**Mục lục**

🙢🕮🙠

* [Chương 1 Mở đầu 1](#_Toc477971628)
* [1.1 Giới thiệu chung 1](#_Toc477971629)
* [1.2 Sự phát triển của thiết bị di động và thiết bị đeo 2](#_Toc477971630)
* [1.2.1 Sự phát triển và tiềm năng ứng dụng của thiết bị di động và thiết bị đeo 2](#_Toc477971631)
* [1.2.2 Bảo mật và an toàn thông tin cho ứng dụng và dịch vụ với thiết bị di động và thiết bị đeo 3](#_Toc477971632)
* [1.3 Lý do thực hiện đề tài 5](#_Toc477971633)
* [1.4 Mục tiêu đề tài 6](#_Toc477971634)
* [1.5 Một số kết quả trong giai đoạn đầu của đề tài 7](#_Toc477971635)
* [1.6 Nội dung báo cáo 9](#_Toc477971636)
* [Chương 2 Tổng quan về chứng thực người dùng sử dụng đặc trưng sinh trắc học 11](#_Toc477971637)
* [2.1 Tổng quan 11](#_Toc477971638)
* [2.2 Các đặc trưng sinh trắc 13](#_Toc477971639)
* [2.3 Hệ thống sử dụng đặc trưng sinh trắc 17](#_Toc477971640)
* [2.4 Kết chương 18](#_Toc477971641)
* [Chương 3 Tổng quan về việc định danh người dùng bằng đặc trưng dáng đi 19](#_Toc477971642)
* [3.1 Mở đầu 19](#_Toc477971643)
* [3.2 Các hướng tiếp cận chính 21](#_Toc477971644)
* [3.3 Thiết lập sensor và thu thập dữ liệu 23](#_Toc477971645)
* [3.4 Tiền xử lí 25](#_Toc477971646)
* [3.4.1 Lọc dữ liệu 26](#_Toc477971647)
* [3.4.2 Phát hiện dáng đi và nhận biết hành động 26](#_Toc477971648)
* [3.5 Phân vùng 27](#_Toc477971649)
* [3.5.1 Các hướng tiếp cận dựa trên chu kỳ 28](#_Toc477971650)
* [3.5.2 Phương pháp dựa trên frame 29](#_Toc477971651)
* [3.6 Biến đổi mẫu dáng đi 30](#_Toc477971652)
* [3.7 Quy trình nhận dạng 31](#_Toc477971653)
* [3.8 Kết chương 32](#_Toc477971654)
* [Chương 4 Tổng quan về Neural Network, Convolutional Neural Network, Recurrent Neural Network 34](#_Toc477971655)
* [4.1 Giới thiệu về neural network 34](#_Toc477971656)
* [4.1.1 Tổng quan 34](#_Toc477971657)
* [4.1.2 Perceptron 36](#_Toc477971658)
* [4.1.3 Kiến trúc của mạng 38](#_Toc477971659)
* [4.1.4 Lan truyền thuận (feed forward) 40](#_Toc477971660)
* [4.1.5 Lan truyền ngược (backpropagation) và phương pháp gradient descent 41](#_Toc477971661)
* [4.2 Các thành phần cơ bản của Convolutional Neural Network (CNN) 43](#_Toc477971662)
* [4.2.1 Convolution 44](#_Toc477971663)
* [4.2.2 Cổng phi tuyến (non-linear gating) 46](#_Toc477971664)
* [4.2.3 Pooling 47](#_Toc477971665)
* [4.2.4 Chuẩn hóa (Normalization) 48](#_Toc477971666)
* [4.2.5 Kiến trúc mạng CNN 48](#_Toc477971667)
* [4.3 Phương pháp lan truyền ngược 51](#_Toc477971668)
* [4.4 Deep CNN là mạng học đặc trưng nhiều tầng 54](#_Toc477971669)
* [4.5 Một số vấn đề nâng cao về mạng CNN 55](#_Toc477971670)
* [4.5.1 Dữ liệu huấn luyện 55](#_Toc477971671)
* [4.5.2 Kiến trúc mạng 56](#_Toc477971672)
* [4.5.3 Một số cải tiến trong việc huấn luyện 56](#_Toc477971673)
* [4.5.4 Phương pháp Dropout 57](#_Toc477971674)
* [4.6 MatConvNet 58](#_Toc477971675)
* [4.7 Kết chương 62](#_Toc477971676)
* [Chương 5 63](#_Toc477971677)
* [Chương 6 Dữ liệu và thử nghiệm nhận biết người dùng bằng đặc trưng dáng đi 64](#_Toc477971678)
* [6.1 Các tập dữ liệu thử nghiệm 64](#_Toc477971679)
* [6.1.1 OU-ISIR Gait Database, Inertial Sensor Dataset 64](#_Toc477971680)
* [6.1.2 Tập dữ liệu của Hoang et.al 66](#_Toc477971681)
* [Chương 7 Các hướng tiếp cận chính trong việc xây dựng quy trình chứng thực 67](#_Toc477971682)
* [7.1 Giới thiệu chung 67](#_Toc477971683)
* [7.2 Ứng dụng chứng thực 67](#_Toc477971684)
* [7.3 Lưu trữ chứng thực 69](#_Toc477971685)
* [7.4 Phân loại chứng thực 70](#_Toc477971686)
* [7.4.1 Chứng thực thông thường 70](#_Toc477971687)
* [7.4.2 Chứng thực dựa trên sinh trắc học 72](#_Toc477971688)
* [7.5 Thuật toán chứng thực 74](#_Toc477971689)
* [7.6 Mô hình chứng thực 76](#_Toc477971690)
* [7.7 Kết chương 78](#_Toc477971691)
* [Chương 8 Quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc và hệ thống truy cập dịch vụ trực tuyến 79](#_Toc477971692)
* [8.1 Chứng thực với sinh trắc học 79](#_Toc477971693)
* [8.2 Đề xuất quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc 80](#_Toc477971694)
* [8.2.1 Đề xuất quy trình chứng thực 80](#_Toc477971695)
* [8.2.2 Chứng minh tính an toàn 84](#_Toc477971696)
* [8.2.3 Phân tích hiệu quả của quy trình chứng thực 89](#_Toc477971697)
* [8.2.4 Tổng kết phần đề xuất quy trình chứng thực dựa trên sinh trắc 90](#_Toc477971698)
* [8.3 Đề xuất quy trình chứng thực cho hệ thống tương tác thông minh 93](#_Toc477971699)
* [8.3.1 Đề xuất quy trình chứng thực 93](#_Toc477971700)
* [8.3.2 Phân tích độ an toàn 96](#_Toc477971701)
* [8.4 Kết chương 98](#_Toc477971702)
* [Chương 9 Quy trình chứng thực an toàn sử dụng đa thức Chebysev 99](#_Toc477971703)
* [9.1 Giới thiệu 99](#_Toc477971704)
* [9.2 Qui trình của Chang và các phân tích đánh giá 101](#_Toc477971705)
* [9.2.1 Qui trình của Chang 102](#_Toc477971706)
* [9.2.2 Pha đăng kí 102](#_Toc477971707)
* [9.2.3 Pha chứng thực 103](#_Toc477971708)
* [9.2.4 Pha thay đổi mật khẩu 104](#_Toc477971709)
* [9.2.5 Pha khôi phục thẻ 104](#_Toc477971710)
* [9.3 Phân tích đánh giá qui trình Chang và các cộng sự 105](#_Toc477971711)
* [9.3.1 Không cung cấp tính nặc danh người dùng 105](#_Toc477971712)
* [9.3.2 Tấn công mạo danh 105](#_Toc477971713)
* [9.3.3 Tấn công khóa phiên 106](#_Toc477971714)
* [9.4 Qui trình đề xuất 107](#_Toc477971715)
* [9.4.1 Pha đăng kí 107](#_Toc477971716)
* [9.4.2 Pha đăng nhập 108](#_Toc477971717)
* [9.4.3 Pha chứng thực và thỏa hiệp khóa 109](#_Toc477971718)
* [9.4.4 Pha cập nhật mật khẩu 109](#_Toc477971719)
* [9.4.5 Pha khôi phục thẻ 110](#_Toc477971720)
* [9.5 Các phân tích độ an toàn và tính hiệu quả 110](#_Toc477971721)
* [9.5.1 Chứng minh độ chính xác 111](#_Toc477971722)
* [9.5.2 Phân tích các hình thức tấn công phổ biến 114](#_Toc477971723)
* [9.5.3 Phân tích tính hiệu quả 116](#_Toc477971724)
* [9.6 Kết chương 117](#_Toc477971725)
* [Tài liệu tham khảo 120](#_Toc477971726)

**Danh sách hình**

🙢🕮🙠

[Hình 4.2. Các hàm kích hoạt (activation function). [65] 39](#_Toc477971727)

[Hình 4.3. Một ví dụ của neural network. [65] 40](#_Toc477971728)

[Hình 4.4. Mạng neural network với các neuron được kết nối đầy đủ với nhau 45](#_Toc477971729)

[Hình 4.5. Mạng neural network với các neuron được liên kết cục bộ với các neuron thuộc layer trước 46](#_Toc477971730)

[Hình 4.6. Một pha trong mạng CNN 49](#_Toc477971731)

[Hình 4.7. Mạng CNN sâu bao gồm nhiều pha ở giữa và các layer kết nối đầy đủ ở những layer cuối cùng. 50](#_Toc477971732)

[Hình 4.8. Kiến trúc mạng CNN được sử dụng trong cuộc thi ImageNet Classification 2012 51](#_Toc477971733)

[Hình 4.9. Phạm vi chịu ảnh hưởng của một điểm đặc trưng đối với ảnh đầu vào. 54](#_Toc477971734)

[Hình 4.10. Ảnh trực quan hóa các layer của mạng CNN sau quá trình huần luyện. 55](#_Toc477971735)

[Hình 4.11. Hiệu quả của việc sử dụng phương pháp Dropout giúp làm giảm độ lỗi trong quá trình huấn luyện và phân loại đối tượng. 58](#_Toc477971736)

[Hình 6.1. Cách lắp đặt sensor để thu thập dữ liệu cho OU-ISIR Gait Database, Inertial Sensor Dataset 65](#_Toc477971737)

[Hình 6.2. Một số ví dụ về dữ liệu ghi nhận trong OU-ISIR Gait Databasem Inertial Sensor Dataset 66](#_Toc477971738)

[Hình 9.1. So sánh chi phí thời gian giữa Tn(g) mod p và gn mod p 117](#_Toc477971739)

Danh sách hình

🙢🕮🙠

[Hình 1‑1 zdcfzfczx 5](#_Toc477972020)

[Hình 4‑1 sdasd 36](#_Toc477972021)

[Hình 4‑2 asdasd 36](#_Toc477972022)

[Hình 4‑3 Kiến trúc chung của mạng neural kết nối đầu đủ. [62] 38](#_Toc477972023)

[Hình 8‑1 - Pha đăng ký của quy trình chứng thực đề xuất 81](#_Toc477972024)

[Hình 8‑2 - Pha đăng nhập và chứng thực hai phía của quy trình chứng thực đề xuất 83](#_Toc477972025)

Danh sách bảng

🙢🕮🙠

[Bảng 2.1. Tính chất các đặc trưng sinh trắc 16](#_Toc477971740)

[Bảng 8.1. So sánh về khả năng chống lại nhiều kiểu tấn công 89](#_Toc477971741)

[Bảng 8.2. So sánh chi phí tính toán 89](#_Toc477971742)

[Bảng 8.3. So sánh về các đặc tính thân thiện 90](#_Toc477971743)

[Bảng 8.4. So sánh khả năng chống lại nhiều kiểu tấn công khác nhau 98](#_Toc477971744)

[Bảng 9.1. Các kí hiệu dùng trong qui trình 102](#_Toc477971745)

[Bảng 9.2. So sánh độ an toàn giữa các qui trình 116](#_Toc477971746)

[Bảng 9.3. So sánh chi phí tính toán 116](#_Toc477971747)

Danh sách bảng

[Bảng 2‑1 Tính chất các đặc trưng sinh trắc 16](#_Toc477972541)

# Mở đầu

*✍ Nội dung Chương 1 trình bày tổng quan chung và lý do thực hiện đề tài, từ đó nêu lên mục tiêu và nội dung chính trong đề tài. Ở phần cuối chương, chúng tôi trình bày tóm tắt một số kết quả đạt được trong giai đoạn một của đề tài và cấu trúc của báo cáo.*

## Giới thiệu chung

Sự ra đời và phát triển các *thiết bị di động* (*mobile device*) và các *thiết bị tính toán thông minh có thể đeo được* (*wearable device*) đã mở ra *kỷ nguyên mới* cho các ứng dụng với máy tính và dịch vụ trực tuyến phục vụ cuộc sống con người một cách hiệu quả và đa dạng hơn.

Điện thoại di động thông minh hay máy tính bảng là các loại *thiết bị di động* thường gặp, cho phép người dùng có thể sử dụng các tính năng và ứng dụng đa dạng như một máy tính cá nhân đa năng nhỏ gọn và dễ mang chuyển. Trong khi đó, *các thiết bị đeo* như đồng hồ thông minh (*smart* *watch*), vòng đeo hay thiết bị theo dõi luyện tập thể thao (*activity tracker*), kính đeo mắt thông minh (*smart eyeware*)… thường cung cấp tính năng hay tiện ích đặc thù và được người dùng đeo thường xuyên để ghi nhận thông tin, hoạt động của mình.

Nhờ tính phổ biến của thiết bị di động và tiềm năng ứng dụng rộng rãi trong tương lai của thiết bị đeo, nhiều ứng dụng và dịch vụ mới đa dạng và phong phú đã và đang được phát triển. Điều này dẫn đến nhu cầu cấp thiết về các giải pháp để bảo vệ *an toàn thông tin* cho người dùng khi khai thác các ứng dụng, đặc biệt là hệ thống *dịch vụ trực tuyến*, từ thiết bị di động hay thiết bị đeo. Trong đó, *chứng thực an toàn, thuận tiện và hiệu quả* là một trong những bài toán có ý nghĩa quan trọng, cần có trong hầu hết các ứng dụng và dịch vụ vì đây là *bước đầu tiên* để thiết lập giao dịch trực tuyến an toàn. Vì vậy, đây là vấn đề vừa có *ý nghĩa học thuật*, vừa có tiềm năng ứng dụng và *ý nghĩa thực tế* cao.

Việc chứng thực cho ứng dụng với thiết bị di động hay thiết bị đeo bao gồm: (i) *chứng thực đối với thiết bị* và (ii) *chứng thức với hệ thống dịch vụ bằng thiết bị*. Công việc thứ nhất nhằm giúp thiết bị *phân biệt để nhận biết được định danh của người dùng*. Trong công việc thứ hai, thiết bị được sử dụng như một *token an toàn* để giúp chứng thực người dùng với *hệ thống dịch vụ trực tuyến*.

So với các máy tính cá nhân hay máy tính xách tay thông thường, thiết bị di động, đặc biệt là thiết bị đeo, có nhiều *hạn chế* về *năng lực xử lý*, *lưu trữ* và *kết nối mạng*. Điều này dẫn đến những khó khăn, ràng buộc khi thiết kế và xây dựng giải pháp chứng thực với thiết bị di động và thiết bị đeo.

