựa trên công nghệ vi cơ điện tử và vi hệ thống. Nó đã và đang được ứng dụng một cách mạnh mẽ vào hầu hết các lĩnh vực như y sinh, công nghiệp ôtô, điện tử dân dụng, khoa học không gian...

Tính năng chính của cảm biến gia tốc là nhận diện các thay đổi về hướng của thiết bị di động dựa trên dữ liệu thu được và thay đổi chế độ màn hình (chế độ dọc hoặc ngang màn hình) dựa trên góc nhìn của người dùng. Ví dụ, trong trường hợp bạn muốn tăng chiều rộng hiển thị của một trang web, ta có thể chuyển từ chế độ dọc màn hình sang chế độ ngang màn hình. Tương tự như vậy, ứng dụng camera cũng sẽ tự động thay đổi hướng của bức ảnh đang chụp khi chúng ta thay đổi góc độ của smartphone.



Hình 2.1: Minh họa các chiều của cảm biến gia tốc

Về bản chất, cảm biến gia tốc sẽ nhận diện sự thay đổi trong góc độ của thiết bị di động bằng cách nhận biết các thay đổi về hướng trên cả 3 chiều của không gian trong trường hợp thiết bị di động được di chuyển. Một trong những ví dụ về ứng dụng của cảm biến gia tốc của điện thoại là các trò chơi đua xe: người chơi có thể "bẻ lái" bằng cách quay điện thoại hoặc tablet theo hướng mong muốn.

Cảm biến gia tốc thường được ứng dụng trong việc xác định “gia tốc tĩnh”, tức là gia tốc trọng trường. Tùy theo số trục của cảm biến (1 trục, 2 trục hay 3 trục), giá trị đọc về của cảm biến sẽ là hình chiếu của gia tốc trọng trường trên từng trục tọa độ tương ứng. Chúng ta biết rằng, gia tốc trọng trường tại một điểm là không đổi. Khi bộ cảm biến quay một góc nào đó, hệ trục tọa độ gắn với cảm biến cũng quay theo và do đó hình chiếu của gia tốc trọng trường lên các trục tọa độ đó sẽ thay đổi. Từ các giá trị đó, ta có thể xác định được góc nghiêng hiện tại của cảm biến, cũng như là góc đã quay so với vị trí trước. Ví dụ sau thời gian T mà đo được cảm biến đã quay bao nhiêu độ, thì ta có thể suy ra được vận tốc. Dựa trên vận tốc này, ta có thể suy ra được quỹ đạo chuyển động của cảm biến.

Giá trị đọc về của cảm biến thường được tính theo đơn vị “g”, g là gia tốc trọng trường. Do đó, kết quả tính toán góc nghiêng sau khi chia cho nhau sẽ mất đi thành phần “g”, tức là kết quả đo góc không phụ thuộc vào gia tốc trọng trường, không phụ thuộc vào vị trí địa lý.

## Khoảng cách và sự tương đồng

### Khoảng cách giữa hai điểm

Thông thường khi nói về khoảng cách, chúng ta thường nghĩ về chiều dài giữa hai điểm. Nếu hai điểm này nằm trên cùng một mặt phẳng hoặc không gian Euclidean (xem hình 3.3) thì độ dài được tính bằng trị tuyệt đối hiệu số giữa tọa độ của hai điểm. Nếu các điểm **A** và **B** được xác định bởi các tọa độ **a** và **b** tương ứng thì khoảng cách giữa **A** va **B** sẽ bằng **|a - b|**. Chú ý rằng khoảng cách có tính đối xứng vì khoảng cách giữa **A** và **B** cũng chình bằng khoảng cách giữa **B** và **A** (và |a-b| = |b-a|).



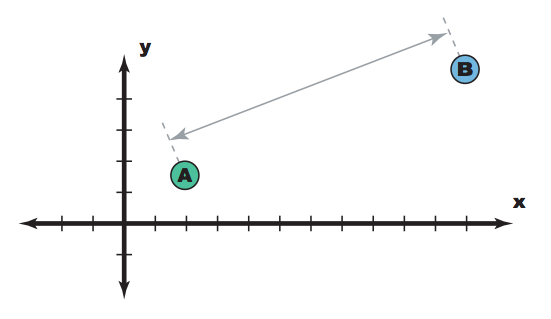
Hình 3.3. Khoảng cách giữa hai điểm trên cùng một mặt phẳng

Trong trường hợp với không gian 2-chiều, mỗi điểm được biểu diễn bởi hai con số cùng nhau tạo nên tọa độ của một điểm. Hai số này chính là vị trí của điểm trên hai trục vuông góc. Chúng được gán nhãn là **x** và **y** như trong hình 3.4.

Nếu các điểm **A** và **B** được xác định bởi các tọa độ  và  tương ứng, thì khoảng cách Euclidean giữa chúng là độ dài của đường thằng nối hai điểm đó với nhau. Độ dài này được tính bởi công thức **Pythagorean**:



Công thức **Pythagorean** được tổng quát hóa để tính khoảng cách giữa hai điểm trong không gian với số chiều bất kỳ. Nếu không gian có D chiều và các điểm A và B được xác định bởi các tọa độ  và  tương ứng thì khoảng cách giữa chúng là . Quay trở lại cách tính khoảng khách giữa hai điểm trên cùng một mặt phẳng hay còn gọi là không gian 1-chiều ta thấy rằng công thức trên vẫn đúng.



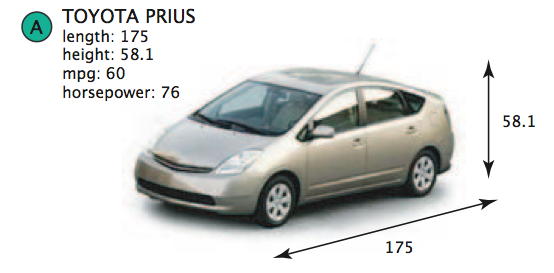
Hình 3.4. Khoảng cách giữa hai điểm trong không gian 2-chiều

### Khoảng cách và sự tương đồng của các đặc điểm

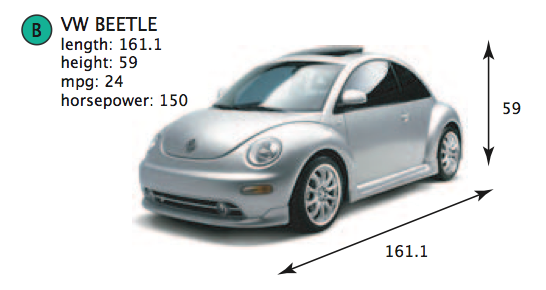
Bây giờ tạm thời hãy bỏ qua các khái niệm về điểm trong không gian. Thay vào đó, chúng ta hãy xem xét một số đối tượng cúng với các đặc điểm của nó. Giả thiết rằng các đặc điểm này có thể được biểu diễn bởi các con số. Ví dụ đơn giản chúng ta có thể coi mỗi chiếc xe hơi là một đối tượng. Thông thường mỗi chiếc xe được miêu tả bởi một vài thông số như chiều dài, chiều cao, số dặm đi được trên mỗi galon nhiên liệu và sức ngựa.

Làm thế nào có thể so sánh 3 đối tượng này với nhau? Prius rõ ràng là tương đồng với Beetle hơn so với Escalade. Nhưng không tồn tại phương pháp đo đối tượng để xác định sự giống nhau và khác nhau giữa những chiếc xe hơi. Phương pháp đơn giản nhất để phân biệt các đối tượng này là chúng ta coi những chiếc xe là các điểm trong một không gian 4-chiều – hoặc có thể gọi là “không gian xe hơi”, ở đó mỗi chiếc xe được biểu diễn bởi một tọa độ gồm 4 số. Trong ví dụ này, điểm A đại diện cho xe Prius được xác định bởi tọa độ <175, 58.1, 60, 76> với các trục tọa độ tương ứng như sau <dài, cao, số dặm cho mỗi galon nhiên liệu, sức ngựa>.

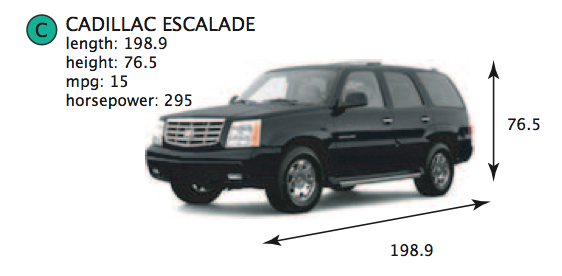
Để tìm ra khoảng cách giữa những chiếc xe hơi, một cách đơn giản là chúng ta sử dụng công thức Euclidean đã được đề cập ở trên. Bằng phương pháp này ta có thể tính được khoảng cách giữa Prius và Beetle là 83.46 và khoảng cách giữa Prius và Escalade là 225.60. Rõ ràng đến đây chúng ta có thể thấy rằng, khoảng cách đã trở thành thước đo để đánh giá sự tương đồng về đặc điểm của các đối tượng. Trên thực tế, tùy theo tiêu chí đánh giá chúng ta có thể cân nhắc một cách hợp lý các đặc điểm khác nhau để làm cho một đặc điểm nào đó quan trọng hơn các đặc điểm khác. Điều này đặc biệt cần thiết bởi vì đơn vị tính cho mỗi đặc điểm là không giống nhau (inches, miles/galon, sức ngựa). Trong ví dụ này, phương pháp đo không đánh trọng số đã cung cấp cho chúng ta cách thức xác định khoảng cách giữa các mô hình xe hơi.