Mặt khác, hai nhóm thiết bị này thường xuyên đi kèm với người dùng nên có khả năng theo dõi và ghi nhận được thường xuyên các thông tin về ngữ cảnh (môi trường và người sử dụng) thông qua các loại *cảm biến* (sensor) khác nhau như cảm ứng chuyển động, từ, ánh sáng, nhiệt độ, nhịp tim…. Nhờ đó các giải pháp chứng thực có thể khai thác được nhiều thông tin khác nhau từ người dùng, đặc biệt là các đặc trưng sinh trắc học như vân tay, gương mặt giọng nói, dáng đi, nét viết/vẽ khi người dùng ký…

## Sự phát triển của thiết bị di động và thiết bị đeo

### Sự phát triển và tiềm năng ứng dụng của thiết bị di động và thiết bị đeo

Từ đầu thế kỷ 21 đến nay, thiết bị di động ngày càng phát triển đa dạng và phong phú. *Điện thoại thông minh* hay *máy tính bảng* là các loại *thiết bị di động* (*mobile device*) phổ biến thường gặp. Nhờ khả năng cho phép khai thác dịch vụ và các ứng dụng tiện ích mọi nơi và mọi lúc, thiết bị di động dễ tiếp cận với người dùng hơn các máy tính truyền thống. Đồng thời, các ứng dụng và dịch vụ trực tuyến cho thiết bị di động ngày càng phát triển đa dạng và phong phú với hàng triệu ứng dụng trên các kho sản phẩm phần mềm cho thiết bị di động.

*Thiết bị tính toán thông minh có thể đeo* hay còn gọi lại*thiết bị đeo* (*wearable device*) là một bước tiến của việc thu nhỏ kích thước các hệ thống tính toán nhằm cung cấp tiện ích với các xử lý thông minh *tích hợp vào trang phục hay dụng cụ đeo trên người* như mắt kiếng, vòng tay, đồng hồ… Thiết bị đeo khai thác để mang lại những lợi ích cho con người theo hướng đi mới so với những thiết bị truyền thống. Các thiết bị thông thường chủ yếu nhận và xử lý thông tin trực tiếp từ phía người dùng khi họ tương tác. Nhưng trong thực tế, người dùng có thể làm những việc khác quan trọng hơn trong khi tương tác với các thiết bị. Đó là lý do thiết bị đeo ứng dụng nhiều hơn nhằm tương tác với người dùng một cách gián tiếp mà không cần người dùng phải tác động. Nhờ vào đặc tính có thể mang được trên người, thiết bị đeo giúp theo dõi và quan sát một cách đầy đủ hơn ngữ cảnh của con người so với ngữ cảnh mà các thiết bị thông thường (máy tính và thiết bị di động) có thể thu nhận được.

Trong nghiên cứu thí nghiệm, các cảm biến (sensor) thường được tích hợp thành thiết bị đeo đơn giản để thu thập dữ liệu, giúp các nhà nghiên cứu thực nghiệm thuật toán trước khi các cảm biến này được tinh chỉnh và tích hợp vào điện thoại thông minh.

### Bảo mật và an toàn thông tin cho ứng dụng và dịch vụ với thiết bị di động và thiết bị đeo

Sự phổ biến của thiết bị di động cho phép người dùng ghi nhận, truy cập và đồng bộ hóa dữ liệu mọi nơi, mọi lúc. Dữ liệu cá nhân (ảnh chụp, video, tài liệu, danh bạ, lịch hẹn, nhật ký…) có thể được gửi từ thiết bị lên dịch vụ lưu trữ trực tuyến cũng như đồng bộ hóa giữa nhiều thiết bị khác nhau của người dùng. Người dùng cũng có thể khai thác các dịch vụ trực tuyến, thực hiện các giao dịch thương mại (m-commerce) hay thanh toán trực tuyến với thiết bị di động. Điện thoại di động có thể được dùng để tiến hành việc thanh toán tại các điểm giao dịch (Point of Sale), quản lý việc sử dụng coupon hay tích lũy điểm thưởng trong các giao dịch. Vì vậy, việc bảo vệ an toàn thông tin cho người dùng khi dữ liệu, thông tin cá nhân cũng như các truy vấn và giao dịch trực tuyến được trao đổi giữa thiết bị với dịch vụ trực tuyến là nhu cầu cấp thiết, đặc biệt khi số lượng dịch vụ trực tuyến càng tăng nhanh.

Vai trò của thiết bị đeo ngày càng được thể hiện rõ trong việc trao đổi những thông tin ngữ cảnh của con người. Thiết bị đeo ghi nhận những thông tin cá nhân, dữ liệu sinh trắc học, cảm xúc và những thông tin môi trường xung quanh của người dùng. Do đó, nhu cầu bảo mật thông tin và chứng thực người dùng luôn là yếu tố được đặt ra trên thiết bị đeo.

Đối với các hệ thống sử dụng thiết bị di động và thiết bị đeo, việc bảo vệ an toàn thông tin bao gồm đầy đủ cả ***5 nhóm bài toán chính*** trong lĩnh vực an toàn thông tin: bảo mật nội dung (*secrecy*), toàn vẹn dữ liệu (*integrity*), chứng thực (*authentication*), chống thoái thác trách nhiệm (*non*-*repudiation*) và bảo vệ tính riêng tư (*privacy*). Trong đó, việc ***chứng thực*** có ý nghĩa quan trọng vì đây là ***giai đoạn đầu tiên để thiết lập các giao dịch*** giữa thiết bị với hệ thống và dịch vụ bên ngoài. Việc chứng thực này bao gồm hai vấn đề chính:

* ***Chứng thực người dùng tại thiết bị***: người dùng chứng thực định danh với thiết bị. Đây có thể xem là bước khởi đầu của quy trình chứng thực người dùng để khai thác dịch vụ trực tuyến từ thiết bị.
* ***Chứng thực người dùng để khai thác dịch vụ từ thiết bị***: thiết bị di động hoặc thiết bị có thể đeo được sử dụng phục vụ quy trình chứng thực người dùng khi khai thác dịch vụ trực tuyến. Thiết bị được xem là client khai thác dịch vụ và cần chứng thực với máy chủ .

Hình 1.1 minh họa 3 tình huống chứng thực thường gặp với hệ thống sử dụng thiết bị di động hay thiết bị đeo. Thiết bị di động hay thiết bị đeo có thể thực hiện chứng thực trực tiếp với dịch vụ trực tuyến (Hình 1.1a và Hình 1.1b). Trên thực tế, hầu hết thiết bị đeo hiện nay thường bị giới hạn về khả năng xử lý và năng lượng kết nối nên thiết bị đeo thường kết nối gần với thiết bị di động (ví dụ như qua *Bluetooth Low Energy* – BLE) và việc chứng thực với hệ thống dịch vụ trực tuyến từ thiết bị di động (Hình 1.1c).

|  |  |
| --- | --- |
|  |  |
| (a) Chứng thực giữa thiết bị di động và dịch vụ | (b) Chứng thực giữa thiết bị đeo và dịch vụ |



Hình 1‑1 zdcfzfczx

(c) Thiết bị đeo kết nối gần với thiết bị di động để khai thác dịch vụ

## Lý do thực hiện đề tài

Các giải pháp hiện nay để chứng thực từ thiết bị để khai thác dịch vụ sử dụng *còn một số điểm yếu trước một số tình huống tấn công*. Vì vậy cần tiếp tục nghiên cứu để đề xuất các quy trình an toàn hơn và phù hợp, hiệu quả khi triển khai với thiết bị di động và thiết bị đeo. Bên cạnh đó, các giải pháp chứng thực từ thiết bị để khai thác dịch vụ sử dụng *phương pháp pairing* thường đòi hỏi *chi phí xử lý cao*, chưa thật sự phù hợp và hiệu quả khi triển khai trên thiết bị di động và đặc biệt là thiết bị đeo.

Việc chứng thực người dùng với đặc trưng sinh trắc học thường tập trung vào các loại *đặc trưng truyền thống* như vân tay, võng mạc, giọng nói, gương mặt. Các *đặc trưng sinh trắc học khác*, ví dụ như đặc trưng dựa vào chuyển động (gait) là *cách tiếp cận mới* cần được nghiên cứu. Đặc biệt, các phương pháp chứng thực với đặc trưng dáng chuyển động đều dùng các *kỹ thuật phân lớp truyền thống* như SVM, láng giềng gần nhất, mạng neuron…, chưa tận dụng được ưu điểm của các kỹ thuật mới trong *deep learning*.

Các công trình nghiên cứu về chứng thực bằng đặc trưng dáng chuyển động chủ yếu tập trung vào việc đề xuất phương pháp phân biệt để nhận biết người dùng dựa vào thông tin chuyển động, *chưa đề xuất quy trình* chặt chẽ để chứng thực người dùng bằng đặc trưng dáng chuyển động.

## Mục tiêu đề tài

* **Mục tiêu chung của đề tài:**

Đề xuất *phương pháp an toàn, hiệu quả* và *phù hợp* cho việc *chứng thực sử dụng thiết bị di động* hay *thiết bị đeo*, bao gồm *chứng thực người dùng đối với thiết bị* sử dụng đặc trưng *dáng chuyển động* (*gait*) và *sử dụng thiết bị* để *chứng thực người dùng* với *hệ thống dịch vụ trực tuyến*.

* **Mục tiêu chi tiết:**
* Nghiên cứu và đề xuất *phương pháp nhận biết* người dùng dựa vàođặc trưng *sinh trắc học* dựa vào *dáng chuyển động* (*gait*) sử dụng kỹ thuật *deep learning*.
* Nghiên cứu và đề xuất *quy trình* *chứng thực* người dùng *đối với thiết bị di động hay thiết bị đeo* sử dụng đặc trưng *sinh trắc học* dựa vào *dáng chuyển động* (*gait*).
* Nghiên cứu và đề xuất *quy trình chứng thực* người dùng với *dịch vụ trực tuyến* sử dụng *thiết bị di động* hay *thiết bị đeo* theo hướng tiếp cận *không sử dụng pairing*.
* **Tính mới của đề tài**
* Để xây dựng quy trình chứng thực an toàn, hiệu quả và phù hợp với thiết bị di động và thiết bị đeo, nhóm nghiên cứu chọn hướng tiếp cận *không dùng phương pháp pairing* có chi phí xử lý cao mà dùng các hàm băm một chiều kết hợp các xử lý trên đường cong eliptic và đại lượng ngẫu nhiên nhằm tăng tính hiệu quả trong xử lý và phù hợp với thiết bị có hạn chế về năng lực xử lý. Đây là hướng tiếp cận mới, đang được quan tâm nghiên cứu trên thế giới trong 5 năm gần đây.
* Việc chứng thực với các đặc trưng sinh trắc học truyền thống như vân tay, võng mạc, giọng nói, gương mặt đã được nghiên cứu nhiều trên thế giới. Do đó, trong đề tài này, nhóm nghiên cứu tập trung nghiên cứu việc *chứng thực dựa vào đặc trưng dáng chuyển động (gait)* là một trong những *hướng tiếp cận mới* hiện đang được quan tâm nghiên cứu trên thế giới.
* Hiện tại, các công trình nghiên cứu trên thế giới về chứng thực bằng đặc trưng sinh trắc học sử dụng phân lớp chủ yếu dùng các *phương pháp phân lớp và máy học kinh điển* như SVM, mạng neuron, láng giềng gần nhất. Việc nghiên cứu các kỹ thuật trong *deep learning* trong việc huấn luyện và phân biệt người dùng dựa vào đặc trưng sinh trắc học là *cách tiếp cận mới, không chỉ trong nước mà cả trên thế giới*.
* Hiện nay chưa có công trình nghiên cứu trên thế giới *đề xuất quy trình chặt chẽ* cho việc chứng thực với đặc trưng dáng chuyển động. Các công trình hiện nay chỉ tập trung vào thuật toán để nhận biết người dùng từ thông tin chuyển động, chưa xét đến *khả năng bị tấn công* và *giải pháp ngăn ngừa* tấn công khi dùng chứng thực bằng đặc trưng dáng chuyển động.
* Hiện nay *chưa có đề tài nghiên cứu nào trong nước* nghiên cứu đề xuất phương pháp nhận biết người dùng sử dụng đặc trưng dáng chuyển động với các kỹ thuật trong deep learning.

## Một số kết quả trong giai đoạn đầu của đề tài

Trong đề tài này, chúng tôi tập trung thực hiện ***ba nội dung chính***: (1) đề xuất phương pháp nhận biết người dùng dựa vào đặc trưng sinh trắc học dựa vào dáng chuyển động (gait) sử dụng kỹ thuật deep learning; (2) đề xuất quy trình chứng thực người dùng đối với thiết bị di động hay thiết bị đeo sử dụng đặc trưng sinh trắc học dựa vào dáng chuyển động (gait) và (3) đề xuất quy trình chứng thực người dùng với dịch vụ trực tuyến sử dụng thiết bị di động hay thiết bị đeo. Trong đó, ***giai đoạn một*** của đề tài tập trung vào ***nội dung thứ nhất***, và ***giai đoạn hai*** của đề tài sẽ giải quyết ***hai nội dung còn lại***.

Trong giai đoạn đầu thực hiện đề tài, chúng tôi đã ***đề xuất*** một ***kiến trúc tổng quát*** cho một ***họ các convolutional neural network*** hiệu quả cho việc ***rút trích*** và ***biểu diễn đặc trưng cấp cao cho dáng đi*** – gait – từ dữ liệu ghi nhận từ sensor chuyển động. Chúng tôi còn đề xuất chiến lược Ensemble SVM ***sử dụng nhiều bộ phân lớp SVM*** để tăng độ chính xác khi nhận biết người dùng từ đặc trưng cấp cao của dáng đi.

Sử dụng kiến trúc của họ Convolutional Neural Network được chúng tôi đề xuất, qua thực nghiệm, chúng tôi đã tìm ra ***nhiều cấu hình và neural network cụ thể*** khác nhau theo kiến trúc này để có thể phân biệt tốt người dùng dựa trên đặc trưng dáng đi. Nhiều neural network cụ thể tuân theo kiến trúc mà chúng tôi xây dựng đạt được chỉ số EER (Equal Error Rate) ***xấp xỉ các phương pháp tốt nhất*** trên ***tập dữ liệu*** đặc trưng dáng đi ***lớn nhất*** hiện nay OU-ISIR Gait Database - Inertial Sensor Dataset.

Trong số các neural network tìm được, chúng tôi chọn thể hiện có chỉ số EER thấp nhất và dùng network này dưới dạng ***pre-trained network*** để ***rút trích*** và ***biểu diễn đặc trưng cấp cao*** của dáng đi. Sử dụng pre-trained network này cùng với chiến lược phân lớp với ***nhiều bộ phân lớp SVM*** và cơ chế bình chọn, phương pháp của chúng tôi đạt được độ chính xác trên 95% trên tập dữ liệu do chúng tôi xây dựng trong đề tài này.

Một phần kết quả của đề tài về việc đề xuất Ensemble SVM với nhiều bộ phân lớp SVM để tăng độ chính xác trong nhận dạng người dùng từ đặc trưng dáng đi đã được chúng tôi công bố trong công trình [CT2]. Hiện nay, chúng tôi đang tiếp tục hoàn thiện bài báo để gửi đăng kết quả về kiến trúc của họ convolutional neural network để rút trích và biểu diễn đặc trưng cấp cao của dáng đi.

Trong quá trình tìm hiểu, nghiên cứu về convolutional neural network để xây dựng kiến trúc tổng quát cho một họ convolutional neural network phục vụ bài toán nhận biết người dùng từ dáng đi, chúng tôi đã đề xuất ra thêm một kiến trúc tương tự cho một họ convolutional neural network khác để chứng thực/kiểm tra người dùng bằng cách so khớp mặt người. Kết quả của việc dùng kiến trúc của họ CNN vào bài toán chứng thực người dùng bằng mặt người đã được chúng tôi công bố trong công trình [CT3]. Tuy nhiên, do kết quả này không thuộc khuôn khổ đề tài này nên chúng tôi không trình bày trong báo cáo đề tài.

Trong đề tài này, mục tiêu mà chúng tôi hướng đến là ***xây dựng giải pháp chứng thực an toàn*** cho người dùng khi ***khai thác các dịch vụ trực tuyến*** ***với thiết bị di động***, trong đó ***đặc trưng dáng đi*** được dùng như một ***cách tiếp cận mới***. Do đó, ngay từ giai đoạn thứ nhất của đề tài, chúng tôi đã ***nghiên cứu và thực hiện thêm*** các nội dung trong ***giai đoạn hai*** của đề tài: chúng tôi đã xây dựng ***quy trình chứng thực có tích hợp nhận biết người dùng từ đặc trưng dáng đi*** (công trình [CT2]) cũng như nghiên cứu và đề xuất một ***hướng tiếp cận mới*** trong việc ***thiết kế quy trình chứng thực*** sử dụng ***đa thức Chebysev***.

Sau năm đầu tiên thực hiện đề tài, chúng tôi đã công bố ***2 bài báo khoa học*** tại hội nghị quốc tế; 1 bài báo của chúng tôi đang trong quá trình phản biện tại tạp chí quốc tế (thuộc nhóm ISI). Hiện nay có ***hai nghiên cứu sinh*** đang tham gia đề tài và ***mỗi nghiên cứu sinh*** đã xuất sắc ***hoàn thành một chuyên đề trực tiếp từ nội dung đề tài này*** (điểm chuyên đề là 9.5 và 9.2). Trong số 03 học viên Cao học tham gia, ***01 học viên đã bảo vệ đề tài*** và đang chờ nhận bằng Thạc sĩ, ***02 học viên sẽ bảo vệ đề tài*** trong năm 2016. Ngoài ra, chúng tôi đã hướng dẫn ***03 sinh viên bảo vệ khóa luận Đại học với kết quả 10/10***, đồng thời 01 nhóm sinh viên đã xuất sắc đạt ***Giải Nhất*** giải thưởng Sinh viên Nghiên cứu khoa học cấp Đại học Quốc gia và ***Giải Nhì*** giải thưởng Sinh viên Nghiên cứu khoa học Eureka của Tp. Hồ Chí Minh năm 2015.

## Nội dung báo cáo

Nội dung báo cáo bao gồm 10 chương. Ngoài Chương 1 – Mở đầu và Chương 10 – Kết luận, các chương còn lại trình bày các kết quả chính đạt được trong đề tài. Trong Chương 5 và Chương 6, chúng tôi trình bày phương pháp mà chúng tôi đề xuất và kết quả thực nghiệm để nhận biết người dùng từ đặc trưng dáng đi với convolutional neural network. Ngoài ra, chúng tôi còn trình bày thêm đề xuất quy trình chứng thực hai chiều tích hợp đặc trưng dáng đi (trong Chương 8) và một hướng tiếp cận mới trong việc thiết kế quy trình chứng thực an toàn với đa thức Chebysev (trong Chương 9).

**Nội dung chi tiết của mỗi chương trong báo cáo như sau:**

***Chương 1***: trình bày tổng quan về đề tài, lý do thực hiện, mục tiêu đề tài, các kết quả chính đã đạt được và cấu trúc nội dung báo cáo.

***Chương 2***: trình bày tổng quan về chứng thực người dùng sử dụng đặc trưng sinh trắc học, bao gồm các loại đặc trưng sinh trắc, các ưu điểm và hạn chế của từng loại đặc trưng

***Chương 3***: trình bày tổng quan về việc định danh người dùng bằng đặc trưng dáng đi, bao gồm các hướng tiếp cận chính, cách thiết lập sensor ghi nhận thông tin và thu thập dữ liệu, các bước tiền xử lý, phân đoạn, các phép biến đổi và quy trình nhận dạng

***Chương 4***: trình bày tổng quan về neural network, tập trung đi sâu vào các thành phần cơ bản của Convolutional Neural Network (CNN), một dạng neural network đặc thù với khả năng liên kết – phụ thuộc cục bộ giữa các node trong 2 layer liên tiếp.

***Chương 5***: chúng tôi đề xuất một kiến trúc tổng quát cho mô hình Convolutional Neural Network để tạo ra nhiều thể hiện (instance) cụ thể của mô hình CNN có cấu trúc tương tự nhau để huấn luyện và nhận biết người dùng dựa trên đặc trưng chuyển động. Chúng tôi còn đề xuất sử dụng kết hợp nhiều bộ phân lớp SVM với cơ chế bình chọn để nhận biết người dùng từ đặc trưng cấp cao của dáng đi.

***Chương 6***: trình bày về các tập dữ liệu được sử dụng để thử nghiệm việc nhận biết người dùng bằng đặc trưng dáng đi, đồng thời trình bày các kết quả thử nghiệm trên 3 tập dữ liệu: OU-ISIR Gait Database - Inertial Sensor Dataset, tập dữ liệu Hoang et.al và tập dữ liệu thực tế do chúng tôi tự xây dựng.

***Chương 7***: tóm tắt một vài công trình liên quan đến việc xây dựng quy trình chứng thực. Bên cạnh đó, việc đánh giá và phân tích các hướng tiếp cận khác nhau trong những trường hợp khác nhau sẽ giúp chúng ta có được các kinh nghiệm quan trọng giúp ích cho việc đề xuất các cải tiến sau này.

***Chương 8***: chúng tôi đề xuất quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc, từ đó áp dụng để xây dựng hệ thống cho phép truy cập thông tin và các dịch vụ trực tuyến với chứng thực sử dụng thiết bị di động và đặc trưng dáng đi.

***Chương 9***: trình bày một hướng tiếp cận mà chúng tôi đề xuất để thiết kế quy trình chứng thực an toàn sử dụng đa thức Chebysev.

***Chương 10***: tổng kết các kết quả chính đã đạt được trong giai đoạn đầu của đề tài, đồng thời trình bày một số vấn đề chính mà nhóm nghiên cứu đang tiếp tục thực hiện.

# Tổng quan về chứng thực người dùng sử dụng đặc trưng sinh trắc học

**Tóm tắt chương:**

*✍ Trong Chương 2, chúng tôi trình bày tổng quan về chứng thực người dùng sử dụng đặc trưng sinh trắc học, bao gồm các loại đặc trưng sinh trắc, các ưu điểm và hạn chế của từng loại đặc trưng*

## Tổng quan

Sinh trắc học, hay công nghệ sinh trắc học là khoa học, công nghệ sử dụng để đo lường và phân tích những đặc tính sinh học, hành vi của con người, chẳng hạn như DNA, vân tay, mống mắt.

Từ nhiều nghiên cứu trước đây, các nhà khoa học đã nhận định rằng các đặc trưng sinh trắc có thể được sử dụng để nhận dạng, phân biệt con người. Các đặc trưng sinh trắc này thì thường mang tính duy nhất, và các đặc trưng này được sử dụng để nhận dạng và mô tả mang tính cá nhân. Từ thế kỷ thứ 16, người Trung Quốc đã sử dụng dấu vân tay, hoặc vân chân để xác định nhân dạng người dùng. Bằng cách sử dụng vân tay được bôi đen bằng mực, dấu vân tay này sẽ được sử dụng như đại điện cho một cá nhân. Ở phương Tây, việc sử dụng dấu vân tay cũng bắt đầu vào khoảng thế kỷ thứ 19 do nhu cầu về việc chống thoái thác trách nhiệm. Tuy nhiên, ngành khoa học về sinh trắc thực sự bắt đầu nghiên cứu vào cuối thế kỷ 19. Năm 1880, Henry Faulds đã đưa ra lý luận về số lượng vân tay để đánh giá mức độ phụ thuộc của vân tay vào gen di truyền. Năm 1868, Robert chỉ ra rằng mỗi ngón tay có một môi trường phát triển vi mô khác nhau. Vào nửa sau cuối thế kỷ 19, Richard Edward Henry đã phát triển phương pháp phân loại và nhận dạng dấu vân tay. Sau đó, Juan Vucetich đã tạo ra một hệ thống phân loại các đặc trưng sinh trắc cho các nước dùng tiếng Tây Ban Nha.

Năm 1870, nhà nhân loại học Alphone Bertillon đã tìm kiếm cách để xác định tội phạm. Ông ấy không chỉ dùng lòng bàn tay và bàn chân mà còn các cử động cơ thể và tất cả các dấu hiệu trên cơ thể. Những ý tưởng của ông đã trở nên phổ biến với các cảnh sát Anh và Mỹ để giúp giảm đi số lượng các nghi phạm. Điều thú vị đó là dấu vân tay, đặc trưng đươc sử dụng phổ biến nhất, cũng được Bertillon phát hiện, nhưng lại không được coi là quan trọng.

Năm 1880, Henry Fauld đã viết bức thư tới Charles Darwin để giải thích về một hệ thống phân biệt vân tay. Khi đó, Charles đã giới thiệu Francis Galton nhằm xây dựng hệ thống này nhưng thất bại. Phương pháp này được Francis Galton cải tiến vào năm 1892 và được sử dụng làm cơ sở thực nghiệm với độ tin cậy cao.

Vào khoảng đầu thế kỷ thứ 20, các đặc trưng sinh học bắt đầu được sử dụng rộng rãi và phổ biến. Năm 1903, nhà tù bang New York đã sử dụng một cách có hệ thống các dấu vân tay tại Mỹ với các tội phạm. Tuy nhiên, các phương pháp của Bertillon đã bị phát hiện lổ hỗng trong quá trình tìm kiếm tội phạm bởi hai người đàn ông song sinh. Dựa trên hệ thống phương pháp của Bertillon, hai người này có cùng các chỉ số và không thể phân biệt được Sau đó, dấu vân tay đươc sử dụng trong quân đội Mỹ.

Vào những năm 1960, các hệ thống nhận dạng dấu tay tự động bắt đầu được tạo ra. Cũng khoảng thời gian này, W. Bledsoe đã đề xuất các phương pháp nhận diện bằng khuôn mặt dựa trên vị trí mắt, mũi và miệng của các ảnh chụp. Sau đó, năm 1965, hệ thống nhận dạng chữ ký tự động cũng được nghiên cứu và áp dụng. Sau đó, các nhà nghiên cứu như Goldstein, Harmon và Lesk đã phát triển phương pháp nhận dạng mặt người vào năm 1980. Phương pháp này dựa trên việc sử dụng 21 đặc trưng cụ thể để tự động hóa việc nhận dạng khuôn mặt. Từ thời gian này, thuật ngữ sinh trắc (biometrics) bắt đầu được sử dụng để diễn tả các phương pháp nhận dạng người tự động dựa trên sinh trắc học. Năm 1983, học viện năng lượng Mỹ đã bắt đầu kiểm tra các đặc trưng sinh trắc tại phòng thí nghiệm quốc gia Sandia và trường nghiên cứu sau đại học Naval. Năm 1985, hệ thống quét tròng mắt đã được sử dụng cho việc truy cập vào văn phòng của trường Naval. Vào khoảng giữa những năm 1980, bang California đã thu thập dấu vân tay cho các ứng dụng xử lý bằng lái xe. Năm 1986, tổ chức quốc tế về nghiên cứu sinh trắc học ra đời. Năm 1990, hệ thống nhận dạng mống mắt do Daugman ở đại học Cambridge đề xuất. Những năm sau đó, các đặc trưng sinh trắc được sử dụng rộng rãi trong các hệ thống kiểm tra sự di chuyển dân cư vào năm 1992, hoặc hệ thống nhận dạng mạch máu tay ở Mỹ. Đến năm 2002, các tiêu chuẩn của đặc trưng sinh trắc được ra đời.

## Các đặc trưng sinh trắc

Theo các nghiên cứu của các nhà khoa học, các đặc trưng sinh trắc mang tính duy nhất, và dùng để phân biệt hoặc nhận dạng người dùng. Tuy nhiên, vì đặc trưng sinh trắc là những đặc điểm mang tính chất vật lý, hoặc hành vi của con người, nên dữ liệu về đặc trưng sinh trắc của con người rất đa dạng và phổ biến Một cách tổng quát, thường các đặc trưng sinh trắc con người có thể phân loại thành hai dạng: đặc trưng sinh lý và đặc trưng hành vi.

Các đặc trưng sinh lý của con người thường liên quan đến cơ thể của con người: như vân tay, mạch máu, DNA, mống mắt, hình dạng ngón tay… Các đặc trưng này khá bền vững với thời gian và mang tính chất tự nhiên. Các đặc trưng sinh trắc dạng này có thể là: vân tay, đặc trưng khuôn mặt, mí mắt, võng mạc, mạch máu, hình học bàn tay, hình học ngón tay, mùi, điện tâm đồ, DNA vành tai, mùi…

Các đặc trưng về hành vi là những khuôn mẫu liên quan đến hành vi của con người như dáng đi, chữ ký, giọng nói… Thường các đặc trưng này dễ bị thay đổi hơn nếu con người thay đổi môi trường sống xung quanh. Có thể kể đến như dáng đi, chữ ký, giọng nói…

Thông thường, việc nhận dạng con người thông qua các đặc trưng sinh học này sẽ đáng tin cậy hơn nhiều so với các biện pháp khác, và đây cũng là ứng dụng lớn nhất của đặc trưng sinh trắc hiện nay. Các biện pháp truyền thống để nhận dạng người dùng thường là các hệ thống nhận dạng chuỗi ký tự (token), chẳng hạn như bằng lái xe hay hộ chiếu, và các hệ thống nhận dạng dựa trên kiến thức như là mật khẩu hoặc số định danh cá nhân. Bởi vì các đặc trưng sinh học thì thường là mang tính duy nhất với mỗi cá thể, cho nên các đặc trưng này sẽ đáng tin cậy hơn so với các phương pháp định danh ký tự và hệ thống kiến thức khác. Ngoài ra, đối với ngành khoa học máy tính, việc nhận dạng con người thông qua các đặc trưng sinh học sẽ tiếp cận việc nhận dạng người dùng một cách tự nhiên hơn. Đối với máy tính, việc nhận dạng người là một phần quan trọng trong việc tương tác người máy, và từ thông tin này, máy tính có thể khai thác thêm những tính năng ưu việt khác như học thông tin về thói quen người dùng, các hành vi…

Một số ưu điểm dễ thấy của các đặc trưng sinh trắc như: người dùng có thể được nhận dạng bằng việc phải hiện diện thực tế tại thời điểm nhận dạng. Với người dùng, việc nhận dạng qua các đặc trưng này cũng không đòi hỏi phải nhớ mật khẩu hoặc mang theo các token. Tuy nhiên, các đặc trưng sinh trắc của con người rất đa đạng và phức tạp. Do đó, các đặc trưng sinh trắc được sử dụng để dùng trong các mục tiêu nhận dạng hoặc kiểm chứng phải thỏa mãn các yếu tố sau:

* Tính phổ biến: đặc trưng này để hiện diện trên mọi người và mang tính phổ biến, sự khiếm khuyết đặc tính này, nếu có, chỉ mang tính chất do tai nạn hoặc bệnh tật.
* Tính ổn định: những đặc trưng này cần phải ổn định, không thay đổi hoặc thay đổi rất ít theo thời gian và không gian. Do đó, các đặc trưng này không phụ thuộc vào tuổi tác, hoặc sức khỏe của người.
* Tính khả đo lường: các đặc trưng này phải phù hợp cho việc ghi nhận dữ liệu thời gian thực và dễ dàng so sánh.
* Tính duy nhất: việc rút trích, ghi nhận các đặc trưng này là phải duy nhất với các cá thể. Các đặc trưng này phải mang tính duy nhất đủ lớn để phân biệt người này với người khác. Chiều cao, cân nặng, màu tóc và màu mắt là những thuộc tính được coi là duy nhất trong vài trường hợp cụ thể, nhưng lại không cung cấp đủ sự khác biệt khi xem xét tập dữ liệu lớn hơn.
* Tính chấp nhận: việc thu nhận các dữ liệu sinh trắc phải thông qua sự chấp nhận của phần đông người dùng.
* Tính rút gọn: các dữ liệu thu thập được phải rút gọn được để dễ dàng xử lý.
* Tính đáng tin cậy: các đặc trưng này phải khó giả mạo bằng nhiều cách khác nhau. Đồng thời, quá trình xử lý các đặc trưng này phải đem lại độ tin cậy cao và có thể tái sử dụng nhiều lần.
* Tính riêng tư: quá trình xử lý, ghi nhận các đặc trưng này phải đảm bảo không vi phạm quyền riêng tư của người dùng.
* Tính dễ so sánh: các đặc trưng này nên dễ so sánh giữa người này với người khác.