Hình 3.5. Đối tượng A – Toyota Prius



Hình 3.6. Đối tượng B – VW Beetle



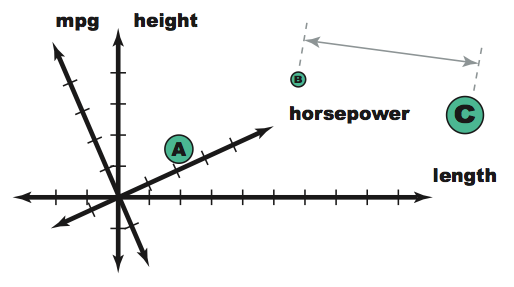
Hình 3.7. Đối tượng C - Cadillac Escalade

### Các loại khoảng cách

Đến thời điểm này, điều quan trọng cần đề cập đến là thực sự không có mối liên hệ không gian nào giữa các đặc điểm khác nhau của những chiếc xe hơi trong phần trước và do đó không cần sử dụng công thức Pythagorean để đo khoảng cách. Nó không phải là một khái niệm chỉ có ý nghĩa về mặt khoảng cách (mặc dù nó có sự liên quan đặt biệt với không gian Euclidean). Tuy nhiên tất cả các phương pháp đo “khoảng cách” đều có đặc điểm chung. Giả sử x, y và z là các đối tượng của một loại nào đó và bất kỳ khái niệm về khoảng cách d nào cũng đều phải tuân thủ 4 tiên đề sau:

* 
*  sao cho x # y
* 
* 

Tất cả các phép đo khoảng cách đều phải tuân theo 4 tiên đề trên. ,  và kể cả công thức Pythagorean tổng quát . Chú ý rằng có hai loại đối tượng ở đây: một là các số (hoặc các thành phần) tạo nên A và B, hai là chính các vector 1-chiều A và B. Điều này dẫn đến các khái niệm khoảng cách khác nhau: khoảng cách giữa các số và khoảng cách giữa các vector 1-chiều. Thực tế là nếu d tuân theo các tiên đề về khoảng cách ở trên thì tổng  là khoảng cách giữa A và B. Đến đây chúng ta có thể từ bỏ công thức Pythagorean, thay vào đó chúng ta sẽ dùng  để nói về công thức đo khoảng cách giữa hai điểm A và B.



Hình 3.8. Khoảng cách giữa hai đối tượng dựa trên các thông số của chúng

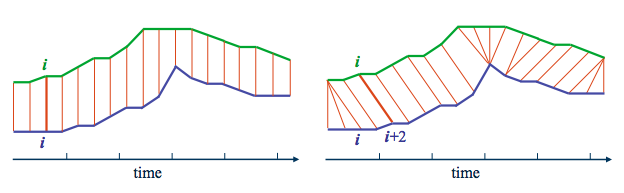
## Nhận dạng cử chỉ dựa trên kỹ thuật so khớp chuỗi thời gian động

### Giới thiệu

Vào năm 1983, **Joseph Kruskal** và **Mark Liberman** đã giới thiệu một kỹ thuật mới cho phép tìm ra đường chuẩn hoá tối ưu dựa trên việc so sánh hai mẫu dữ liệu được vector hoá đặc trưng bằng tính khoảng cách giữa chúng. Kỹ thuật này được gọi là **time warping**, có thể so khớp (**matching**) hai vector có đặc trưng khác nhau về thời gian và tốc độ. Ví dụ, có thể so sánh dựa vào dáng đi của một người đi chậm và người khác đi nhanh hơn hay thậm chí có sự tăng, giảm tốc độ quan sát đối tượng dọc đường đi. Một trong những đặc điểm của DTW rất hữu ích trong lĩnh vực nhận dạng là khả năng xử lý những mẫu dữ liệu có độ dài không bằng nhau (tức là mẫu dữ liệu có một số lượng các điểm toạ độ khác nhau). Điều này cho phép so sánh mà không cần phải lấy lại mẫu. Bởi việc lấy lại mẫu thường xoá bớt thông tin hay thêm thông tin sai (mẫu bao gồm nhiều điểm chứa đựng nhiều thông tin hơn những mẫu ít điểm, vì vậy việc lấy mẫu là không cần thiết), cho nên tốt hơn là không sử dụng.

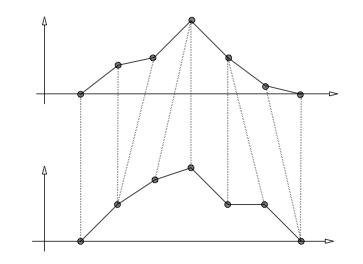
Ban đầu, **Kruskal** và **Liberman** đã đề nghị sử dụng kỹ thuật này trong nhận dạng giọng nói, bởi đặc điểm giọng nói là chuỗi tín hiệu biến thiên liên tục theo thời gian. Nhưng ngay này, kỹ thuật này được ứng dụng rộng rãi trong các lĩnh vực như nhận dạng dáng đi, nhận dạng cử chỉ, khai thác dữ liệu, xác thực chữ ký ...

Về mặt lý thuyết, Euclidean là phương pháp đo khoảng cách hiệu quả mà có thể được sử dụng trong thuật toán. Khoảng cách Euclidean giữa hai chuỗi dữ liệu theo thời gian chỉ đơn giả là tổng bình phương khoảng cách từ một điểm thứ ***i*** ở chuỗi thời gian này đến điểm thứ ***i*** ở chuỗi còn lại. Nhược điểm chính của việc sử dụng khoảng cách Euclidean cho hai chuỗi dữ liệu theo thời gian là kết quả của nó rất không trực quan. Nếu hai chuỗi thời gian giống hệt nhau, nhưng chỉ cần có một sự thay đổi hoặc sai lệch nào đó ở trục thời gian thì phương pháp đo Euclidean lại xem đó là hai chuỗi rất khác nhau. Như vậy việc sử dụng phương pháp đo khoảng cách Euclidean là không khả thi trong bài toán nhận dạng cử chỉ người.



Hình 3.1. So sánh hai phương pháp đo khoảng cách Euclidean và DTW

DTW có thể khắc phục được nhược điểm của phương pháp đo Euclidean và cho phép thực hiện các phép đo trực quan giữa hai chuỗi dữ liệu theo thời gian bằng cách bỏ qua cách thay đổi không cần thiết ở trục thời gian. Hình dưới đây cho ta thấy cách thức một chuỗi dữ liệu theo thời gian được “warp” với một chuỗi khác.



Hình 3.2. Cách thức “warp” các chuỗi dữ liệu trong DTW

Trong hình trên, mỗi đường thẳng nối một điểm trên chuỗi thời gian này với các điểm tương đồng trên chuỗi thời gian kia. Các đường có giá trị giống nhau trên trục y, nhưng đã được tách ra để các đường thẳng đứng giữa chúng có thể dễ dàng nhìn thấy. Nếu cả chuỗi thời gian trong hình giống hệt nhau thì tất cả các đường sẽ là thẳng đứng vì lúc này không cần phải dùng kỹ thuật “time warping” nữa. Khoảng cách đường “warp” là độ đo sự khác nhau giữa hai chuỗi thời gian sau khi được “warp” với nhau, được tính bằng tổng các khoảng cách giữa mỗi cặp điểm được nối với nhau bằng các đường thẳng đứng trong hình trên. Như vậy, hai chuỗi thời gian mà giống hệt nhau ngoại trừ việc kéo dãn cục bộ của các trục thời gian sẽ có khoảng cách DTW bằng 0.

### Phát biểu bài toán

Bài toán Dynamic Time Warping được phát biểu như sau: cho trước hai chuỗi dữ liệu theo thời gian X và Y. Chiều dài lần lượt của hai chuỗi là |X| và |Y|,





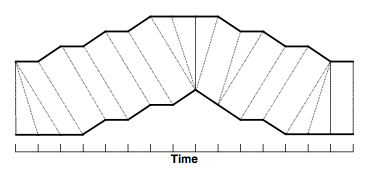
Gọi W là đường warp,

với K là độ dài của đường warp và phần tử thứ k của đường warp là:



với i là chỉ số của chuỗi X và j là chỉ số thuộc chuỗi Y. Đường warp phải bắt đầu ở vị trí đầu tiên của mỗi chuỗi dữ liệu tức là  và kết thúc tại điểm cuối cùng của cả hai chuỗi dữ liệu . Điều này đảm bảo rằng mọi chỉ số của các hai chuỗi dữ liệu đều được sử dụng trong đường warp. Cũng có ràng buộc đối với đường warp đó là i và j phải là đơn điệu tăng trên đường warp, điều này lý giải tại sao các đường thẳng biểu diễn đường warp trong hình 3.9 không bị chồng chéo lên nhau.



Hình 3.9. Đường warp giữa hai chuỗi

Mỗi chỉ số của mỗi chuỗi dữ liệu đều phải được sử dụng. Phát biểu một cách chính thức như sau:

Đường warp tối ưu là đường warp có tổng khoảng cách nhỏ nhất. Khoảng cách của đường warp W được tính theo công thức:

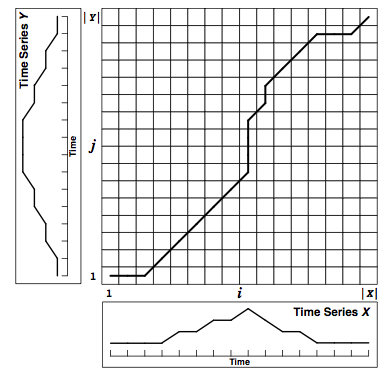


Trong đó là khoảng cách (thường được gọi là khoảng cách Euclidean) của đường warp W, và  là khoảng cách giữa hai điểm thứ i và j tương ứng (một từ X và một từ Y) thuộc thành phần thứ k của đường warp.

### Thuật toán

Cách tiếp cận tuân theo nguyên tắc của quy hoạch động được sử dụng để tìm khoảng cách nhỏ nhất của đường warp. Thay vì cố gắng giải quyết toàn bộ bài toán một lần, ta sẽ giải các bài toán con để xây dựng lời giải cho bài toán lớn hơn. Tiếp tục lặp lại như vậy cho đến khi ta tìm được lời giải cho toàn bộ bài toán.

Gọi D là ma trận chi phí hai chiều |X| x |Y|, D(i,j) là khoảng cách nhỏ nhất của đường warp có thể được tạo ra từ hai chuỗi:  và . Giá trị tại D(|X|, |Y|) chứa khoảng cách nhỏ nhất cuả đường warp giữa hai chuỗi X và Y. Cả hai trục của D đều đại diện cho trục thời gian. Với trục x là thời gian của chuỗi cử chỉ X, và trục y là thời gian của chuỗi cử chỉ Y. Hình sau đây đưa ra ví dụ minh họa một ma trận chi phí và đường warp có khoảng cách nhỏ nhất bắt đầu từ D(1,1) cho đến D(|X|, |Y|).