Dựa trên những tính chất cần phải có trên, các đặc trưng sinh học có thể phù hợp với các điều kiện trên thường là dấu vân tay, đặc trưng khuôn mặt, giọng nói, mống mắt, tròng mắt, mạch máu, NDA, vân tay, chữ ký, giọng nói… Bảng 2.1 trình bày tổng hợp các tính chất của các đặc trưng sinh trắc.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Đặc trưng | Tính phổ biến | Tính duy nhất | Tính bền vững | Tính dễ thu thập | Tính hiệu quả | Tính chấp nhận | Khả năng chống gian lận |
| Khuôn mặt | Cao | Thấp | Trung bình | Cao | Thấp | Cao | Thấp |
| Vân tay | Trung bình | Cao | Cao | Trung bình | Cao | Trung Bình | Cao |
| Hình học  bàn tay | Trung bình | Trung bình | Trung bình | Cao | Trung bình | Trung bình | Trung bình |
| Cách gõ phím | Thấp | Thấp | Thấp | Trung bình | Thấp | Trung bình | Trung bình |
| Tĩnh mạch tay | Trung bình | Trung bình | Trung bình | Trung bình | Trung bình | Trung bình | Cao |
| Mống mắt | Cao | Cao | Cao | Trung bình | Cao | Thấp | Cao |
| Tròng mắt | Cao | Cao | Trung bình | Thấp | Cao | Thấp | Cao |
| Chữ ký | Thấp | Thấp | Thấp | Cao | Thấp | Cao | Thấp |
| Giọng nói | Trung bình | Thấp | Thấp | Trung bình | Thấp | Cao | Thấp |
| Biểu đồ nhiệt khuôn mặt | Cao | Cao | Thấp | Cao | Trung bình | Cao | Cao |
| Mùi | Cao | Cao | Cao | Thấp | Thấp | Trung bình | Thấp |
| DNA | Cao | Cao | Cao | Thấp | Cao | Thấp | Thấp |
| Dáng người | Trung bình | Thấp | Thấp | Cao | Thấp | Cao | Trung bình |
| Vành tai | Trung bình | Trung bình | Cao | Trung bình | Trung bình | Cao | Trung bình |

Bảng 2‑1 Tính chất các đặc trưng sinh trắc

* Dấu vân tay được sử dụng rất nhiều từ xưa tới nay. Điển hình nhất là ở Trung Quốc đã biết cách sử dụng dấu vân tay từ thời rất xa xưa. Kỹ thuật ghi nhận dấu vân tay thường là rút trích thành những điểm đặc trưng như điểm kết thúc gờ vân tay, vị trí nơi gờ vân tay chia thành nhiều đường, điểm vân tay… Điều này là nguyên nhân để tính hiệu quả của đặc trưng vân tay là rất cao. Để tăng tính chính xác, những đầu đọc vân tay thường chủ yếu dựa vào quang học, nhiệt độ, silicon hoặc sóng siêu âm. Trong đó, đầu đọc quang học, hoạt động dựa trên nguyên lý sự phản xạ ánh sáng bị thay đổi tại vị trí vân tay chạm vào là phổ biến nhất. Còn với đầu đọc bằng silicon thì ra đời đầu tiên. Hoạt động của đầu đọc này là bộ cảm ứng điện dung đo dòng điện từ ngón tay đặt vào. Do các vân tay lồi ra, nên sẽ có điện dung cao hơn và ngược lại, các rãnh giữa các vân tay có điện dung thấp. Tuy nhiên, yếu tố điện dung của ngón tay lại bị ảnh hưởng rất nhiều vào độ ẩm của ngón tay. Do đó, độ chính xác của phương pháp này là kém nhất. Còn đối với đầu đọc vân tay siêu âm thì đây là phương pháp mới nhất, chính xác nhất nhưng lại có chi phí hoạt động cao. Một cách tổng quát, hầu hết các tính chất của đặc trưng vân tay là khá cao như ở Bảng 2.1, nên đặc trưng này rất phổ biến để sử dụng trong thực tế. Từ những hệ thống tính thời gian, xét quyền truy cập đến kiểm tra định danh đều có thể áp dụng phương pháp này.
* Mống mắt là vòng màu của dải mô xung quanh con ngươi của mắt. Đây là đặc trưng thỏa mãn rất cao các yếu tố để phân biệt người dùng. Thậm chí, với những cặp song sinh có dấu vân tay khá giống nhau, thì đặc trưng mống mắt lại rất khác nhau. Bên cạnh đó, việc đánh giá và phân biệt người dùng với cơ sở dữ liệu là rất dễ dàng mà không phụ thuộc quá nhiều vào các yếu tố ngoại cảnh. Các máy quét mống mắt hoạt động trong điều kiện thiếu sáng rất hiệu quả.
* Giọng nói: đây là một đặc trưng rất phổ biến, được người dùng rất ưa chuộng nhưng lại không được hiệu quả. Hầu hết các chỉ số thỏa mãn các tính chất đặc trưng sinh trắc đều khá thấp như ở Bảng 2.1. Việc xử lý đặc trưng này chủ yếu dựa vào quang phổ ghi nhận được từ các thiết bị thu âm. Tuy nhiên đặc trưng này có tính hiệu quả phụ thuộc rất nhiều vào chất lượng các yếu tố âm thanh, chất lượng thiết bị ghi âm, sức khỏe người dùng, tính chất vùng miền. Một cách tổng quát, nhận diện giọng nói của người dùng có thể chia làm hai phương pháp: phương pháp phụ thuộc vào văn bản và phương pháp độc lập văn bản. Phương pháp độc lập văn bản là phương pháp hoạt động không cần văn bản. Còn phương pháp phụ thuộc văn bản là đòi hỏi người dùng đọc văn bản.

## Hệ thống sử dụng đặc trưng sinh trắc

Thông thường, các hệ thống nhận dạng bằng đặc trưng sinh trắc là các hệ thống nhận dạng khuôn mẫu được định danh bởi người dùng bằng việc xác định những đặc trưng vật lý hoặc hành vi cụ thể của người dùng. Do đó, các công nghệ sinh trắc học được định nghĩa là một hệ thống tự động nhận diện hoặc phân quyền một người sống dựa trên các đặc trưng về vật lý hoặc hành vi. Các hệ thống sinh trắc học có thể là hệ thống nhận dạng người dùng hoặc phân quyền người dùng:

Hệ thống nhận dạng người dùng (một với nhiều): các sinh trắc học được sử dụng để xác định danh tính người dùng mà không cần người dùng cung cấp kiến thức. Chẳng hạn, việc camera quét qua đám đông cùng với công nghệ nhận dạng khuôn mặt, hệ thống có thể xác nhận người dùng với một cơ sở dữ liệu cho trước.

Hệ thống phân quyền người dùng (một với một): Các đặc trưng sinh trắc học được sử dụng để xác nhận lại danh tính người dùng. Ví dụ, hệ thống có thể cấp quyền truy cập vào một khu vực bảo mật trong tòa nhà bằng việc sử dụng dấu vân tay hoặc cấp quyền truy cập vào tài khoải ngân hàng tại ATM bằng việc quét tròng mắt.

Việc nhận dạng đặc trưng sinh trắc đòi hỏi phải so sánh với các mẫu sinh trắc học đã được đăng ký hoặc cung cấp từ trước với một mẫu mới. Do đó, đây là một quá trình gồm ba bước: ghi nhận, xử lý và đăng ký cơ sở dữ liệu tùy thuộc và quá trình xử lý nhận dạng hoặc kiểm chứng người dùng.

Trong suốt quá trình ghi nhận, dữ liệu đặc trưng sinh trắc sẽ được thu thập dưới dạng dữ liệu thô bằng các cảm biến, hoặc thiết bị. Chẳng hạn, với giọng nói là các ảnh phổ bằng thiết bị ghi âm. Ở giai đoạn thứ hai, quá trình xử lý sẽ bắt đầu bằng việc rút trích các đặc trưng từ các dữ liệu sinh trắc thô và đưa vào quá trình xử lý nhận dạng. Cuối cùng là giai đoạn đăng ký với việc biểu diễn các dữ liệu này dưới dạng toán học và lưu trữ vào các cơ sở dữ liệu.

## Kết chương

Nội dung chương này trình bày tổng quan về việc chứng thực người dùng sử dụng đặc trưng sinh trắc học. Trong Chương 3, chúng tôi sẽ trình bày tập trung về việc định danh người dùng với một loại đặc trưng sinh trắc học mới: đặc trưng dáng đi.

# Tổng quan về việc định danh người dùng bằng đặc trưng dáng đi

**Tóm tắt chương:**

*✍ Trong Chương 3, chúng tôi trình bày tổng quan về việc định danh người dùng bằng đặc trưng dáng đi, bao gồm các hướng tiếp cận chính, cách thiết lập sensor ghi nhận thông tin và thu thập dữ liệu, các bước tiền xử lý, phân đoạn, các phép biến đổi và quy trình nhận dạng*

## Mở đầu

Bên cạnh các loại đặc trưng sinh trắc học xuất phát từ hệ thống tính toán thông thường và được đưa vào thiết bị, việc nghiên cứu các đặc trưng sinh trắc học khác sử dụng ***thông tin về người dùng được ghi nhận từ các cảm biến của thiết bị*** là một hướng mới, hiện đang được quan tâm nghiên cứu và phát triển trên thế giới.

Các đặc trưng truyền thống ra đời và được nghiên cứu độc lập với sự ra đời và phát triển của thiết bị di động hay thiết bị đeo. Vì vậy, các giải pháp chứng thực dùng đặc trưng truyền thống thường ít mang tính đặc thù dành riêng cho thiết bị di động hay thiết bị đeo. Trong khi đó, các đặc trưng sinh trắc học mới thường khai thác các đặc tính riêng của thiết bị, cụ thể là ***khả năng ghi nhận ngầm thông tin về người dùng một cách thường trực của thiết bị***.

**Dáng chuyển động** (*gait*) là một loại đặc trưng sinh trắc học mới trong việc chứng thực trên thiết bị, khai thác thông tin về chuyển động của một bộ phận hay toàn bộ cơ thể người dùng để nhận biết và phân biệt người dùng qua các đặc điểm riêng khi di chuyển (*gait authentication*). Loại đặc trưng này gắn liền với các cảm ứng chuyển động thường được tích hợp sẵn trong hầu hết các thiết bị di động và thiết bị đeo, không đòi hỏi phải tích hợp thêm các thiết bị bổ sung như camera, thiết bị chụp ảnh mống mắt hay thiết bị lấy vân tay.

Tính chất *gait* là đặc trưng cho dáng đi mỗi người trong một khoảng thời gian [1]. Loại đặc trưng này được đánh giá là khả thi dùng để định danh giữa những người khác nhau và phù hợp hơn các phương thức khác trên điện thoại [2][3]. Đặc trưng dáng chuyển động định danh cho mỗi người bởi đặc trưng này phụ thuộc vào thói quen di chuyển, đặc điểm cơ thể như cấu tạo cơ xương cũng như chỉ số cân nặng, chiều cao[4][5] cũng như yếu tố về tâm lý học [6].

Quy trình nhận biết dáng chuyển động thường bao gồm các công đoạn sau:

* ***Thu thập và xử lý tín hiệu***

Giai đoạn này bao gồm các bước nội suy tín hiệu để được một tần số ổn định,và các bộ lọc để khử nhiễu tín hiệu. Đối với các thiết bị sử dụng cảm biến đo hướng, tín hiệu của thiết bị được quy chiếu về các hệ trục tọa độ cố định vì trong quá trình sử dụng, các thiết bị này có thể bị sai lệch.

* ***Phân tách tín hiệu***

Giai đoạn này bao gồm việc phân tách các tín hiệu vào các khung thời gian cố định để tiện lợi cho việc rút trích thông tin. Độ dài cho các khung thời gian được thí nghiệm với các khoảng khác nhau để tìm ra giá trị tối ưu nhất dựa vào đặc điểm của tín hiệu.

* **So khớp và phân lớp**

Trong hướng tiếp cận Matching Method, các tín hiệu trong các khung thời gian được sử dụng để tìm ra các bộ mẫu tốt nhất, các bộ này thể hiện rõ nét các đặc điểm di chuyển “gait” của người dùng. Khi có tín hiệu mới, tín hiệu này được so sánh với các bộ mẫu của người chủ thiết bị để xác nhận. Hướng đề cập này dựa trên các phương pháp như khoảng cách Euclide [9], auto-correlation [8], láng giềng gần nhất [10], Dynamic Time Warping (DTW) [11][7].

Chứng thực người dùng với đặc trưng dáng chuyển động có thể được sử dụng kết hợp với các chứng thực bằng các đặc trưng sinh trắc học khác để tạo ra giải pháp an toàn, chống lại tấn công giả mạo đối với cách chứng thực bằng đặc trưng sinh trắc học truyền thống. Ngoài ra, đặc trưng dáng chuyển động sẽ phù hợp cho việc chứng thực trên các thiết bị không có màn hình để nhập mật khẩu hay mã PIN, cũng như không có các thiết bị tiếp nhận thông tin khác như camera, bộ phận đọc vân tay hay chụp ảnh mống mắt.