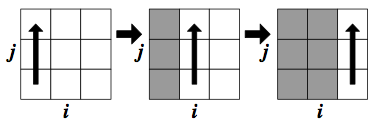
Hình 3.10. Ma trận trọng số và đường warp có khoảng cách nhỏ nhất

Ma trận trọng số và đường warp trong hình 3.10 chính là biểu diễn cho hai chuỗi cử chỉ ở hình 3.9. Đường warp là **W = {(1,1), (2,1), (3,1), (4,2), (5,3), (6,4), (7,5), (8,6), (9,7), (9,8), (9,9), (9,10), (10,11), (10,12), (11,13), (12,14), (13,15), (14,15), (15,15), (16,16)}**. Nếu đường warp đi qua một ô D(i,j) trong ma trận trọng số, thì có nghĩa là điểm thứ i của chuỗi cử chỉ X được warp với điểm thứ j của chuỗi cử chỉ Y. Chú ý là tại các đoạn thẳng đứng của đường warp thì một điểm trên chuỗi cử chỉ X được warp với nhiều điểm trên chuỗi cử chỉ Y và ngược lại cho những đoạn nằm ngang. Do một điểm có thể được ánh xạ đến nhiều điểm ở các vector khác, nên các chuỗi cử chỉ không nhất thiết phải có độ dài bằng nhau. Nếu X và Y là các vector giống hệt nhau thì đường warp trên ma trận chi phí sẽ là đường chéo thẳng.

Để tìm ra đường warp có khoảng cách nhỏ nhất thì tất cả các ô trên ma trận chi phí cần phải được điền giá trị. Ý tưởng chính của DTW đối với bài toán này là khi giá trị tại D(i,j) là khoảng cách warp nhỏ nhất của hai chuỗi cử chỉ có độ dài lần lượt là i và j, nếu các khoảng cách warp nhỏ nhất cho các chuỗi cử chỉ có độ dài kề với i và j đều đã được biết thì giá trị tại D(i,j) bằng khoảng cách nhỏ nhất cho tất cả các đường warp có thể xảy ra cho các chuỗi cử chỉ ma có độ dài nhỏ hơn i và j một đơn vị công với khoảng cách giữa hai điểm  và . Do đường warp có tính đơn điệu tăng, nên các khoảng cách cho các đường warp tối ưu ở trước đó một bước sẽ được lưu tại D(i-1,j), D(i,j-1) và D(i-1,j-1). Do vậy giá trị của một ô trong ma trận là:



Đường warp đến D(i,j) phải đi qua một trong 3 ô trên ma trận trọng số và do khoảng cách nhỏ nhất của đường warp có thể có cho từng ô đã được biết trước, tất cả chỉ đơn giả là cộng khoảng cách của hai điểm hiện tại với một giá trị nhỏ nhất trong 3 ô trước đó. Do công thức trên xác định giá trị của một ô trong ma trận chi phí bằng cách sử dụng các giá trị tại các ô khác nên thứ tự mà các ô được tính là rất quan trọng. Ma trận trọng số được điền theo cột từ dưới lên trên và từ trái sang phải giống như trong hình 3.11.



Hình 3.10. Thứ tự điền giá trị cho ma trận chi phí

Sau khi toàn bộ ma trận chi phí đã được điền giá trị, một đường warp phải được tìm thấy từ D(1,1) đến D(|X|, |Y|). Thực ra đường warp được tính theo trật tự ngược lại bắt đầu tại D(|X|, |Y|). Vị trí tiếp theo được đưa vào đường warp là vị trí có giá trị nhỏ nhất trong 3 ô đừng liền kế với ô hiện tại (ô bên trái, ô bên dưới theo chiều thẳng đứng và ô bên dưới theo đường chéo). Thực hiện lặp tương tự như vậy cho đến khi gặp ô D(1,1) và kết thúc việc tìm kiếm.

### Độ phức tạp của thuật toán

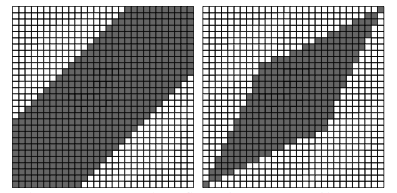
Khá dễ dàng để xác định độ phức tạp về không gian (Space) và thời gian (Time) của DTW. Mỗi ô trong ma trận trọng số |X| x |Y| được điền đúng một lần. Việc làm cho cả độ phức tạp về không gian và thời gian đều bằng |X| x |Y|, tức là bằng  nếu N = |X| = |Y|. Độ phức tạp về không gian mà bằng hàm số mũ là một điều cấm kỵ bởi vì bộ nhớ yêu cầu dung lượng terabyte cho các chuỗi thời gian chỉ chứa khoảng 177.000 phép đo. Rõ ràng chúng ta có thể thực thi thuật toán DTW với độ phức tạp về thời gian tuyến tính bởi vì chúng ta chỉ cần lưu giá trị của các cột hiện tại và cột trước đó trong bộ nhớ vì ma trận chi phí được điền từ trái sang phải (như hình 3.10). Với việc chỉ duy trì hai cột tại bất kỳ thời điểm nào, khoảng cách warp tối ưu giữa hai chuỗi cử chỉ vẫn có thể được xác định. Tuy nhiên, chúng ta không thể xây dựng lại đường warp giữa hai chuỗi đó bởi vì thông tin cần thiết để tìm đường warp đã bị mất ở những cột mà ta không lưu lại giá trị. Đây không phải là vấn đề nếu bài toán chỉ yêu cầu tính khoảng cách giữa hai chuỗi cử chỉ, nhưng với các ứng dụng cần tìm các vùng tương ứng giữa các chuỗi dữ liệu hoặc trộn các chuỗi dữ liệu lại với nhau thì đường warp cần phải được tìm ra.

### Các ràng buộc của thuật toán DTW

Độ phức tạp về thời gian và không gian theo hàm bậc hai của DTW đặt ra yêu cầu cần phải cải thiện tốc độ thực hiện của nó. Các phương pháp được sử dụng để làm cho DTW chạy nhanh hơn được chia làm 3 loại như sau:

* Các ràng buộc – Hạn chế số lượng ô cần tính toán trong ma trận chi phí.
* Trích rút dữ liệu – Thực thi DTW trên một đại diện đã được rút gọn của dữ liệu ban đầu.
* Đánh chỉ số - Sử dụng các đặc điểm của tiệm cận biên để giảm số lần DTW phải thực hiện trong quá chình phân lớp hoặc phân nhóm các chuỗi dữ liệu.

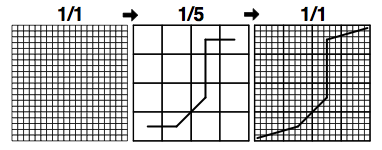
Các ràng buộc được sử dụng rộng rãi để tăng tốc độ cho DTW. Hai trong số các ràng buộc được sử dụng phổ biến nhất là Sakoe-Chuba Band and the Itakura Parallelogram được thể hiện trong hình 3.11.



Hình 3.11. Hai ràng buộc Sakoe-Chuba Band (bên trái) và Itakura Parallelogram (bên phải)

Các phần bóng mờ trong hình 3.11 là các ô của ma trận chi phí cần phải được điền giá trị bởi thuật toán DTW cho mỗi ràng buộc. Chiều rộng của mỗi phần bóng mờ hay còn gọi là cửa sổ (window) được xác định bởi một tham số. Khi các ràng buộc này được sử dụng, thuật toán DTW sẽ tìm đường warp tối ưu thông qua ràng buộc cửa sổ. Tuy nhiên, toàn bộ đường warp tối ưu sẽ không được tìm thấy nếu nó không nằm hoàn toàn bên trong cửa sổ. Việc sử dụng các ràng buộc để tăng tốc độ thực hiện của DTW bởi một hằng số. Nhưng thuật toán DTW vẫn có độ phức tạp  nếu kích thước đầu vào của cửa sổ bằng với chiều dài của chuỗi cử chỉ. Các ràng buộc hoạt động tốt trong các bài toán mà đường warp tối ưu dự kiến gần với đường warp tuyến tính và đi qua ma trận chi phí theo đường chéo và đi theo một đường tương đối thẳng. Các ràng buộc không thể hiện được thế mạnh của mình nếu các chuỗi dữ liệu là các sự kiện mà bắt đầu và dừng lại ở những thời điểm hoàn toàn khác nhau bởi vì khi đó đường warp có thể đi ra rất xa đường warp tuyến tính và gần như toàn bộ ma trận chi phí cần phải được tính để tìm ra đường warp tối ưu.

Phương pháp trích rút dữ liệu cải tiến thuật toán DTW bằng cách chạy DTW trên một đại diện rút gọn của dữ liệu ban đầu. Ở phía bên trái của hình 3.12 là một ma trận chi phí có kích thước đầy đủ mà một đừng warp tối ưu cần phải được tìm ra. Thay vì thực hiện thuật toán DTW trên ma trận chi phí đầy đủ (tỉ lệ 1/1), các chuỗi dữ liệu được rút gọn để làm cho số lượng các ô trong ma trận chi phí dễ dàng quản lý hơn. Đường warp được tìm thấy cho chuỗi dữ liệu rút gọn sẽ được ánh xạ trở lại ma trận chi phí đầy đủ kích thước.



Hình 3.12. Tăng tốc DTW bằng phương pháp trích rút dữ liệu

Kết quả là thuật toán DTW được tăng tốc đáng kể theo một hằng số, nhưng thuật toán vẫn có độ phức tạp về không gian và thời gian là . Rõ ràng, khoảng cách warp được tính giữa hai chuỗi cử chỉ ngày càng trở lên không chính xác và nó tỷ lệ thuận với việc gia tăng mức độ trích rút dữ liệu. Việc chiếu đường warp ở độ phân giải thấp lên ma trận chi phí đầy đủ độ phân giải sẽ tạo ra một đường warp ngày càng xa phương án tối ứu bởi vì ngay cả khi đường warp tối ưu thực sự đi qua các ô có độ phân giải thấp thì việc chiếu đường warp lên độ phân giải cao hơn bỏ qua các thay đổi cục bộ trong đường warp mà có thể rất chúng rất quan trọng.