Do mới bắt đầu được nghiên cứu trong khoảng 5 năm gần đây nên các công trình nghiên cứu hiện nay còn một số hạn chế sau:

* Mỗi công trình nghiên cứu sử dụng bộ dữ liệu thử nghiệm tự xây dựng với quy mô còn giới hạn (dưới 50 người), chưa sử dụng bộ dữ liệu chung để đánh giá và so sánh.
* Việc chứng thực người dùng chỉ mới xét trong tình huống người dùng bước đi bình thường (*walk*), chưa xét các tình huống khác như khi người dùng chạy (*run*) hay đi nhanh (*jog*).
* Các công trình nghiên cứu chủ yếu tập trung vào việc đề xuất phương pháp phân biệt để nhận biết người dùng dựa vào thông tin chuyển động, chưa xem xét các tình huống bị tấn công và chưa đề xuất quy trình chặt chẽ để chứng thực người dùng bằng đặc trưng dáng chuyển động. Ví dụ như như cần hủy bỏ thông tin định danh đang có khi người dùng đột ngột thay đổi dạng chuyển động để tránh việc người dùng bị lấy mất thiết bị đeo hay thiết bị di động…

## Các hướng tiếp cận chính

Đặc trưng dáng đi (gait) thường được xác định và phân tích theo hai cách tiếp cận chính sau đây:

* **Phân tích dựa vào tham số sinh lý của dáng đi**: ước lượng tường minh các tham số sinh lý của dáng đi, ví dụ như các tham số không-thời gian (nhịp, độ dài bước chân, tính đối xứng trong dáng đi, khoảng cách trong giữa hai bàn chân…) [B15], xác định pha của dáng đi [B5] hay tham số động học (góc ở khớp) [B4][B16]. Các phương pháp theo hướng tiếp cận này tập trung khai thác các tính chất sinh lý trong việc chuyển động nên phù hợp cho việc phép khảo sát và phân tích hoạt động của từng bộ phận cơ thể tham gia trong quá trình chuyển động.
* **Phân tích dựa vào rút trích đặc trưng**: sử dụng các phương pháp rút trích đặc trưng đặc biệt để tạo ra các thông tin đặc thù từ dữ liệu dáng đi. Trong nhóm phương pháp này, dữ liệu dáng đi sẽ được biến đổi bằng các phép biến đổi dữ liệu khác nhau để tạo ra các loại đặc trưng cho dáng đi khác nhau. Do nhóm phương pháp này chủ yếu dựa trên việc xử lý và biến đổi dữ liệu, không phải dựa vào phân tích đặc điểm sinh lý của chuyển động và dáng đi, các đặc trưng được trích ra từ các phương pháp này thường không mang ngữ nghĩa trực tiếp là các thuộc tính sinh lý của chuyển động.

Việc nhận dạng dáng chuyển động thường tập trung vào chuyển động trong ***điều kiện đi lại tự nhiên thường ngày***: đi trên đoạn đường thẳng, bằng phẳng với nhịp chân và khoảng cách bước chân bình thường. Tần số bước chân thông thường từ 0.7-0.75 Hz đến 1.35-1.51Hz [13][14]. Tuy nhiên, dáng đi tự nhiên có thể bị tác động của nhiều nhân tố khác nhau, bao gồm nhân tố sinh lý và nhân tố môi trường [72], tạo ra các sai khác nhỏ trong dáng đi, hoặc thậm chí làm thay đổi đáng kể các mẫu trong dáng đi.

* **Nhân tố sinh lý**: dáng đi có thể bị thay đổi dần dần mà bản thân con người không chủ ý tạo ra và cũng không ý thức về việc đang thay đổi dần một số đặc trưng/mẫu dáng đi. Những thay đổi này có thể vĩnh viễn (ví dụ như những chấn thương hay bệnh mãn tính), thay đổi theo thời gian (ví dụ như chấn thương tạm thời, bệnh không mãn tính, theo cảm xúc, các nhân tố về tuổi tác, sức khỏe, thời tiết…). Dáng đi cũng có thể bị thay đổi do con người chủ động tập luyện.
* **Nhân tố môi trường**: bao gồm những nhân tố có ảnh hưởng trực tiếp hay gián tiếp làm thay đổi mẫu dáng đi của một người, ví dụ như quần áo, giày dép, bề mặt đường đang di chuyển, góc nghiêng của đường đi, chướng ngại vật…

Ý tưởng nhận biết dáng chuyển động với thông tin sensor đã được đề xuất hơn 30 năm trước [15]. Những thử nghiệm đầu tiên đã tập trung quan sát chuyển động của cơ thể dựa trên ánh sáng của các đèn được đính trên các khớp của người di chuyển. Sau đó, các nghiên cứu dựa trên hình ảnh ghi nhận từ camera được quan tâm nghiên cứu. Đặc biệt trong thời gian gần đây, với sự phát triển của các sensor cho phép có thể ghi nhận lại tín hiệu chuyển động, giúp mở ra khả năng nhận biết người dùng từ dáng đi với thông tin ghi nhận từ sensor chuyển động.

Các phương pháp này có thể được chia thành các nhóm sau: (a) sử dụng thông tin hình ảnh ghi nhận từ video [16], (b) sử dụng thông tin ghi nhận từ sensor trên sàn nhà [17], sử dụng thông tin ghi nhận từ sensor đeo trên người [17].

Việc nghiên cứu sử dụng thông tin từ sensor chuyển động để nhận biết dáng đi bắt đầu được quan tâm từ đầu thế kỷ 21, và đặc biệt trong 5 năm gần đây. Từ những công trình đầu tiên do Ailisto và Mantyjarvi [18][19], Gafurov [20] , các nghiên cứu trong 5 năm gần đây trên thiết bị thông minh ngày càng phát triển mạnh

## Thiết lập sensor và thu thập dữ liệu

Thông tin quán tính của dáng đi có thể đo đạc được bằng cách sử dụng các sensor quán tính thiết lập theo 2 cấu hình sau: sử dụng sensor độc lập hoặc sensor tích hợp vào các thiết bị thông minh đang có trên thị trường. Cách thứ nhất được dùng với mục tiêu làm thí nghiệm với 3 tham số thu thập dữ liệu như sau: tần suất lấy mẫu, phạm vi và độ phân giải đo lường. Những tham số này cần được cân nhắc do quá trình xử lý tín hiệu tiếp theo nhằm tránh những trường hợp bị nhiễu và sai lệch dữ liệu không mong muốn có thể làm ảnh hưởng tới hình dạng của dáng đi (ví dụ: nhiễu răng cưa, lỗi của phép cắt hoặc phép lượng tử - quantization). Bên cạnh đó, các thiết bị sensor độc lập cho phép chúng ta thí nghiệm với các cấu hình cài đặt sensor bất kỳ để từ đó có thể ứng dụng nhằm kiểm tra sự ảnh hưởng của sensor đối với việc nhận dạng (ví dụ: vị trí, hướng quay) [21][22][23].

Một trong những câu hỏi nghiên cứu quan trọng nhất là liệu chúng ta có thể thay thế những cấu hình sensor đặc biệt bằng những thiết bị thông minh đang có rộng rãi trên thị trường đồng thời thích ứng với những hạn chế xảy ra trong quá trình sử dụng thông thường hay không. Sprager et al. [24] cùng với những nhóm khác [25][26][27] đã có báo cáo về những thành công đầu tiên của việc nhận biết dáng đi dựa trên dữ liệu thu thập được từ smartphone. Không giống như những cấu hình độc lập, các sensor quán tính được tích hợp vào bảng mạch ở nhiều vị trí và đặt bên trong các thiết bị thông minh tùy thuộc vào các model và nhà sản xuất khác nhau. Nhằm lấy dữ liệu quán tính theo một cách thống nhất, các tham số thu thập dữ liệu đều được điều khiển và quản lý bởi API của sensor; điều này cho phép các lập trình viên ứng dụng có thể lựa chọn tốc độ lấy mẫu theo ý mình. Chúng ta cũng mong muốn đảm bảo được hiệu năng và tuổi thọ của pin dài hơn bằng cách lấy mẫu dữ liệu với tốc độ càng thấp càng tốt. Ngoài ra, tốc độ lấy mẫu thường phụ thuộc và thay đổi theo thời gian, vì vậy cần phải thực hiện thêm các bước khác để đảm bảo khoảng cách bằng nhau giữa các khoảng thời gian lấy mẫu, phục vụ cho việc tính toán sau này. Việc này thường được thực hiện bằng phép nội suy tuyến tính hoặc cubic [24][25][26][27]. Tuy nhiên, tốc độ lấy mẫu cũng phải vừa đủ cao để có thể đối phó với các sự thay đổi xuất hiện trong dữ liệu quán tính trong lúc di chuyển. Hầu hết các bài báo khoa học đã báo cáo rằng đối với một dáng đi tự nhiên, chúng ta chỉ cần thiết lập tốc độ lấy mẫu trong khoảng trên vài chục Hz là đủ. Trong một số dự án nghiên cứu đầu tiên, các nhà nghiên cứu đã thí nghiệm với tốc độ lấy mẫu khá cao, tầm 250 Hz [18][19][29][30]. Trong những năm tiếp theo, hầu hết các phương pháp sử dụng sensor độc lập đều dùng tốc độ lấy mẫu trong khoảng từ 50 đến 100 Hz [21][23][31][32]. Tương tự, các phương pháp sử dụng smartphone đã dùng tốc độ lấy mẫu dưới 100 Hz, trong đó các phương pháp hiệu quả nhất thậm chí chỉ sử dụng tốc độ lấy mẫu khá thấp, gần 25 Hz [33][34][35].

Thông tin quán tính của dáng đi thường được ghi nhận bằng hai loại sensors: gia tốc kế và con quay hồi chuyển. Như chúng ta có thể nhận thấy, phần lớn các phương pháp đều sử dụng dữ liệu từ gia tốc kế, bởi vì thông tin dáng đi thường được phản ánh tốt thông qua việc đo lường gia tốc. Mặt khác, cũng đã có nhiều hướng tiếp cận nhằm giải quyết bài toán nhận biết dáng đi chủ yếu dựa vào thông tin về vận tốc góc [31][34][36], cách làm này dẫn đến kết quả nhận dạng không được tốt khi so sánh với phương pháp sử dụng thông tin gia tốc. Tuy nhiên, việc sử dụng con quay hồi chuyển cũng có mang lại những đóng góp quan trọng, như việc đề ra phương pháp sử dụng kết hợp giữa gia tốc kế và con quay hồi chuyển (như IMU), nhằm để giải quyết vấn đề sai lệch hướng quay hoặc thực hiện việc nhận dạng kết hợp hai loại thông tin. Phạm vi đo lường gia tốc thường thấy trong việc nhận diện dáng đi là trong khoảng từ +- 2 đến +- 8g, trong khi đó phạm vi đo lường vận tốc góc quay đo đạc bởi con quay hồi chuyển thường trong khoảng từ +- 150 độ đến +- 2000 độ trên 1 giây. Về độ phân giải đo lường, dữ liệu quán tính được số hóa bằng máy chuyển đổi tín hiệu analog sang digital (A/D converter) thường trong khoảng từ 8 đến 12 bit.

Dữ liệu quán tính có thể được thu thập bằng tín hiệu đơn biến, đa biến, hoặc sử dụng nhiều sensor. Tín hiệu đơn biến được sử dụng hầu hết bởi các phương pháp nhận dạng dáng đi đầu tiên dựa trên smartphones, vì độ lớn gia tốc có thể được tính bằng cách biến đổi các phép đo gia tốc đa biến. Cách thức biểu diễn đơn biến này khá phổ biến vì nó mang lại sự bất biến về phép quay đối với việc giảm thiểu đáng kể sự khác nhau của kiểu dáng đi. Tín hiệu đơn biến đồng thời cũng là giá trị trả ra của phép đo lường sử dụng sensor quán tính đơn trục trong điều kiện không gian đơn chiều. Phần lớn các phương pháp nhận biết dáng đi đã được cải thiện đều sử dụng phép đo đa biến, thu thập được từ gia tốc kế ba chiều một cách tự động hoặc kết hợp với con quay hồi chuyển ba chiều. Đối với phương pháp state-of-the-art bây giờ, việc sử dụng nhiều sensor quán tính đã được áp dụng với mục đích thí nghiệm nhằm kiểm tra sự ảnh hưởng của vị trí đặt sensor đối với kết quả nhận dạng. Tuy nhiên, những phương pháp này cũng có thể được sử dụng khi ý tưởng kết hợp nhiều thiết bị sensor đeo trên người (ví dụ: body area network) có thể đưa vào ứng dụng, vì nhiều nghiên cứu đã cho thấy việc sử dụng kết hợp các sensor đã làm tăng đáng kể sự hiệu quả của quá trình nhận dạng [34][35][36].

## Tiền xử lí

Sau khi thu thập dữ liệu, việc tiền xử lí chúng được đề xuất bởi một vài hướng tiếp cận hiện thời đối với bài toán nhận biết dáng đi. Bước khởi đầu này được thực hiện nhằm mục đích chuẩn bị kĩ lưỡng các dữ liệu quán tính thu thập được cho các quá trình xử lí tiếp theo, như là loại bỏ các dữ liệu nhiễu bằng cách áp dụng các cách lọc dữ liệu, hay là rút trích ra nhiều đoạn nhỏ dữ liệu nhưng vẫn đảm bảo đủ thông tin phân biệt dáng đi của người dùng, phù hợp để xử lí hiệu quả hơn.

### Lọc dữ liệu

Trong lớp bài toán xử lí tín hiệu, bộ lọc đóng vai trò là một trong những bước quan trọng nhất để loại bỏ dữ liệu nhiễu. Sử dụng bộ lọc cũng được áp dụng bởi một số hướng tiếp cận hiện thời trong bài toán nhận diện dáng đi, khi mà dữ liệu nhiễu được phát hiện là những tín hiệu với tần số cao được sản sinh từ nhiều nguồn (như đeo thiết bị bị lỏng, lỗi đặt vị trí, v.v..). Vì vậy, một số hướng tiếp cận đã áp dụng bộ lọc moving average [38][43], hoặc phân tách và tái tạo sóng nhiều lớp [44][45] để loại bỏ các phần nhiễu đó. Một số phương pháp cũng áp dụng zero-normalization để loại bỏ thông tin trọng trường khỏi tín hiệu gia tốc [39][46]. Cách làm này có thể thực hiện được nếu như sensor được đặt ngay ngắn với chiều ngang và chiều dọc của hệ thống GPS. Để phát hiện giá trị góc quay lệch, bộ lọc moving average với cửa số trượt dài cũng được sử dụng [28]. Về cơ bản, việc sử dụng bộ lọc là để giải quyết những khó khăn xuất phát từ các yếu tố ảnh hưởng của sensor đối với dáng đi. Tuy nhiên, những hướng tiếp cận đó vẫn còn khá hạn chế và không vững vàng, vì vậy bài toán đó cần được giải quyết bằng 1 phương pháp mang tính hệ thống hơn.