Việc đánh chỉ số bằng cách sử dụng các tiệm cận để cắt bớt số lần DTW cần phải thực hiện cho một nhiệm vụ nào đó như phân nhóm một tập các chuỗi dữ liệu hoặc tìm ra các chuỗi dữ liệu giống với một chuỗi cho trước nhất. Việc đánh chỉ số tăng tốc độ đáng kể cho nhiều ứng dụng DTW bằng cách giảm bớt số lần DTW phải thực hiện, nhưng nó không làm tăng tốc độ của DTW về mặt bản chất.

Trong phần tiếp theo, chúng ta sẽ tìm hiểu về thuật toán **iDTW**, thuật toán này áp dụng ý tưởng của cả các ràng buộc và trích rút dữ liệu. Việc sử dụng kết hợp cả hai phương pháp giúp iDTW khắc phục được các hạn chế khi sử dụng từng phương pháp riêng rẽ và đạt được độ phức tạp thuật toán cả về không gian và thời gian là .

## Một số cải tiến kỹ thuật so khớp chuỗi thời gian động cho nhận dạng cử chỉ

Cách tiếp cận theo nhiều mức mà iDTW sử dụng được lấy ý tưởng từ cách tiếp cận nhiều mức được sử dụng trong bài toán đồ thị chia đôi. Đồ thị chia đội là nhiệm vụ chia đồ thị thành các phần bằng nhau sao cho tổng số cạnh bị phá vỡ càng nhỏ càng tốt. Thuật toán tỏ ra chính xác và hiệu quả với các đồ thị nhỏ, nhưng với các đồ thị lớn, các phương án tìm ra thường xa so với phương án tối ưu. Cách tiếp cận nhiều mức có thể được sử dụng để tìm ra phương án tối ưu cho đồ thị nhỏ, và sau đó liên tục mở rộng các đồ thị và khắc phục các phương án trước đó cho bài toán lớn hơn. Cách tiếp cận theo nhiều mức hoạt động tốt với các bài toán lớn khó có thể giải quyết toàn bộ bài toán cùng lúc, trong khi đó các phương án thành phần có thể được cải tiến một cách hiệu quả ở các kích thước khác nhau. Bài toán Dynamic Time Warping cũng có thể được giải quyết bằng cách áp dụng cách tiếp cận nhiều mức. Thuật toán iDTW áp dụng cách tiếp cận này và có khả năng tìm ra đường warp chính xác với độ phức tạp về thời gian và không gian là tuyến tính.

### Thuật toán iDTW

Thuật toán iDTW sử dụng phương pháp tiếp cận nhiều mức với ba thao tác chính như sau:

* **Làm thô** (Coarsening) - Co một chuỗi cử chỉ thành một chuỗi nhỏ hơn mà thể hiện được chính xác nhất có thể đường cong tương tự nhưng với ít điểm hơn.
* **Chiếu** (Projection) - Tìm đường warp có kích thước nhỏ nhất ở độ phân giải thấp và sử dụng đường warp này như một phương án giả định ban đầu cho độ phân giải cao hơn.
* **Cải tiến** (Refine) – Cải tiến đường warp được chiếu từ độ phân giải thấp thông qua một số điều chỉnh cục bộ của đường warp.

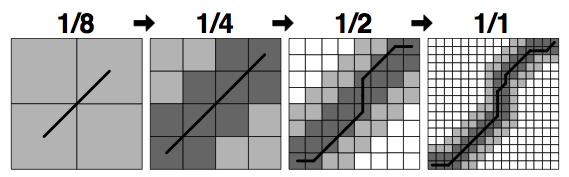
Việc làm thô làm giảm kích thước (hay còn gọi là độ phân giải) của chuỗi cử chỉ bằng lấy trung bình của cặp các điểm kề nhau. Chuỗi cử chỉ kết quả là một chuỗi mới bắng một nửa chuỗi ban đầu. Việc làm thô được thực hiện một vài lần để tạo ra chuỗi cử chỉ ở các độ phân giải khác nhau.

Thao tác chiếu sẽ sử dụng một đường warp đã được tìm ra ở độ phân giải thấp và xác định những ô nào trong chuỗi chử chỉ ở độ phân giải cao hơn mà đường warp sẽ đi qua. Do độ phân giải tăng theo hệ số 2, nên mỗi điểm trong đường warp ở độ phân giải thấp sẽ được chiếu tới ít nhất 4 điểm ở độ phân giải cao hơn (có thể lớn hơn 4 nếu |X| khác |Y|). Đường được chiếu sau đó sẽ được sử dụng như một phỏng đoán (**heuristic**) trong quá trình cải tiến phương án để tìm ra đường warp ở độ phân giải cao hơn.

Thao tác cải tiến được sử dụng để tìm ra đường warp tối ưu trong phạm vi lân cận của đường warp được chiếu, trong đó phạm vi lân cận được xác định bởi tham số bán kính (radius).

Thuật toán DTW chuẩn có độ phức tạp tính toán  bởi vì tất cả các ô trong ma trận chi phí phải được điền giá trị để đảm bảo một phương án tối ưu được tìm thấy, và kích thước của ma trận tăng theo bình phương kích thước của chuỗi cử chỉ. Với iDTW, ma trận chi phí chỉ được điền giá trị trong phạm vi lân cận với đường được chiếu từ độ phân giải trước đó. Vì chiều dài của đường warp tăng tuyến tính với kích thước của chuỗi cử chỉ đầu vào nên iDTW là một thuật toán .

Ban đầu, thuật toán iDTW sử dụng thao tác làm thô để tạo ra tất cả các độ phân giải sẽ được tính toán. Hình 3.13 minh họa 4 độ phân giải được tạo ra khi chạy thuật toán iDTW cho một chuỗi cử chỉ. Thuật toán DTW chuẩn được sử dụng để tìm đường warp tối ưu cho chuỗi cử chỉ ở độ phân giải thấp nhất. Đường warp cho độ phân giải thấp nhất được thể hiện ở phía bên trái của hình 3.13. Sau khi đường warp ở độ phân giải thấp nhất được tìm thấy, nó sẽ được chiếu lên độ phân giải thiếp theo. Trong hình 3.13, thao tác chiếu đường warp từ độ phân giải 1/8 được thể hiện bởi các ô bóng mờ trên độ phân giải 1/4.



Hình 3.13. Bốn độ phân giải khác nhau được đánh giá trong thuật toán iDTW

Để cái tiến đường chiếu, thuật toán DTW hạn chế được chạy với ràng buộc cụ thể là chỉ có các ô thuộc đường warp được chiếu mới được đánh giá. Điều này có nghĩa là thuật toán sẽ tìm đường warp tối ưu trong phạm vi đường warp đã được chiếu từ độ phân giải thấp. Tuy nhiên toàn bộ đường warp tối ưu có thể nằm trong phạm vi chiếu. Để tăng cơ hội tìm được phương án tối ưu, người ta sử dụng tham số bán kinh để điều khiển số lượng ô được thêm vào mỗi phía của đường được chiếu, những ô thêm vào này sẽ được đánh giá trong quá trình cái tiến đường warp. Trong hình 3.13, bán kính được thiết lập bằng 1. Khi đường warp được cải tiến ở độ phân giải 1/4, nó sẽ được chiếu lên độ phân giải ½, được mở rộng theo bán kính bằng 1 và tiếp tục được cái tiến. Cuối cùng đường warp được chiếu lên một độ phân giải đầy đủ 1/1. Thao tác chiếu được mở rộng bởi tham số bán kính và được cải tiến lần cuối cùng. Đường warp sau khi được cải tiến sẽ là kết quả đầu ra của thuật toán.

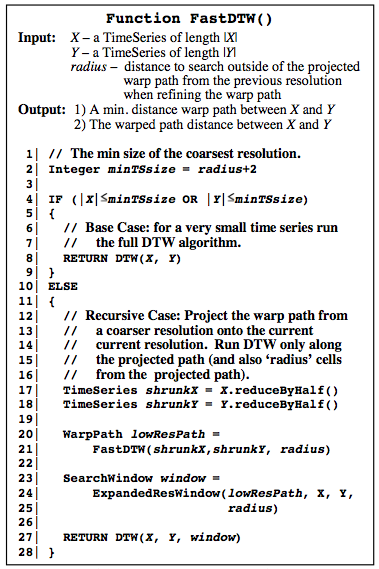
Chú ý là đường warp được tìm ra bởi thuật toán iDTW trong hình 3.13 chính là đường warp tối ưu được tìm ra bởi thuật toán DTW chuẩn trong hình 3.10. Tuy nhiên, iDTW chỉ tính toán trên những ô đánh dấu mờ, trong khi DTW phải tính toán cho tất cả các ô trong ma trận trọng số. Ví dụ đối với chuỗi cử chỉ có độ dài 16, iDTW cần tính toán trên 4 + 16 + 44 + 100 = 166 ô cho tất cả các độ phân giải, trong khi đó DTW cần tính toán cho tất cả 235 (162­­­­­­) ô. Sự gia tăng hiệu năng này không quá quan trọng đối với những bài toán nhỏ, đặc biệt khi tính đến chi phí của việc tạo ra tất cả độ phân giải. Tuy nhiên, số lượng ô mà iDTW cần phải tính toán tăng tuyến tính theo độ dài của chuỗi cử chỉ, trong khi đó DTW luôn tăng theo bình phương của chiều dài chuỗi cử chỉ. iDTW tăng tuyến tính vì độ rộng của đường đi qua ma trận trọng số là hằng số cho tất cả các độ phân giải.

Ví dụ trong hình 3.13 tìm được đường warp tối ưu, nhưng thuật toán iDTW không đảm bảo luôn tìm được đường warp mà nó là tối ưu. Tuy nhiên, đường warp được tìm thấy thường rất gần với phương án tối ưu. Giá trị của tham số bán kính càng lớn thì đường warp tìm được càng chính xác. Nếu giá trị của bán kính bằng kích thước của chuỗi cử chỉ đầu vào thì iDTW lại giống với DTW chuẩn, luôn tìm được phương án tối ưu nhưng độ phức tạp là .