### Phát hiện dáng đi và nhận biết hành động

Khi quan sát chuyển động của cơ thể con người từ một góc nhìn thực tế, những giai đoạn sau sẽ xuất hiện lặp đi lặp lại trong dữ liệu quán tính ta thu thập được: di chuyển (dáng đi), đứng yên (chịu ảnh hưởng của tư thế) và những hoạt động còn lại, bao gồm sự chuyển tiếp giữa các giai đoạn hoặc dữ liệu nhiễu (tap lên màn hình, quá trình đeo thiết bị vào cơ thể, v.v..). Từ góc nhìn dựa trên phương pháp, những phần tương ứng với giai đoạn di chuyển cần được phát hiện từ dữ liệu quán tính. Các giai đoạn còn lại không được sử dụng cho việc nhận biết dáng đi và có thể được lược bỏ. Tại đây, chúng ta có thể nhận thấy quá trình này khá gần giống với bài toán nhận dạng hành động mà ta có thể giải quyết bằng cách sử dụng chủ yếu dữ liệu quán tính, kết hợp với sử dụng phương pháp cửa sổ chạy. Theo cách này, các phương pháp nhận biết hành động có thể được áp dụng vào một phần của việc tiền xử lí dữ liệu trong bối cảnh tương tự đối với bài toán nhận biết dáng đi dựa trên sensor quán tính.

Việc rút trích các đoạn từ dữ liệu quán tính có chứa thông tin dáng đi được thực hiện bởi các phương pháp nhận biết dáng đi hiện tại bằng 3 cách khác nhau: thủ công (làm bằng tay), tự động, hoặc thực hiện ngầm như một phần trong chu kỳ phát hiện dáng đi trong quá trình phân đoạn. Do tính chất ổn định về chu kỳ của dáng đi, cách thực hiện ngầm được chú ý đặc biệt bằng cách sử dụng các tính chất positive (rõ ràng). Tuy nhiên, phần lớn các phương pháp đã có, đặc biệt là các phương pháp đầu tiên đều đã sử dụng phép rút trích thủ công, khi mà mục tiêu chính của bài toán lúc đó chỉ mới là đánh giá khả năng của phương pháp, và tính ứng dụng trong đời thực chưa được quan tâm đến. Bằng cách phát hiện thủ công, dữ liệu quán tính được quan sát bằng mắt và những phần có chứa thông tin dáng đi được chú thích một cách dễ dàng nhờ vào tính chất tuần hoàn và hình dạng xác định. Mặt khác, vì việc phát hiện một cách tự động các phần có thông tin dáng đi là cần thiết nhằm ứng dụng vào thực tế, một số phương pháp gần đây đã ứng dụng các phương thức xử lí tín hiệu và nhận biết pattern (mẫu) cơ bản, ví dụ như áp dụng phương thức moving window [33], phân loại bằng decision trees (cây quyết định) dựa vào các đặc trưng cơ bản [28] và giới hạn quỹ đạo di chuyển cũng như signal autocorrelation [27].

## Phân vùng

Phân vùng là một quy trình trong đó dữ liệu quán tính thu thập được sẽ bị chia thành nhiều phần nhỏ hơn. Những thành phần này sẽ phù hợp cho những bước xử lý tiếp theo. Khi xem xét khả năng áp dụng vào thực tế của các phương pháp nhận dạng bằng cảm biến quán tính, hai khía cạnh quan trọng cần có là: độ phức tạp tính toán phải thấp và độ trễ khi nhận dạng phải thấp. Những điền kiện này có thể được thỏa mãn bởi các hướng tiếp cận mà trong đó hiệu suất nhận dạng được bảo toàn kể cả khi phải xử lý những dáng đi có chu kỳ rất ngắn (vài giây) lấy được từ một lần đi thử duy nhất. Thao tác phân vùng rất phù hợp, đặc biệt khi ta xét đến việc dáng đi có tính lặp lại theo một chu kỳ nhất định. Vì thế, dữ liệu quán tính thu được trong dáng đi có thể được chia thành nhiều chu kỳ. Một chu kỳ dáng đi có được là do đặc tính trong chuyển động của hai chân người và được định nghĩa bằng khoảng thời gian kể từ lúc một chân mới chạm vào mặt đất cho đến khi chân đó chạm đất trở lại. Một vài phương pháp nhận dạng dáng đi lại không áp dụng các hướng tiếp cận dựa trên chu kỳ mà thao tác trực tiếp trên những frame có độ dài cố định.

### Các hướng tiếp cận dựa trên chu kỳ

Các quy trình phát hiện chu kỳ là nền tảng cho việc ước lượng tốc độ của dáng đi [B9], và cũng có thể được dùng trong việc nhận dạng dáng đi. Trong dữ liệu quán tính, các chu kỳ dáng đi được thể hiện bởi các khuôn mẫu lặp đi lặp lại. Một giai đoạn sẽ đại diện cho một chu kỳ dáng đi; hoặc là một bước đi trong trường hợp mà cảm biến được gắn ở một vị trí đối xứng qua trục đứng của cơ thể(ví dụ như là ở chính giữa lưng). Không giống như các hướng tiếp cận dựa trên khung ảnh, các hướng tiếp cận dựa trên chu kỳ cho phép ta có thể phân tích từng chu kỳ dáng đi cụ thể. Các quy trình canh chỉnh xử lý các biến dạng theo thời gian trong các mẫu dáng đi, các biến dạng này là hệ quả của các yếu tố ảnh hưởng đến dáng đi (ví dụ như biến thiên tốc độ của dáng đi). Tuy nhiên, ta cần phải xét tới việc hiệu suất nhận dạng phụ thuộc trực tiếp vào khả năng của quy trình nhận dạng dáng đi. Bên cạnh đó, việc canh chỉnh các chu kỳ cũng có thể dẫn đến những thay đổi rất lớn trong hình thái của mẫu dáng đi.

Hiện giờ, các phương pháp nhận dạng dáng đi dựa trên chu kỳ phụ thuộc vào các phương thức phát hiện dáng đi có tận dụng việc phân tích cực đại địa phương [18][19][24][25][38], cùng với phát hiện **zero-crossing** [20][29][30][46], phát hiện vector trọng tâm [49][50], phân tích giai đoạn [22][31], phát hiện biến đổi động [51], và hệ số tương quan [36][44][48]. Sau khi đã phát hiện chu kỳ dáng đi, độ dài của các chu kỳ dáng đi sẽ được thống nhất. Ta thống nhất chúng bằng cách chuẩn hóa độ dài, hoặc là bằng quy trình canh chỉnh. Việc chuẩn hóa độ dài cho ra các chu kỳ dáng đi có độ dài bằng nhau, trong đó hình dạng của mẫu dáng đi sẽ không thay đổi. Việc này được thực hiện bằng phép nội suy tuyến tính [24][38][46] hoặc nội suy cubic-spline [40]. Mặt khác, việc canh chỉnh sẽ ảnh hưởng đến cấu trúc thời gian của mẫu dáng đi nhằm mục đích là để thực hiện so khớp tối ưu hai chu kỳ. Hầu hết các phương pháp dựa trên canh chỉnh chu kỳ hiện giờ sử dụng quy trình Dynamic Time Warping (DTW) [25][29][30][32], hay quy trình tương tự nhưng phức tạp hơn là phase-based self-DTW [22][31].

### Phương pháp dựa trên frame

Khác với phân vùng dựa trên chu kỳ, các hướng tiếp cận dựa trên frame không đòi hỏi bất kỳ quy trình xử lý bổ sung nào vì dữ liệu quán tính thu được bị chia thành những khoảng chồng lên nhau hoặc tách rời nhau. Những hướng tiếp cận này cũng bảo toàn hình thái của mẫu dáng đi. Tuy nhiên, việc phân vùng theo frame không kiểm soát được thông tin về chu kỳ dáng đi, và đồng thời cũng không xử lý được biến dạng theo thời gian trong các mẫu dáng đi. Nhiều phương pháp nhận dạng dáng đi hiệu quả phụ thuộc vào phân vùng theo frame mà trong đó có xét tới nhiều độ dài frame khác nhau. Ta dễ thấy rằng các phương pháp nhận dạng dáng đi dựa trên frame phải xét ngưỡng chặn dưới xác định bởi tốc độ dáng đi kỳ vọng thấp nhất mà ta đã biết trước. Ta giả định rằng một frame phải chứa ít nhất một chu kỳ dáng đi hoàn chỉnh. Các hướng tiếp cận được đánh giá với các độ dài frame thường gặp như: thời gian kỳ vọng dài nhất của chu kỳ dáng đi dưới 3 giây [33][35][39], từ 3 đến 5 giây [33][35][39], từ 5 đến 15 giây [27][28][35].

Tuy nhiên, một vài hướng tiếp cận, đặc biệt là những hướng dựa trên máy học, thí nghiệm với phân vùng nhỏ hơn, trong đó từng phân vùng có độ dài ngắn hơn chu kỳ dáng đi kỳ vọng lớn nhất. Mặc dù vậy, các chu kỳ dáng đi hoàn chỉnh sẽ được xem xét trong quá trình học vì tất cả các mảnh phủ hết một chu kỳ được cho vào bộ training. Thêm vào đó, ta cần chú ý rằng một vài hướng tiếp cận xuất hiện gần đây có thể thực thi hiệu quả kể cả khi không dùng các quy trình phân vùng đặc biệt vì việc này đã được xử lý ngầm bằng phép chuyển đổi sang không gian đặc trưng, hoặc trong quy trình nhận dạng.

## Biến đổi mẫu dáng đi

Một bước quan trọng trong mỗi phương pháp nhận dạng dáng đi là việc mô tả các mẫu dáng đi theo một cách phân biệt, nhằm hỗ trợ cho việc nhận dạng có hiệu quả ở bước tiếp theo. Như đã giải thích ở Phần 3, mẫu dáng đi của từng cá nhân được xác định bởi việc ước lượng các tham số dáng đi, thể hiện thông qua sinh lý học hay ngầm hiểu trong các đặc trưng. Do tính đơn giản và hiệu quả của nó, các đặc trưng trở thành cách thuận tiện nhất để tạo ra những mẫu dáng đi đủ khác biệt. Việc này cũng đã được xác nhận bởi quá trình phê duyệt. Qúa trình phê duyệt cho thấy rằng đại đa số các hướng tiếp cận hiện nay tận dụng việc chuyển đổi qua không gian đặc trưng. Các mẫu dáng đi thể hiện bằng đặc trưng có thể được thu thập bằng 3 cách: (a) xây dựng mẫu dáng đi trong bước phân vùng; (b) tính toán đặc trưng chung và (c) các cách rút trích đặc trưng cấp cao.

Trong cách đầu tiên, mẫu dáng đi vẫn giữ thông tin rõ rang về dữ liệu quán tính. Nền tảng để tạo ra mẫu dáng đi là chu kỳ dáng đi hoặc là frame thu được từ quy trình phân vùng. Những mẫu này có thể được truyền trực tiếp tới quy trình nhận dạng dưới dạng những phân khúc không đổi [18][29], hoặc là có thể được xử lý thêm nữa. Một trong những cách đơn giản mà hiệu quả nhất là xác định chu kỳ dáng đi trung bình [25] [30][38] rút trích từ các chu kỳ đã được phân mảnh dưới dạng một chu kỳ dáng đi duy nhất được dùng làm mẫu trong quá trình nhận dạng. Trong cách khác, đặc trưng chung mô tả các mẫu dáng đi bằng cách tính toán các tham số đơn giản, thường là về thời gian, tần suất hoặc các tham số thống kê. Thông thường, các đặc trưng chung nàu có thể được dùng độc lập (dưới dạng vector đặc trưng) hoặc tổng hợp lại trong quá trình nhận dạng. Các phương pháp phụ thuộc vào các tham số về mặt thời gian áp dụng việc phân tích cực trị địa phương [27][44], zero-crossing [43], độ dài chu kỳ [20], tần suất của chu kỳ dáng đi [41][44], tính đối xứng của dáng đi [53] hoặc phân tích khoảng động [41][51]. Liên quan đến các tham số về mặt tần suất, các hướng tiếp cận hiện giờ áp dụng các hệ số FFT [19][44], biến đổi wavelet [47], các hệ số cepstral [28][39][50] và biến đổi consine rời rạc [39][44]. Các đặc trưng chung có thể được thể hiện dưới dạng tham số thống kê (trung bình, giá trị, skewness, kurtosis, moment bậc cao) [27][28][43] và các histogram [19][27]. Hầu hết các phương pháp gần đây nhất và cũng là hiệu quả nhất dựa vào các quy trình rút trích đặc trưng rất tinh vi và tiên tiến, bao gồm các hướng tiếp cận dựa trên PCA [52], so khớp template hình học [26][27], lý thuyến tính toán về perceptron [48], đăng ký phase liên chu kỳ [22][31]…

## Quy trình nhận dạng

Tất cả những phương pháp nhận dạng dáng đi dựa trên cảm biến quán tính phụ thuộc vào nguyên tắc đã mô tả. Nguyên tắc này có 2 giai đoạn: đăng ký và nhận dạng. Trong cả hai giai đoạn đăng ký và nhận dạng, mỗi hướng tiếp cận dùng cách thể hiện mẫu dáng đi giống nhau trong không gian đặc trưng thu được bằng quy trình biến đổi đã được chọn trước, như đã mô tả trong phần trước. Nhận dạng có thể được thực hiện bằng 2 cách: (a) so khớp độ giống nhau của mẫu dựa đối với các mẫu dáng đi đã biết hoặc (b) bằng các phương pháp máy học, trong đó nhận dạng dáng đi được xem như là một bài toán phân loại. Trong cả hai trường hợp, có hai nhóm cần phải được xem xét: một nhóm chứa mẫu dáng đi đã đăng ký, thường được gọi là thư viện mẫu trong các hướng tiếp cận dùng sự giống nhau của mẫu, hay gọi là bộ huấn luyện trong các hướng tiếp cận dùng máy học; nhóm kia chứa các mẫu dành cho nhận dạng, thường được gọi là mẫu thử nghiệm (trong các hướng dùng sự giống nhau của mẫu), hay gọi là bộ test (hướng dùng máy học). Trong các hướng dùng máy học, mỗi mẫu trong bộ huấn luyện được gán nhãn tương ứng với lớp của nó (người có dáng đi đó). Sau đó, quy trình phân loại sẽ gán một trong những nhãn đã được định nghĩa trong bộ huấn luyện vào những mẫu trong bộ test. Mặt khác, trong các hướng dùng sự giống nhau của mẫu, các mẫu dáng đi được biến đổi vào trong không gian đặc trưng được xác định trước và so sánh đôi một với nhau. Điều này có nghĩa là nhận dạng dáng đi được thực hiện bởi việc ước lượng sự giống nhau giữa cặp mẫu bất kỳ, gồm một mẫu của 1 người bất kỳ đã đăng ký, một mẫu mới được đưa vào để nhận dạng.

Những hướng tiếp cận dựa trên ước lượng sự giống nhau giữa các mẫu thường sử dụng các độ đo đơn giản để tính toán sự khác nhau giữa các mẫu dáng đi, bao gồm sự tương quan về histogram [20], khoảng cách Manhattan [21][38], khoảng cách Euclide [21][29][38], hệ số tương quan [18][19][21], khoảng cách Tanimoto [21][36], khoảng cách Hamming [42]. Bên cạnh những độ đo đơn giản, một số độ đo phức tạp hơn như sau cũng được sử dụng, trong đó độ đo thường được sử dụng rộng rãi nhất là DTW hoặc biến thể [25][31][38]. Các hướng tiếp cận xem bài toán nhận diện dáng đi như một bài toán phân loại, thường dựa trên một số kỹ thuật phân loại nổi tiếng, bao gồm K láng giềng gần nhất (k-NN) [30][33][35], SVM [24][26][32], cây quyết định [27], random forest [33], mạng neuron [27], mô hình Markov ẩn [39], mô hình GMM [28][34], logistic regression [43], bộ phân loại sử dụng cho tập hợp mã thưa [23]…

## Kết chương

Trong chương này, chúng tôi đã trình bày tổng quan về các hướng tiếp cận chính và các giai đoạn chính trong quy trình xử lý để định danh người dùng bằng đặc trưng dáng đi. Trong đề tài này, chúng tôi không sử dụng hướng tiếp cận so khớp mẫu mà chọn hướng tiếp cận dựa vào máy học.