Giả code cho thuật toán iDTW được thể hiện trong hình 3.14. Đầu vào của thuật toán là hai chuỗi cử chỉ và giá trị của tham số bán kính. Đầu ra của iDTW là đường warp và khoảng cách giữa hai chuỗi cử chỉ theo đường warp đó. Dòng thứ 2 xác định độ dài nhỏ nhất của một chuỗi cử chỉ tại độ phân giải thấp nhất. Kích thước này phụ thuộc vào tham số bán kính và nó xác định kích thước của độ phân giải nhỏ nhất có thể.

iDTW thực hiện theo cơ chế đệ quy. Trường hợp cơ bản là khi một trong các chuỗi cử chỉ đầu vào có độ dài nhỏ hơn hoặc bằng **minTSsize**. Với trường hợp này, thuật toán chỉ đơn giản là trả lại kết quả của thuật toán DTW chuẩn. Trường hợp đệ quy có 3 bước chính:

* Đầu tiên, hai chuỗi cử chỉ mới ở độ phân giải thấp hơn được tạo ra. Chúng cố số điểm bằng một nữa số điểm của chuỗi ban đầu. Đây chính là thao tác làm thô (**coarsening**). Bước này được thực hiện bởi các dòng 17 và 18 trong hình 3.14.
* Tiếp theo, đường đi ở độ phân giải thấp được tìm thấy cho chuỗi cử chỉ đã được làm thô và đường này được chiếu lên độ phân giải cao hơn (các dòng từ 23-25). Đường warp dự kiến cũng được mở rộng bởi các ô nằm trong bán kính cho phép. Bán kính này sẽ tạo ra một không gian tìm kiếm (**search window**) đóng vai trò như một ràng buộc đối với thuật toán DTW chuẩn – chỉ tính toán trên những ô thuộc không gian tìm kiếm.
* Thuật toán DTW chuẩn với rằng buộc về không gian tìm kiếm tiến hành tinh chỉnh đường warp được chiếu từ độ phân giải thấp. Kết quả sau khi được tinh chỉnh sẽ được trả lại.



Hình 3.14. Thuật toán iDTW

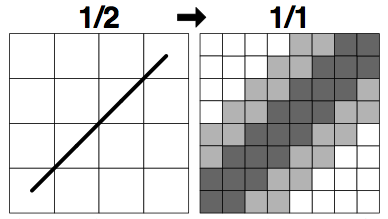
Việc thực hiện thuật toán iDTW chạy lặp lại liên tục các dòng 17-18 trong các lời gọi đệ quy để các độ phân giải thấp hơn được tạo ra bởi dòng 21. Việc tạo ra nhiều độ phân giải này được thực hiện cho đến khi đạt được trường hợp cơ sở (độ phân giải nhỏ hơn hoặc bằng **minTSsize**). Trường hợp cơ sở chỉ được thực hiện duy nhất một lần và sau đó các dòng 23-27 được thực hiện một lần cho mỗi lời gọi đệ quy.

Tiếp theo chúng ta sẽ phân tích độ phức tạp về thời gian và không gian của thuật toán iDTW.

### Độ phức tạp về thời gian

Để đơn giản hóa cho việc tính toán, cả hai chuỗi cử chỉ đầu **X** và **Y** vào đều có độ dài bằng nhau và bằng **N**. Tất cả các phân tích sẽ được thực hiện dựa trên trường hợp xấu nhất.

Số lượng ô trong ma trận chi phí được điền giá trị bởi iDTW ở một độ phân giải bằng với số lượng ô nằm trong đường warp được chiếu cộng thêm các ô khác nằm trong bán kính cho phép (ký hiệu là **r**) với đường warp. Trường hợp xấu nhất, đường warp được chiếu là một đường thẳng chạy chéo qua ma trận chi phí như trong hình 3.15.



Hình 3.15. Số lượng ô lớn nhất cần được tính với bán kính bằng 1

Số lượng ô mờ nhạt trong hình 3.15 là **2Nr** ô cho mỗi bên của đường chiếu. Đường chiếu được thể hiện bởi các ô mờ đậm, có tất cả **3N** ô. Do vậy đường chiếu có số lượng tối đa các ô ở một độ phân giải với hai chuỗi cử chỉ có độ dài N như sau:

 [1]

Độ dài của mỗi chuỗi cử chỉ tại mỗi độ phân giải (**res**) tuân theo dãy sau (**N** điểm được chứa trong chuỗi cử chỉ ban đầu):

 [2]

Do đó, số lượng ô cần được tính ở tất cả các độ phận giải là (kết hợp phương trình 1 và 2):

 [3]

Dãy trong phương trình 3 tương đương với dãy sau:

 [4]

Nhân vế với vế hai phương trình 1 và 4 ta được:

 [5]

Do dãy ở phương trình 5 tương tự với dãy ở phương trình 3, nên số lượng ô được tính toán ở tất cả các độ phân giải là:

**Tổng số ô được điền giá trị = ** [6]

Ngoài số lượng ô cần được tính toán, cũng có độ phức tạp về thời gian cho việc tạo ra các độ phân giải và xác định đường warp bằng cách theo viết trên ma trận.

Độ phức tạp thời gian cần thiết để tạo ra các độ phân giải tỷ lệ thuận với số lượng điểm trong tất cả các độ phân giải, nó chính là dãy ở phương trình 2. Đáp án của phương trình 2 thu được bằng cách nhân các vế của phương trình 4 với N, và kết quả là 2N. Do có nhiều độ phân giải được tạo ra cho cả hai chuỗi cử chỉ nê:

**Thời gian để tạo ra tất cả các độ phận giải = 4N** [7]

Độ phức tạp về thời gian cần để xác định lại đường warp thông qua ma trận chi phí được đo bởi độ dài của đường warp. Nếu độ phân giải có chứa N điểm, thì đường warp có độ dài 2N trong trường hợp xấu nhất (trường hợp tốt nhất có độ dài bằng N với đưởng warp là đường chéo qua ma trận chi phí). Nhân phương trình 4 với 2N ta sẽ được chiều dài của tất cả các đường warp trong trường hợp xấu nhất:

**Thời gian để xác định đường warp = 4N** [8]

Cộng các phương trình [6], [7] và [8] ta được tổng độ phức tạp thời gian trong trường hợp xấu nhất của iDTW bằng:

**Độ phức tạp về thời gian của iDTW = N(8r + 14)** [9]

Nó bằng  nếu giá trị của bán kính là một hằng số nhỏ (<N).

### Độ phức tạp về không gian

Độ phức tạp về không gian của iDTW bao gồm không gian cần thiết để lưu tất cả các độ phân giải (ngoại trừ độ phân giải đầy đủ của chuỗi cử chỉ truyền vào), tổng số lượng lớn nhất các ô được sử dụng vào một thời điểm bất kỳ trong ma trận chi phí và kích thước của đường warp được lưu trong bộ nhớ.

Độ phức tạp về không gian cho việc lưu trữ tất cả các độ phân giải phát sinh không kể để độ phân giải đầy đủ do các chuỗi cử chỉ truyền vào chính bằng phương trình 2 nhưng loại bỏ phần tử đầu tiên **2N – N = N**. Cho cả hai chuỗi cử chỉ đầu vào thì:

**Không gian cho các độ phân giải (bao gồm độ phân giải đầy đủ) = 2N** [10]

Độ phức tạp về không gian cho ma trận chi phí là kích thước lớn nhất của ma trận chi phí được tạo ra cho ma trận ở độ phân giải đầy đủ. Số lượng ô trong ma trận là phương trình 1:

**Không gian cho ma trận chi phí = N(4r + 3)** [11]

Độ phức tạp về không gian để lưu trữ đường warp bằng với đường warp dài nhất có thể có cho độ phân giải đầy đủ. Nếu đường warp đi theo chu vi của ma trận, thì chiều dài sẽ là:

**Không gian để lưu trữ đường warp = 2N** [12]

Cộng các phương trình 10, 11 và 12 độ phức tạp về không gian trong trường hợp xấu nhất.

**Độ phức tạp về không gian của iDTW = N(4r + 7)** [13]

Nó cũng bằng  nếu giá trị của bán kính là hằng số nhỏ (<N).

## Xác thực bằng nhận dạng cử chỉ

Các nghiên cứu trước đây đã chỉ ra rằng xác thực dựa trên cử chỉ với các cử chỉ tay và các bộ cảm biến gia tốc là khả thi. Xác thực dựa trên cử chỉ tỏ ra đầy hứa hẹn các thiết bị di động, bởi vì các khả năng về giao diện sử dụng bị giới hạn. Các cử chỉ tay là các đặc điểm sinh trắc của từng người và có một số đặc điểm đầy hứa hẹn. Người dùng thực sự/chính hãng không nhất thiết phải nhớ một mã bí mật. Thay vào đó, anh ta huấn luyện một cử chỉ và nó sẽ được lưu một cách ngầm định trên vỏ não. Do đó, bằng chứng xác thực không thể được chuyển qua cho người khác một cách dễ dàng. Xác thực dựa trên cử chỉ có thể là một lựa chọn hữu ích thay thế cho các cơ chế xác thực dựa trên tri thức cho các thiết bị di động.

Để có được đánh giá bước đầu cho cơ chế xác thực dựa trên cử chỉ, có 4 câu hỏi được xem là quan trọng cần được nghiên cứu một cách chi tiết:

1. Các đặc trưng về sinh trắc học của mỗi người liệu có đủ để tiến hành xác thực?
2. Cơ chế xác thực dựa trên cử chỉ yêu cầu những gì từ các người dùng tiềm năng?
3. Làm thế nào có thể sử dụng cơ chế xác thực dựa trên cử chỉ đừng từ quan điểm của người sử dụng?
4. Các thể loại tấn công có thể và thực sự đối với cơ chế xác thực này?

Những câu hỏi này đã được sử dụng như những hướng dẫn trong luận văn này. Câu hỏi 1 là về tính khả thi. Các gợi ý cho câu hỏi này đã được đưa ra bởi nghiên cứu trước đây về xác thực người dùng dựa trên cử chỉ người bằng việc sử dụng các bộ cảm biến gia tốc được trình bầy ở phần 2.3.4. Luận văn này nhằm mục đích chứng minh xác thực dựa trên cử chỉ người là khả thi trên các thiết bị di động bằng việc sử dung các bộ cảm biến gia tốc tích hợp sẵn. Trước khi thảo luận chi tiết về câu hỏi 2 và câu hỏi 3, các yêu cầu cho cơ chế xác thực trên thiết bị di động cần được phân tích. Điều này rất quan trọng vì quan điểm người dùng có thể phát hiện ra các yêu cầu, có thể là không nhìn thấy trực tiếp nhưng nó rất liên quan. Sau đó, cơ chế xác thực dựa trên cử chỉ người sẽ được trình bầy trong luận văn này. Phần này cũng trả lời câu hỏi 2 và câu hỏi 3. Đến cuối chương này, chúng ta sẽ thảo luận về các cuộc tấn công tiềm năng.

### Các yêu cầu đối với cơ chế xác thực người dùng trên thiết bị di động

Khả năng sử dụng của một cơ chế bảo mật có thể hoặc là làm nên hoặc phá hỏng hệ thống bảo mật. Do đó, sẽ là không đủ nếu chỉ phân tích các yêu cầu dựa trên quan điểm bảo mật mà bỏ qua quan điểm về khả năng sử dụng. Để nghiên cứu kỹ hơn cần phải tập trung vào người sử dụng như là xác định người sử dụng chính và các trường hợp sử dụng chính của họ. Tuy nhiên điều này gần như là không thể cho các thiết bị di động vì chúng được sử dụng bởi tất cả mọi người và trong hầu hết các trường hợp. Trong phần tiếp theo, các yêu cầu xuất phát từ các đặc trưng của thiết bị di động được giới thiệu, chúng rất quan trọng với khả năng sử dụng của các cơ chế xác thực trên thiết bị loại này.

Các thiết bị di động có khả năng di chuyển và có thể được sử dụng trong hầu hết các trường hợp. Điều này ám chỉ rằng việc sử dụng các thiết bị di động không bị hạn chế bởi địa điểm và thời gian. Để có sự tương tác hữu ích cần phải có khả năng sử dụng các thiết bị di động ở các địa điểm công cộng và cả những nơi không biết. Đặc biệt là những nơi công cộng có thể được xem là không an toàn, bởi vì có những người khác ở xunh quanh. Một cơ chế xác thực người dùng trên thiết bị di động hữu ích và được sử dụng rộng rãi không nên tạo ra bất cứ giả định và yêu cầu nào về vị trí tiến hành xác thực. Một cơ chế xác thực cũng không nên đòi hỏi các hành động của người dùng. Mỗi hành động phải hoàn toàn phù hợp với người sử dụng.

Từ quan điểm sử dụng, một cơ chế xác thực cần phải nhanh và dễ dàng sử dụng. Khi người sử dụng bắt đầu tương tác với thiết bị, mục đích của anh ta. Mục tiêu của anh ta không phải là để chứng minh danh tính của mình với điện thoại. Một cơ chế cần đủ rời rạc để nó có thể chấp nhận sự gián đoạn trước khi tương tác dự định có thể xảy ra. Hơn thế nữa, một cơ chế xác thực nên được thiết kế theo cách mà các hạn chế và khả năng về giao diện người dùng cần được xem xét. Nếu không, quá trình xác thực có thể gây phiền nhiễu và mệt mỏi cho người dùng. Một cơ chế xác thực cũng không nên đòi hỏi sự tập trung hoàn toàn trong quá trình xác thực, bởi vì trong một số trường hợp là không thể. Ngoài ra, việc xác thực cũng có thể xảy ra trong khi người dùng đang di chuyển. Ví dụ một người dùng có thể tiến hành việc xác thực trong khi đang đi bộ.

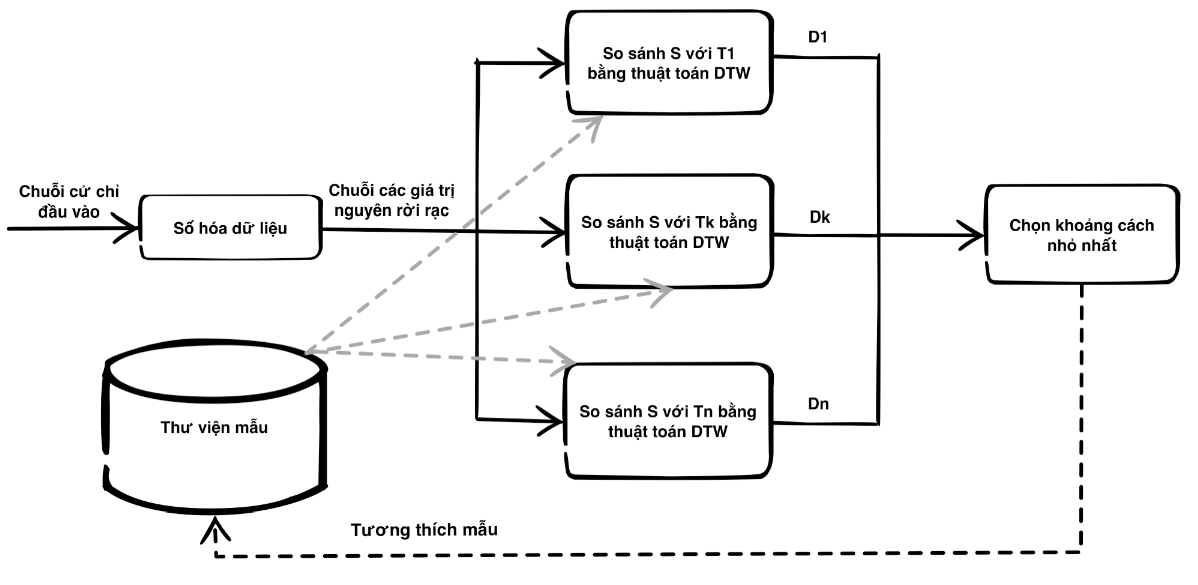
Một hạn chế khác xuất hiện bởi giới hạn về thời gian sử dụng pin. Một cơ chế xác thực có thể được sử dụng rất thường xuyên và nên tiêu thụ năng lượng ở mức tối thiểu cho mỗi lần xác thực. Nếu không, việc sử dụng cơ chế xác thực sẽ làm giảm thời gian sử dụng thiết bị và do đó có thể gây phiền toái cho người sử dụng.

Từ quan điểm người sử dụng một cơ chế xác thực cần phải đáng tin cậy. Một người sử dụng sẽ chỉ sử dụng một cơ chế nếu quá trình xác minh chập nhật các bằng chứng của anh ta một cách đáng tin cậy. Ngoài ra, đứng từ quan điểm bảo mật, một cơ chế bảo mật cũng cần phải đáng tin cậy nhưng theo một cách khác. Quan điểm bảo mật đòi hỏi cơ chế đó phải từ chối truy cập nếu gặp phải một bằng chứng sai. Tuy nhiên, người dùng chỉ có thể nhận thức được ý nghĩa đầu tiên về độ tin cậy và bỏ qua các khía cạnh bảo mật và ý nghĩa của nó. Việc chấp nhận những thứ không đáng tin cậy, ví dụ như từ chối các bằng chứng hợp lệ có thể gia tăng nếu người dùng biết và hiểu các khái niệm của cơ chế xác thực người dùng trong cách sử dụng. Đây là một vấn đề tổ chức và không liên quan trực tiếp đến cơ chế và các thiết bị di động, nhưng quan trọng đối với việc chấp nhận người sử dụng đặc biết là phương pháp tiếp cận sáng tạo đối với xác thực người dùng.

### Thuật toán xác thực

Trong phần này chúng ta sẽ tìm hiểu về cách thức tích hợp thuật toán DTW vào bài toán nhận dạng cử chỉ người để tạo ra một thuật toán nhận dạng cử chỉ người trên các thiết bị di động. Tiền đề của thuật toán này đó là các cử chỉ người có thể được đặc trưng bởi chuỗi các lực tác động theo thời gian lên thiết bị cầm tay – hay còn gọi là các chuỗi cử chỉ. Do đó, thuật toán này hoạt động dựa trên nhận dạng sự tương đồng của các chuỗi cử chỉ được đo bởi một bộ cảm biến gia tốc 3-chiều.

Để phục vụ cho quán trình nhận dạng, chúng ta sẽ tạo ra một thư viện mẫu cử chỉ để lưu trữ một hoặc nhiều cử chỉ đã được nhận dạng cho từng cử chỉ cơ bản. Các mẫu này thường được nhập vào bởi người sử dụng. Hình 3.16 mô tả quá trình nhận dạng. Đầu vào của thuật toán là một chuỗi dữ liệu cảm biến gia tốc 3-chiều. Về mặt toán học nó là một vector gồm 3 thành phần tương ứng với gia tốc trên 3 trục.



Hình 3.16. Thuật toán nhận dạng cử chỉ

Trước tiên, thuật toán nhận dạng cử chỉ người sẽ số hóa dữ liệu cảm biến gia tốc thành một chuỗi các giá trị rời rạc. Quá trình này cũng được áp dụng cho các mẫu. Tiếp theo nó sử dụng thuật toán DTW để đo sự tương đồng giữa chuỗi dữ liệu đầu vào với các mẫu cử chỉ. Thuật toán sẽ nhận ra cử chỉ dựa trên mẫu có sự tương đồng cao nhất. Kết quả nhận dạng sẽ được xác nhận bởi người dùng là đúng hay sai, và có thể được sử dụng để chỉnh sửa các mẫu hiện có và cập nhật những thay đổi của cử chỉ theo thời gian.

Thuật toán nhận dạng cử chỉ người bao gồm 3 phần chính: số hóa dữ liệu đầu vào, sử dụng thuật toán DTW để đo sự tương đổng giữa hai chuỗi cử chỉ và tương thích mẫu. Trong đó có thể nói DTW là thành phần cốt lõi của thuật toán nhận dạng cử chỉ. Trong phần tiếp theo chúng ta sẽ đi tìm hiểu về chức năng và nhiệm vụ của từng phần trong thuật toán nhận dạng cử chỉ. Do các nội dung về thuật toán DTW đã được trình bầy chi tiết trong phần 3.3. Giải thuật nên chúng ta sẽ không đề cập đến trong phần này nữa.