Hiện nay, hầu hết các phương pháp chứng thực với đặc trưng dáng chuyển động sử dụng máy học đều dùng các kỹ thuật phân lớp truyền thống như SVM, láng giềng gần nhất, mạng neuron…, chưa tận dụng được ưu điểm của các kỹ thuật mới trong deep learning. Trong đề tài này, chúng tôi đề xuất việc ứng dụng convolutional neural network để nhận biết người dùng từ đặc trưng dáng đi.

Trong Chương 4, chúng tôi sẽ trình bày tổng quan về neural network và convolutional neural network. Dựa trên kiến thức nền tảng này, chúng tôi trình bày phương pháp mà chúng tôi đề xuất dựa trên convolutional neural network để nhận biết người dùng từ dáng đi được trình bày trong Chương 5, và kết quả thử nghiệm được trình bày trong Chương 6.

# Tổng quan về Neural Network, Convolutional Neural Network, Recurrent Neural Network

**Tóm tắt chương:**

*✍ Nội dung Chương 4 trình bày tổng quan về neural network, từ đó tập trung đi sâu vào các thành phần cơ bản của Convolutional Neural Network (CNN), một dạng neural network đặc thù với khả năng liên kết – phụ thuộc cục bộ giữa các node trong 2 layer liên tiếp. Trong phần cuối chương, chúng tôi trình bày thêm về một số vấn đề nâng cao khi huấn luyện và cải tiến CNN.*

*Dựa trên cấu trúc và đặc điểm của mỗi loại layer trong Convolutional Neural network, chúng tôi đề xuất một kiến trúc tổng quát cho một họ CNN cụ thể sẽ được dùng trong đề tài này để rút trích và biểu diễn đặc trưng cấp cao của dáng đi.*

## Giới thiệu về neural network

### Tổng quan

Mạng nơ-ron nhân tạo (Artificial Neural Network - ANN) là một mô hình xử lý thông tin lấy cảm hứng từ hệ thống thần kinh sinh học, chẳng hạn như não. Yếu tố then chốt của mô hình này là cấu trúc mới của hệ thống xử lý thông tin. Nó bao gồm một số lượng lớn các yếu tố xử lý kết nối cao (highly interconnected processing) nơ-ron (neurones) làm việc đồng thời để giải quyết các vấn đề cụ thể. ANNs cũng giống như con người học bằng các ví dụ. Một ANN được cấu hình cho một ứng dụng cụ thể, chẳng hạn như nhận dạng mẫu hoặc phân loại dữ liệu, thông qua một quá trình học trên tập dữ liệu để học (training dataset). Học trong các hệ thống sinh học liên quan đến việc điều chỉnh các kết nối tiếp hợp (synaptic connections) tồn tại giữa các nơ-ron (neurones) và từ đó được áp dụng tương tự cho ANN.

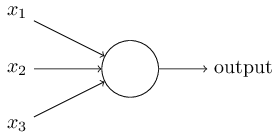
Neural network là một trong những thuật toán học có giám sát phổ biến nhất. Tư tưởng của neural networks, như ý nghĩa của tên phương pháp, xuất phát từ việc mô phỏng cấu trúc phức tạp và cơ chế hoạt động hiệu quả của bộ não con người. Phương pháp này được sử dụng nhiều trong những năm 80 và đầu 90 của thế kỉ 20 nhưng dần ít phổ biến vào nửa sau thập niên 90. Tại thời điểm đó, neural network được xem là thuật toán kém hiệu quả bởi nó yêu cầu chi phí tính toán quá lớn so với khả năng của phần cứng máy tính đương thời. Minsky và Papert đã xuất bản một quyển sách (năm 1969) mô tả tóm lược các vấn đề về sự khó khăn trong việc áp dụng neural networks từ các nhà nghiên cứu và cũng nhận được nhiều sự đồng tình ở giới nghiên cứu bấy giờ. Từ đầu những năm 2000, chi phí tính toán trở nên rẻ hơn đáng kể nhờ vào những thành tựu vượt bậc của phần cứng máy tính. Từ thực tế này, neural network lại nổi lên như một phương pháp đầy tiềm năng để giải những bài toán máy học có giám sát khó và yêu cầu thuật toán học phi tuyến mạnh.

Neural networks có khả năng tuyệt vời trong việc trích xuất đặc tính trong các dữ liệu phức tạp và không chính xác, điều mà có thể sử dụng để cấu tạo nên được các mẫu (patterns) và phán đoán xu hướng (trends) từ những dữ liệu quá phức tạp đối với con người và những công nghệ hay công trình khoa học máy tính khác. Một mô hình neural networks đã được huấn luyện (trained) có thể được đánh giá là “nhà chuyên gia” trong việc phân loại một số trường (categories) dữ liệu nhất định. Với các điểm nổi mạnh như sau:

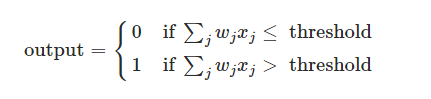
* Khả năng học có tính thích nghi: khả năng học làm sao giải quyết vấn đề (tasks) dựa trên những dữ liệu được cung cấp và những khởi tạo giá trị ban đầu.
* Khả năng tự sắp xếp: ANN có thể tạo ra sự sắp xếp của mình hoặc thể hiện được các thông tin mà nó nhận được trong lúc học.
* Phép thực hiện thời gian thực: Sự tính toán ANN có thể được thực thế hóa xử lý song song, các thiết bị phần cứng đặc biệt được thiết kế và thực thi sẽ có thể tận dụng được khả năng này.
* Khả năng kháng lỗi thông qua sự lưu thông tin dự phòng (Redundant Information Coding): xây dựng mạng cục bộ có thể dẫn đến vấn đề và performance, nhưng một vài mạng có thể giữ lại được dù có chịu sự thiệt hại lớn (major network damage).

### Perceptron

Mô hình neuron đầu tiên được phát triển bởi Frank Rosenblatt trong những năm 50 và 60 của thế kỉ 20 từ ý tưởng của Warren McCulloch và Walter Pitts được gọi là perceptron. ***Đầu vào* *(input)***của perceptron là nhiều biến nhị phân, , và ***đầu ra* *(output)***là một kết quả nhị phân duy nhất. Nó có thể được xem như một hệ thống đưa ra quyết định dựa vào các yếu tố ảnh hưởng và ***trọng số (weight)*** của mỗi yếu tố.



Hình 4‑1 sdasd



Hình 4‑2 asdasd

Giả sử ta có 1 mô hình perceptron với 3 biến đầu vào là và . Trong trường hợp tổng quát, số lượng biến đầu vào của một mô hình perceptron có thể là bất kỳ con số nào. Theo đề xuất của Rosenblatt, giá trị đầu ra được tính dựa trên các biến đầu vào và trọng số của mỗi biến. Trọng số là những số thực biểu diễn mức độ ảnh hưởng hay tầm quan trọng của biến đầu vào tương ứng với giá trị đầu ra. Một tham số khác của perceptron là ***ngưỡng (threshold)***. Ngưỡnglà một giá trị tham chiếu để xác định giá trị đầu ra là 0 hay 1. Về mặt toán học, cơ chế hoạt động của mô hình perceptron được thể hiện trong phương trình sau:

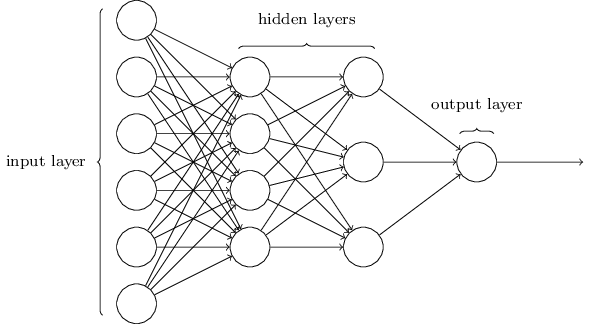
Các mô hình quyết định khác nhau có thể được tạo ra bằng cách thay đổi các trọng số và ngưỡng. Mặc dù có cấu trúc đơn giản, perceptron hiện thực hóa ý tưởng kết hợp một cách có hiệu quả nhiều yếu tố đầu vào để tạo ra một kết quả đầu ra.

Cấu trúc phức tạp được phát triển từ perceptron là multi-layer perceptron. Trong cấu trúc này, lớp thứ nhất đưa ra một số giá trị trung gian (số lượng cụ thể phụ thuộc vào cấu hình của mạng) từ dữ liệu đầu vào. Mỗi perceptron của lớp thứ 2 đưa ra 1 giá trị trung gian từ các giá trị trung gian được truyền từ lớp thứ nhất. Vì vậy, một perceptron có thể tính toán được giá trị trung gian phức tạp và rút ra được đăng trưng của dữ liệu đầu vào trừu tượng hơn các perceptron ở lớp đầu tiên. Sau đó, mỗi perceptron ở các lớp tiếp thu lấy thông tin từ lớp liền trước, tính toán giá trị và truyền cho lớp liền sau. Cuối cùng, perceptron ở lớp cuối có khả năng tính toán giá trị phức tạp và trừu tượng nhất để đưa ra kết quả cuối cùng cho toàn bộ mô hình. Rõ ràng, multi-layer perceptron có thể đóng vai trò là hệ thống đưa ra quyết định trong những tình huống phức tạp. Điều cần chú ý là kết quả đầu ra của multi-layer perceptron là một giá trị cụ thể.

Để đơn giản hóa việc kí hiệu, các tác giả vector hóa giá trị đầu vào (input) và trọng số (weight), đồng thời giới thiệu một tham số mới là ***giá trị lệch (bias)***. Giá trị lệch là thước đo cho ta biết mức độ dễ dàng để kết quả đầu ra (output) là 1. Cơ chế hoạt động của mạng perceptron được thể hiện trong phương trình sau:

### Kiến trúc của mạng

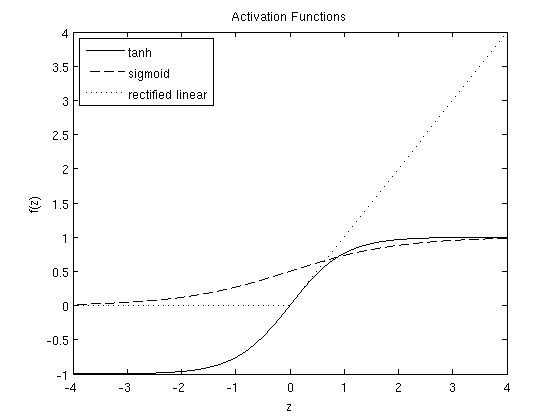
Vì ý tưởng của mạng neural nhân tạo được xuất phát từ việc mô phỏng cấu trúc và cơ chế hoạt động của bộ não con người, kiến trúc chung của mạng bao gồm nhiều nút (node) được sắp xếp thành các tầng (layer) với đường nối (link) có hướng giữa các nút của 2 tầng liên tiếp. Neural network được tạo ra bằng sự kết hợp của các neuron đơn giản sao cho đầu ra của neuron này là đầu vào của neuron liền sau. Neural network có kiến trúc phân tầng chặt chẽ.



Hình 4‑3 Kiến trúc chung của mạng neural kết nối đầu đủ. [62]

Trong Hình 4‑1 tầng ngoài cùng bên trái được gọi là ***tầng đầu vào (input layer)***, trong khi tầng ngoài cùng bên phải được gọi là ***tầng đầu ra (output layer)*** hay ***tầng kết quả***. Những tầng còn lại được gọi là ***tầng trung gian*** hoặc ***tầng ẩn (hidden layers)***. Mặc dù có tên là “tầng ẩn”, những tầng này chỉ đơn giản là các tầng không phải tầng đầu vào và tầng đầu ra. Thực tế, tầng ẩn có thể được nhìn thấy bởi mọi người. Mỗi nút trên các tầng được gọi là neuron. Những neuron trên tầng chỉ được nối tới những neuron trên tầng . Sự kết nối được kí hiệu bằng những mũi tên có hướng.

Vì thói quen từ lịch sử sử dụng, multi-layer network có thể được gọi là multi-layer perceptron mặc dù có thể có sigmoid neuron trong multi-layer network.



Hình 4.2. Các hàm kích hoạt (activation function). [65]

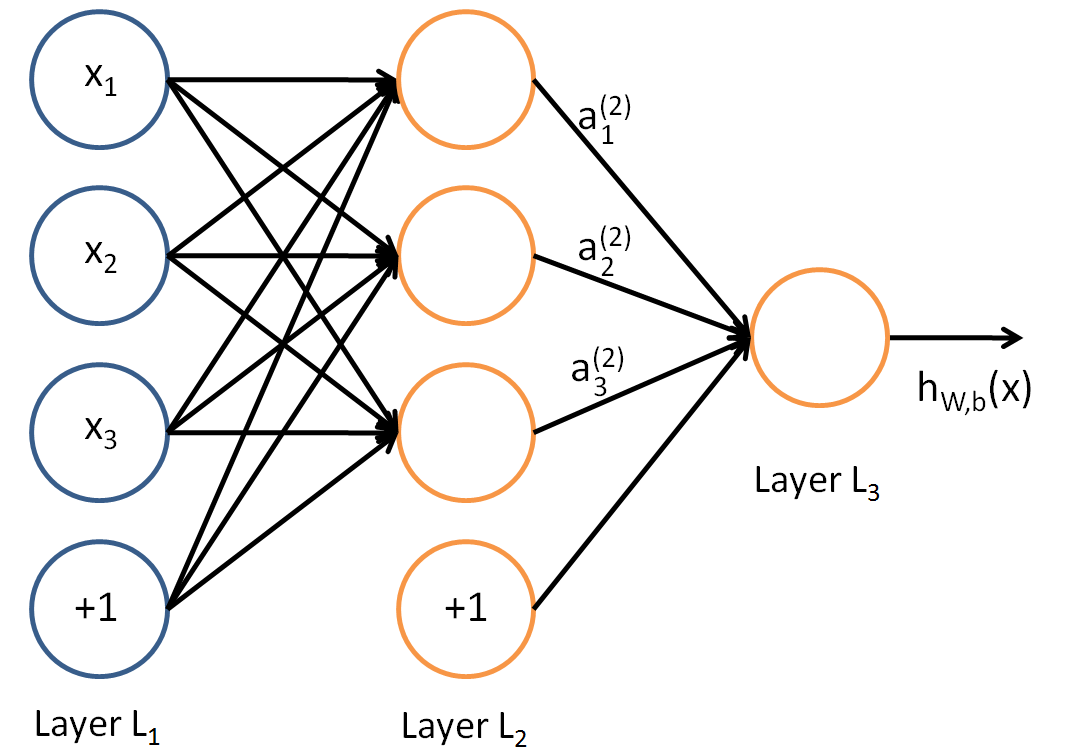
Việc thiết kế tầng đầu vào và tầng đầu ra phụ thuộc vào định dạng của dữ liệu đầu vào và mục tiêu huấn luyện ở đầu ra của mạng. Tuy nhiên, việc thiết kế các tầng trung gian đòi hỏi kỹ thuật cao vì không có một công thức chung để cài đặt cấu hình của các tầng này. Thay vào đó, các nhà nghiên cứu làm việc với neural network đã phát triển nhiều cấu hình dựa trên phương pháp heuristics. Tầng trung gian có ý nghĩa quyết định đối với khả năng sử dụng của neural network. Neural network sẽ trở nên phức tạp hơn khi càng có nhiều tầng trung gian. Khi dữ liệu đầu vào đi sâu hơn qua các tầng trung gian, những đặc trưng phức tạp và trừu tượng hơn được rút trích. Khi chúng ta tăng số neuron tại mỗi tầng, tầng đó có khả năng rút trích nhiều đặc trưng hơn.