#### Số hóa dữ liệu gia tốc

Thuật toán tiến hành số hóa dữ liệu cảm biến gia tốc trước khi tiến hành việc nhận dạng. Thao tác này sẽ tiến hành giảm bớt kích thước của chuỗi dữ liệu đầu vào cho thuật toán DTW để nâng cao hiệu năng tính toán. Nó cũng chuyển các số đo cảm biến gia tốc thành các giá trị nguyên rời rạc để giảm bớt việc tính toán trên số thực. Đây có thể được coi như quá trình làm mịn dữ liệu đầu vào để nâng cao độ chính xác của việc nhận dạng bằng cách loại bỏ các thay đổi không thuộc về đặc trưng của cử chỉ như nhiễu gia tốc, nghiêng hoặc rung tay.

Quá trình này bao gồm 2 bước. Ở bước thứ nhất, chuỗi dữ liệu cảm biến được nén lại theo giá trị trung bình của mỗi 50ms và di chuyển theo bước 30ms. Cụ thể là, điểm dữ liệu đầu tiên là giá trị trung bình của gia tốc được tạo ra trong 50ms đầu tiên, điểm thứ hai là là giá trị trung bình được tạo ra trong khoảng từ 30ms đến 80ms, điểm thứ 3 là giá trị trung bình trong khoảng 60ms đến 110ms, và cứ tiếp tục như vậy cho đến hết. Điều này làm giảm bớt độ dài của chuỗi dữ liệu đầu vào cho DTW. Không những thế, lý do đằng sau còn là bản thân gia tốc sinh ra bởi các di chuyển bằng tay không thay đổi một cách bất thường và các thay đổi về gia tốc thường do nhiễu, rung tay hoặc nghiêng tay. Ở bước thứ hai, dữ liệu cảm biến được chuyển thành 1 trong 33 mức giá trị, được tổng hợp ở bảng 3.1. Việc số hóa phi tuyến tính này được áp dụng bởi vì chúng ta nhận ra rằng hầu hết các mẫu nằm trong khoảng từ -g đến +g và rất ít giá trị vượt quá +2g hoặc nhỏ hơn -2g.

Bảng 3.1. Bảng giá trị chuyển đổi cho dữ liệu cảm biến

|  |  |
| --- | --- |
| **Dữ liệu cảm biến (a)** | **Giá trị chuyển đổi** |
| a > 2g | 16 |
| g < a < 2g | 11 đến15 |
| 0 < a < g | 1 đến 10 |
| a = 0 | 0 |
| -g < a < 0 | -1 đến -10 |
| -2g < a < -g | -15 đến -11 |
| a < -2g | -16 |

#### Tương thích mẫu

Như chúng ta sẽ thấy trong phần đánh giá, có sự khác biệt đáng kể giữa các mẫu cử chỉ được thực hiện bởi cùng một người nhưng ở những ngày khác nhau. Lý tưởng là thuật toán nhận dạng phải có cơ chế tương thích mẫu để có thể điều tiết các thay đổi theo thời gian. Tương thích mẫu của thuật toán DTW cho giọng nói đã được nghiên cứu rất nhiều và đã chứng minh được tính hiệu quả. Tuy nhiên, trong luận văn này chúng ta chỉ đưa ra hai phương án đơn giản để tương thích mẫu. Bởi vì mục tiêu của chúng ta không phải là tìm ra các phương pháp tương thích mẫu hiệu quả nhất mà chỉ là chứng minh tương thích mẫu có thể được thực hiện một cách dễ dàng và rất hiệu quả trong việc cải thiện độ chính xác qua nhiều ngày.

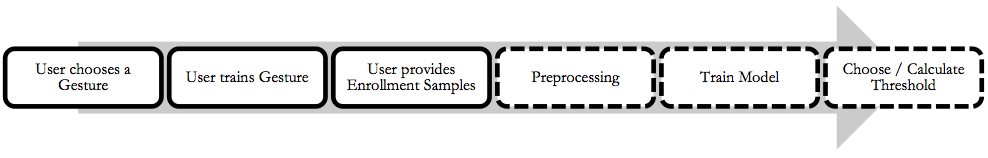
Quá trình tương thích mẫu hoạt động như sau, thuật toán nhận dạng cử chỉ lưu hai mẫu được tạo ra ở hai ngày khác nhau cho từng cử chỉ. Nó so sánh tính tương đồng của cử chỉ đầu vào với cả hai mẫu và lấy chi phí tương đồng nhỏ hơn làm chi phí tương đồng giữa cử chỉ đầu vào và cử chỉ mẫu.

Mỗi mẫu đều có mốc thời gian – timestamp – khi nó được tạo ra, vào ngày đầu tiên chỉ có một mẫu cho từng cử chỉ. Khi người dùng nhập vào nhiều mẫu cử chỉ, thuật toán sẽ cập nhật các mẫu dựa trên tiêu chí thời gian tồn tại của các mẫu hiện tại và mức độ khớp nhau của các mẫu với các chuỗi cử chỉ đầu vào mới. Chúng ta phát triển hai phương pháp cập nhật mẫu đơn giản. Ở phương pháp đầu tiên, nếu cả hai mẫu cho một cử chỉ trong thư viện tồn tại từ một ngày trở lên và cử chỉ đầu vào được nhận dạng chính xác, thì mẫu có thời gian tồn tại lâu hơn sẽ được thay thế bởi cử chỉ đầu vào mới được công nhận. Chúng ta gọi phương pháp này là cập nhật tích cực (**Positive Update**). Phương pháp thứ hai chỉ khác phương pháp thứ nhất đó là chúng ta thay thế mẫu có thời gian tồn tại lâu hơn bởi cử chỉ đầu vào khi nó không được nhận dạng chính xác. Chúng ta gọi phương pháp này là cập nhật tiêu cực (**Negative Update**). Cập nhật tích cực chỉ yêu cầu người dùng thông báo quá trình nhận dạng không thành công. Cập nhật tiêu cực yêu cầu người dùng chỉ ra cử chỉ đúng cử chỉ khi có lỗi xảy ra trong quá trình nhận dạng, ví dụ bằng cách nhấn một nút tương ứng để xác định một mẫu đầu vào.

### Quá trình đăng ký và xác thực

Quá trình đăng ký của một cơ chế xác thực dựa trên cử chỉ bao gồm 6 bước như trong hình 2.2.

* Đầu tiên, người dùng chọn một cử chỉ mà anh ta muốn sử dụng nó để tiến hành xác thực. Người sử dụng có thể hoặc là chọn cử chỉ của riêng mình hoặc chọn một kiểu cử chỉ nào đó đã được chuẩn bị trước.
* Sau đó anh ta sẽ huấn luyện cử chỉ của mình cho đến khi anh ta có khả năng lặp lại cử chỉ đó đủ giống.
* Ở bước thứ 3, người dùng cung cấp đủ số lượng các mẫu đăng ký chính hãng. Các mẫu này được ký hiệu bởi chữ T.
* Quá trình tiền xử lý các mẫu thô sẽ được mô tả trong phần 6.2 và sau đó các mẫu này sẽ được sử dụng để tạo ra một mô hình.
* Sau đó, mô hình sẽ được sử dụng để tính sự giống nhau của một mẫu chưa xác định bằng việc sử dụng các đặc trưng đã học được từ các mẫu đăng ký.
* Ở bước cuối cùng, ngưỡng chấp nhận được lựa chọn hoặc tính toán. Ngưỡng này sẽ xác định cận dưới của sự tương đồng. Để các mẫu chưa xác định được chấp nhận là chính hãng thì quá trình nhận dạng cần phải đạt được cận này. Ngưỡng này có thể được chọn theo mức độ ưu tiên hoặc được tính bằng cách sử dụng các mẫu ghi danh. Các quá trình tiền xử lý các mẫu, huấn luyện mô hình và tính toán ngưỡng được thực hiện tự động bằng cơ chế mà không cần tương tác người dùng.



Hình 2.2. Thủ tục đăng ký của cơ chế xác thực dựa trên cử chỉ

Trong quá trình xác thực, mô hình đã được huấn luyện và ngưỡng chấp nhận được sử dụng để quyết định xem mẫu hiện tại có phải là chính hãng hay không. Một mẫu chưa xác định được chấp nhận nếu hàm chấp nhận (Acceptance Function) G trả lại true. Hàm này kết hợp kết quả của hàm chấp nhận mô hình (Model Acceptance Function) M và ràng buộc về độ dài (Length Constraint).

### Tiền xử lý

Trước khi giới thiệu chi tiết về hai thuật toán, trước tiên chúng ta cần tìm hiểu về quá trình tiền xử lý. DTW và HMM yêu cầu tần suất lấy mẫu là không đổi, có nghĩa là sự chênh lệch về thời gian của hai phép đo liên tiếp là bằng nhau cho một trình tự hoàn chỉnh. Hơn nữa, nó cũng yêu cầu tất cả các mẫu phải có tần số lấy mẫu như nhau. Ở lần đánh giá đầu tiên của các phép đo được ghi lại, chúng ta phát hiện ra tần số khác nhau.

Để khắc phục vấn đề này, nội suy tuyến tính được áp dụng để chuẩn hóa tần số lấy mẫu. Công thức nội suy tuyến tính được thể hiện trong công thức (1). Với mỗi mốc thời gian ***t*** mà phép đo  sẽ tồn tại,  được xấp xỉ hóa bằng việc sử dụng tiền tố  và hậu tố  . Mốc thời gian của tiến tố được ký hiệu là  và của hậu tố là :

 (1)

Việc làm mịn các số đo đối với việc nhận dạng cử chỉ bằng việc sử dụng các bộ cảm biến gia tốc tỏ ra rất hiệu quả. Thật vậy, thuật toán HMM đã cho thấy rằng việc làm mịn giúp cải thiện hiệu suất của một mô hình. Tất cả các mẫu được làm mịn cho thuật toán HMM bằng việc sử dụng thuật toán **Simple Moving Average**. Thuật toán này tính toán giá trị của điểm hiện tại bằng cách tính giá trị trung bình của ***n*** điểm cuối cùng bao gồm cả điểm hiện tại.

# – THỬ NGHIỆM VÀ ĐÁNH GIÁ

Giới thiệu chương: Chương này sẽ trình bầy về thực nghiệm và đánh giá phương pháp nhận dạng cử chỉ và xác thực đã đề xuất trong chương 2. Nội dung chương 3 được cấu trúc theo các mục sau:

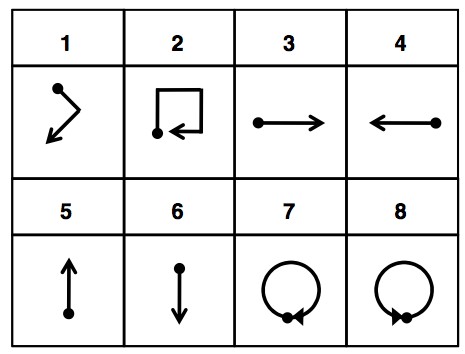
* Thu thập dữ liệu.
* Kết quả thực nghiệm
* Phân tích và đánh giá.
* Các kết luận.

## Thu thập dữ liệu

Để đánh giá phương pháp nhận dạng cử chỉ người và áp dụng nó để xây dựng một cơ chế bảo mật trên các thiết bị di động, chúng ta sử dụng hai tập dữ liệu. Tập dữ liệu đầu tiên bao gồm các cử chỉ cơ bản và tập dữ liệu thứ hai bao gồm các chữ ký của người sử dụng.

### Tập các cử chỉ cơ bản

Tập các cử chỉ cơ bản bao gồm 8 cử chỉ đơn giản được thực hiện bởi Nokia - Phần Lan. Những cử chỉ này được xem là được ưa thích bởi người sử dụng khi tương tác với các thiết bị. Hình 3.1 thể hiện các cử chỉ là các đường di chuyển bằng tay.



Hình 3.1. Các dữ liệu mẫu được tập hợp bởi VTT

Các cử chỉ được tập hợp từ 8 người với bộ điều kiển từ xa Wii. Hai trong số họ là sinh viên đại học và số còn lại đã tốt nghiệp. Chỉ có một người là Nam, còn lại đều là Nữ. Tất cả đều trong độ tuổi từ 20-30, có khả năng nhận thức và thao thác một cách bình thường.

Cơ sở dữ liệu được tập hợp theo phương pháp sau. Với mỗi người tham gia, các cử chỉ được thu tập theo 7 ngày khác nhau trong khoảng thời gian 3 tuần. Ở mỗi ngày, người tham gia cầm bộ điều khiển từ xa Wii trên tay và thực hiện lần lượt 8 cử chỉ như trong hình 3.1 và mỗi cử chỉ được lặp lại 10 lần. Người tham gia được thoái mái cầm thiết bị điều khiển theo cách mà họ muốn. Chúng ta chỉ yêu cầu họ giữ nó ổn định nhất có thể. Cơ sở dữ liệu bao gồm tổng số 4480 cử chỉ, mỗi người thực hiệc 560 cử chỉ. Mặc dù những người tham gia không phải là những đại diện về nhân khẩu học, nhưng cơ sở dữ liệu này sẽ cung cấp cho chúng ta một tiêu chuẩn mang tính thống kê về độ chính xác của thuật toán nhận dạng.

Dữ liệu được lưu trong các thư mục, mỗi thư mục chứa tập hợp các cử chỉ của một người thực hiện trong một ngày. Tên của các thư mục được đặt theo nguyên tắc sau: **U$userIndex-D$dayIndex**, trong đó userIndex là chỉ số của người tham gia thực hiện cử chỉ từ 1 đến 8, và $dayIndex là chỉ số của ngày thực hiện cử chỉ từ 1 đến 7. Ví dụ thư mục U1-D3 sẽ chứa tập hợp tất cả các cử chỉ của người tham gia thứ nhất đã thực hiện trong ngày thứ 3.

### Tập các chữ ký

## Kết quả thực nghiệm DTW

### Phương pháp thực nghiệm

Tập các mẫu thử từ một người tham gia được sử dụng để tạo ra các mẫu đối sánh và các kiểm tra với cùng một chủ đề. Phương pháp sau đây được áp dụng cho từng người tham gia một cách riêng rẽ. Để rõ ràng hơn, chúng ta gán nhãn cho các mẫu của từng cử chỉ theo trật tự thực hiện. Với test thứ ***i***, chúng ta sử dụng mẫu thử thứ ***i*** cho từng chỉ cử của người tham gia để tạo ra 8 mẫu đối sánh và sử dụng các mẫu thử còn lại để thử nghiệm. Do vậy ***i*** sẽ tăng từ 1 đến 70 (lặp lại 10 lần mỗi ngày và trong vòng 7 ngày), do vậy chúng ta có 70 thử nghiệm cho mỗi người tham gia. Mỗi thử nghiệm sẽ tạo ra một ma trận kết quả thể hiện tỷ lệ phần trăm số lần mẫu được nhận ra. Chúng ta lấy trung bình kết quả của các ma trận của 70 thử nghiệm thì sẽ được ma trận kết quả cho từng người tham gian.

Sau đó, ta tính trung bình ma trận kết quả cho tất cả người tham ra để tạo ra ma trận kết quả cuối cùng. Hình 3.2 thể hiện kết quả nhận dạng của thuật toán DTW với tập dữ liệu từ Nokia. Trong các ma trận, các cột là các cử chỉ được nhận dạng và các hàng là các đặc điểm nhận dạng cho các cử chỉ đầu vào.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  | **88.38** | 0 | 1.91 | 1.59 | 0 | 8.1 | 0 | 0 |
|  | 1.57 | **81** | 0.89 | 1.3 | 1.08 | 4.04 | 9.71 | 0.38 |
|  | 0.02 | 0 | **99.34** | 0.44 | 0 | 0.18 | 0 | 0 |
|  | 0 | 0 | 0.1 | **98.69** | 0.26 | 0.93 | 0 | 0 |
|  | 0 | 0 | 0.48 | 2.46 | **97.02** | 0.02 | 0 | 0 |
|  | 1.87 | 0 | 1.71 | 6.24 | 0 | **90.16** | 0 | 0 |
|  | 0.69 | 1.1 | 1.77 | 1.13 | 1.26 | 0.97 | **92.97** | 0.06 |
|  | 0.3 | 0.04 | 1.04 | 0.83 | 0.77 | 0.48 | 0 | **96.51** |

## Kết quả thực nghiệm của iDTW

## Phân tích và đánh giá

## Kết luận

# KẾT LUẬN

Trong khóa luận tốt nghiệp này, tôi đã tìm hiểu về thread, multithread và các lợi thế của thread và multithread so với tiến trình và đa tiến trình. Ngoài ra, tôi cũng đồng thời cài đặt thành công vào bài toàn tính cước data 3g cho Vinaphone để thấy được hiệu quả của việc sử dụng multithread. Biều đồ so sánh trong chương 4 đã chỉ rõ rằng, với lượng dữ liệu đầu càng lớn, thì hiệu năng tính toán của việc sử dụng thuật toán tuần tự càng lớn so với việc không sử dụng tính toán song song.

Như vậy với đề tài “**NGHIÊN CỨU TÍNH TOÁN SONG SONG VÀ ỨNG DỤNG VÀO HỆ THỐNG TÍNH CƯỚC DATA 3G**” tôi mong muốn đem lại phần nào kiến thức để giúp mọi người có thể ứng dụng vào các bài toán tính toán với số liệu lớn.

Để tôi có được những kết quả như ngày hôm nay cũng như hoàn thành nội dung luận văn tốt nghiệp Thạc sĩ khoa học này, trước hết phải kể đến công lao đào tạo của tất cả các Thầy, Cô giáo trong Học viện Công nghệ Bưu chính - Viễn thông, sự động viên giúp đỡ của tất cả người thân, bạn bè.

Đặc biệt tôi xin được bày tỏ lòng kính trọng và biết ơn tới TS.Trịnh Anh Tuấn, người đã gợi ý cho tôi hướng nghiên cứu của luận văn, hỗ trợ giúp đỡ tôi những kiến thức khoa học bổ ích. Thầy đã đưa ra những nhận xét quý giá và trực tiếp hướng dẫn tôi trong quá trình thực hiện luận văn này.

Tôi xin chân thành cám ơn các anh chí đồng nghiệp trong Công ty NEO nơi tôi đang công tác. Và đối tác Vinphone đã tạo điều kiện cho tôi tham gia và phát triển chương trình.

Cuối cùng, tôi xin gửi lời cảm ơn tới gia đình và bạn bè của tôi, những người đã động viên, khuyến khích tôi rất nhiều trong cuộc sống cũng như trong quá trình công tác và học tập.

Do thời gian có hạn nên chương trình không thể tránh được các thiếu sót các mặt còn hạn chế chẳng hạn như:

- Thiếu các giao diện chức năng để cấu hình các tham số thiết lập bảng giá cước, thông tin quản lý tham số, thông tin các công văn khuyến mại.

- Chưa áp dụng tính toán song song vào chức năng thu thập số liệu.

Tôi mong muốn nhận được sự chỉ bảo, góp ý chân thành của các Thầy Cô giáo cùng các anh chị đồng nghiệp.

|  |  |
| --- | --- |
|  | *Xin chân thành cảm ơn.* |
|  | *Hà Nội, tháng 11/2013* |
|  | **Hà Quang Tấn** |

# HƯỚNG PHÁT TRIỂN TIẾP THEO

# DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng việt

1. PSG TS Nguyễn Đức Nghĩa (2007), Tính Toán Song Song, Nhà xuất bản Đại học Quốc gia Hà Nội.

Tiếng Anh

1. Dimitri P. Bertsekas and John N. Tsitsiklis. Parallel and Distributed Computation, Numerical Methods. Massachusets Institute of Technology. Prentice Hall Press.
2. Enrico P. The lecture notes on Parallel Computing (CS 491). Computer Science Dept. New Mexico State University, USA. Spring 2004.
3. Michael J. Quinn. Parallel Computing, theory and practice, 2nd edition. Oregon State University, USA. McGraw Hill Inc.
4. Posix thread programing, http://computer.llnl.gov.tutorials/pthreads.
5. Pthreads API. Available: <http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Fapis%2Fusers_16.htm>.
6. Flynn, Michael J. (1995). *Computer architecture: pipelined and parallel processor design*. Boston
7. Lib and include pthread 64bit, available: <ftp://sourceware.org/pub/pthreads-win32/dll-latest>; access: 10/08/2013