Trong trường hợp tổng quát, hàm sigmoid có thể được thay thế bởi các hàm khác, ví dụ hàm hyperbolic tan, hàm rectified linear unit,... Những hàm này được gọi chung là ***hàm kích hoạt (activation function)*** . Hình 4.2 biểu diễn đồ thị của 3 hàm kích hoạt phổ biến. Công thức của 2 hàm kích hoạt như sau:

Miền giá trị của hàm hyperbolic tan là [−1, 1] trong khi hàm sigmoid trả về giá trị trong đoạn [0, 1]. Hàm rectified linear là hàm tuyến tính từng phần (piece-wise linear).

### Lan truyền thuận (feed forward)

Việc huấn luyện neural network là một quá trình lặp lại nhiều lần với 2 bước: ***lan truyền thuận (feed forward)*** và ***lan truyền ngược (backpropagation)***. Trong lan truyền thuận, các tham số và dữ liệu đầu vào được đưa vào mạng để tính kết quả cuối cùng. Trong lan truyền ngược, độ lỗi (error hoặc loss value) được tính dựa vào sự sai khác hay trùng khớp giữa giá trị mẫu và giá trị được dự đoán bởi mô hình máy học chúng ta đang xây dựng, rồi được truyền ngược theo mạng để điều chỉnh các giá trị tham số. Sau mỗi lần thực hiện 2 bước lan truyền thuận và ngược, giá trị tham số tiến gần hơn giá trị tốt nhất.



Hình 4.3. Một ví dụ của neural network. [65]

Để thuận tiện, chúng ta dùng mạng trong hình 2.12 cùng các kí hiệu để mô tả rõ hơn về 2 bước lan truyền. là các giá trị đầu vào. Các nút +1 trong 2 tầng đầu tiên là các giá trị lệch. is the layer . Các tham số trong mạng là , với là trọng số của đường nối từ nút ở tầng đến nút ở tầng . là giá trị đầu ra trung gian (còn gọi là activation) của nút ở tầng . là tổng có trọng số được dùng làm đầu vào của nút ở tầng . Cuối cùng, đặt là hàm kích hoạt và là hàm giả thuyết tương ứng với tham số và giá trị đầu vào . Quá trình lan truyền thuận được thể hiện qua hệ phương trình sau:

Trong trường hợp tổng quát, hệ phương trình dạng vector của quá trình lan truyền thuận:

### Lan truyền ngược (backpropagation) và phương pháp gradient descent

Trong lĩnh vực Máy Học, ***gradient descent*** là một thuật toán hiệu quả để tìm bộ tham số làm cho mô hình khớp nhất với dữ liệu huấn luyện, nhất là khi dữ liệu huấn luyện lớn. Ý tưởng của gradient descent là lặp nhiều lần việc cập nhật giá trị mới của các tham số dựa trên giá trị hiện tại và độ lỗi của kết quả dự đoán. Gradient descent có 3 dạng phổ biến: batch gradient descent (còn được gọi là “gradient descent”), stochastic gradient descent và mini-batch gradient descent. Với phương pháp batch gradient descent, cả tập dữ liệu được sử dụng mỗi lần tham số được cập nhật. Vì vậy, các giá trị gradient thay đổi ít nhưng ổn định và hướng đến giá trị cực tiểu toàn cục. Stochastic gradient descent cập nhật giá trị gradient dựa trên mỗi mẫu nên gradient có thể thay đổi theo hướng ngược với giá trị tối ưu cần đạt được. Hệ quả là giá trị gradient thay đổi thường xuyên hơn và kém ổn định hơn phương pháp trước. Khi áp dụng stochastic gradient descent, giá trị gradient cuối cùng chỉ dao động quanh cực tiểu toàn cục chứ không dừng tại giá trị chính xác. Mini-batch gradient descent là một dạng trung gian của 2 phương pháp trên. Mỗi lần cập nhật sử dụng 1 phần của tập dữ liệu. Nhìn chung, 2 kỹ thuật sau làm cho gradient hội tụ nhanh hơn batch gradient descent.

Để tính tổn thất do việc dự đoán sai, chúng ta định nghĩa ***hàm chi phí (cost function)*** như sau:

Số hạng thứ nhất trong công thức thứ 2 của hàm chi phí là trung bình của tổng các bình phương độ lỗi. Số hạng thứ 2 - ***đại lượng kiểm soát (regularization term*** hay ***weight decay)*** – được dùng để tránh tình trạng ***overfit*** (nghĩa là mô hình học quá khớp với dữ liệu huấn luyện, dẫn đến giảm khả năng dự đoán với các dữ liệu khác). là ***hệ số kiểm soát (regularization rate)***. Nếu hệ số kiểm soát quá lớn, các tham số sẽ tiến về 0 và mô hình của chúng ta có thể bị underfit (nghĩa là mô hình học sai lệch một cách đáng kể với dữ liệu huấn luyện, dẫn đến độ lỗi trong quá trình huấn luyện quá lớn). Mặt khác, nếu hệ số kiểm soát quá nhỏ, đại lượng kiểm soát sẽ có giá trị không đáng kể và mô hình có thể bị overfit.

Áp dụng phương pháp gradient descent vào hàm chi phí, chúng ta có công thức:

là ***hệ số huấn luyện (learning rate)***. Đây cũng là một tham số quan trọng trong neural network. Nếu nhỏ, hệ thống huấn luyện có thể cần nhiều lần lặp để gradient hội tụ. Ngược lại, nếu lớn, giá trị gradient có thể dao động với biên độ lớn và bỏ qua vùng hội tụ.

Số hạng thứ 2 của các phương trình trên có chứa phép tính đạo hàm từng phần. Ta tính các số hạng đó:

Ý tưởng của lan truyền ngược như sau. Đầu tiên, mạng lan truyền thuận dữ liệu đầu vào để tính giá trị kích hoạt tại mỗi nút và kết quả cuối cùng của mạng. Sau đó, chúng ta tính độ lỗi tại mỗi nút để xác định phần đóng góp của mỗi nút trong kết quả đúng hoặc sai của mạng. Giá trị tham số mới được cập nhật tại mỗi nút dựa theo giá trị hiện tại và độ lỗi của nút đó. Sau mỗi lần chạy, độ lỗi chung của mạng có xu hướng giảm và giá trị tham số có xu hướng tiến đến giá trị tối ưu.

## Các thành phần cơ bản của Convolutional Neural Network (CNN)

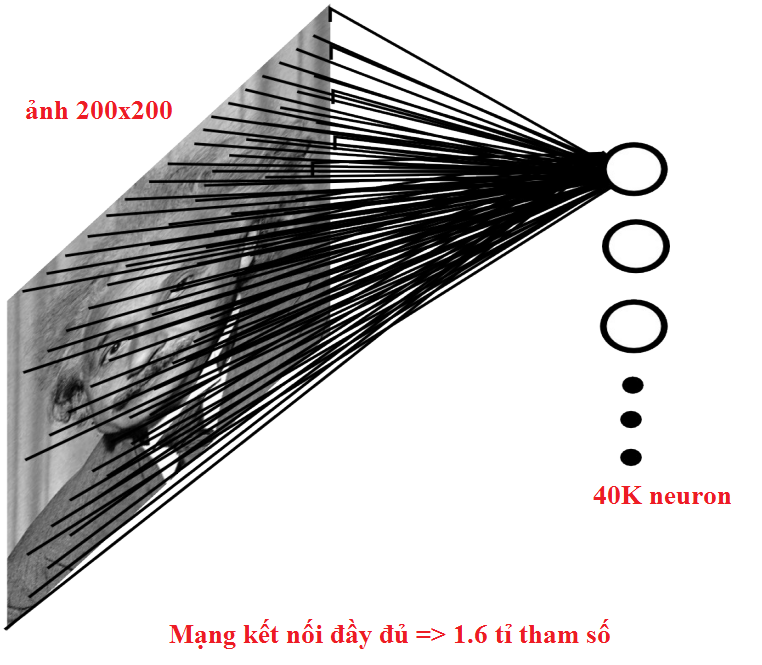
Khi áp dụng neural network vào các bài toán nhận dạng dựa vào ảnh, ta nhận thấy có nhiều bước tính toán thừa. Ví dụ, khi cần rút trích đặc trưng của một vùng ảnh, ta tính tất cả điểm ảnh với các trọng số khác nhau. Điều này không cần thiết vì đặc trưng địa phương chỉ do các điểm ảnh lân cận vùng ta cần rút đặc trưng quy định. Như vậy, chúng ta chỉ cần tính các điểm ảnh lân cận với trọng số phù hợp. Cách tính này giúp ta vừa giảm chi phí tính toán, vừa giảm chi phí lưu trữ các tham số cho neural network. Đây là ý tưởng chính của convolutional neural network.

Mạng neural network lan truyền thuận là một hàm hợp có dạng như sau:

Mỗi hàm nhận dữ liệu đầu vào và vector tham số để tạo ra dữ liệu output . Đầu ra của hàm này là đầu vô của hàm liền sau. Việc chọn lựa các hàm số được thiết kế bằng tay trong khi tham số được khởi tạo ngẫu nhiêu hoặc sử dụng phương pháp học không giám sát và liên tục cập nhật cho đến khi đạt được yêu cầu của bài toán ban đầu đặt ra. Đối với mạng CNN, dữ liệu và các hàm thành phần sẽ có thông tin về mặt cấu trúc. Trong phần này, để thuận tiện trong việc trình bày các ý tưởng của CNN, các tác giả giới hạn bài toán trong dữ liệu ảnh dưới dạng cấu trúc mảng hai chiều các pixel. Một cách hình thức, dữ liệu tại mỗi tầng là ma trận ảnh kích thước các số thực. Trong đó, và là các chiều theo trục không gian ảnh, là số kênh của ma trận. Đầu vào của mạng CNN là ảnh gốc , trong khi dữ liệu tại các tầng khác được gọi là *feature map* (bản đồ đặc trưng). Mỗi hàm trong mạng CNN là một trong số những loại sau đây: convolution, hàm phi tuyến (non-linear gating), pooling và chuẩn hóa (normalization).

### Convolution

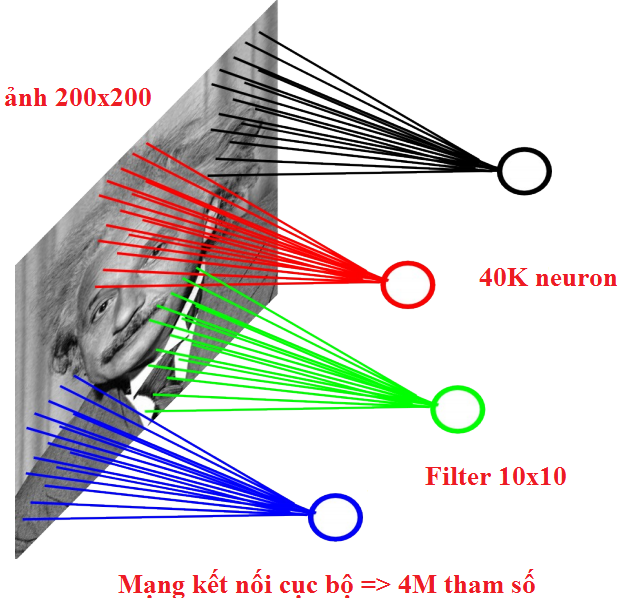
Mạng NN dạng chuẩn với kết nối đầy đủ giữa hai layer liên tiếp sẽ có số lượng tham số rất lớn. Hình 4.5 minh họa ví dụ với mạng NN có input là ảnh , layer ẩn có 40 000 neuron thì tổng số tham số cần phải ước lượng lên đến 1.6 tỉ! Để có thể huấn luyện được mạng NN này, số lượng dữ liệu huấn luyện cần phải rất lớn. Điều này gây khó khăn cho việc huấn luyện trên hai yếu tố: chi phí để xây dựng dữ liệu huấn luyện lớn và thời gian huấn luyện lâu.



Hình 4.4. Mạng neural network với các neuron được kết nối đầy đủ với nhau

Để giảm số lượng tham số, mỗi neuron chỉ cần kết nối tới một vùng cục bộ của ảnh thay vì trên toàn bộ ảnh (Hình 4.5). Ví dụ với ảnh kích thước , layer ẩn có 40 000 neuron và filter có kích thước thì tổng số tham số cần ước lượng chỉ còn 4 triệu. Với giả sử rằng các vùng ảnh cục bộ là tương đối ổn định với các tính chất thống kê (statistics) giống nhau tại những vị trí khác nhau, convolutional layer giả sử rằng tham số của các filter là giống nhau tại tất cả các vị trí trên ảnh. Bộ tham số này còn được gọi dưới tên khác là kernel và được học trong quá trình huấn luyện mạng CNN. Với giả sử này, một convolutional layer chỉ còn 100 tham số. Tuy nhiên, một tầng biến đổi convolution sẽ bao gồm kernel có kích thước (hay còn gọi là filter bank). Một cách hình thức, convolutional layer là một ánh xạ:

trong đó,



Hình 4.5. Mạng neural network với các neuron được liên kết cục bộ với các neuron thuộc layer trước

Giả sử kích thước ảnh đầu vào là , kernels với kích thước được sử dụng với bước nhảy . Khi đó, kích thước của ảnh đầu ra là . Nếu bước nhảy là 1, kích thước ảnh được xem như không thay đổi sau khi đi qua tầng này. Ngược lại, bước nhảy lớn hơn 1 được sử dụng khi ta muốn giảm kích thước (downsample) ảnh. Hàm convolution xử lí từng vị trí pixel của tất cả channel cùng 1 lúc. Ngoài ra trong trường hợp muốn bảo toàn kích thước ảnh, ta có thể chèn thêm *pad* pixel với một giá trị màu cho trước (thường là 0) xung quanh viền của ảnh input.

### Cổng phi tuyến (non-linear gating)

Về cơ bản, convolution là một phép biến đổi tuyến tính. Nếu tất cả các neuron được tổng hợp bởi các phép biến đổi tuyến tính thì một mạng neuron đều có thể đưa về dưới dạng một hàm tuyến tính. Khi đó mạng NN sẽ đưa về bài toán logistic regression. Do đó tại mỗi neuron cần có một hàm activation dưới dạng phi tuyến. Có nhiều dạng hàm phi tuyến được sử dụng trước đây như *sigmoid* và *hyperbolic tan*. Tuy nhiên, các nghiên cứu gần đây chứng minh được việc sử dụng hàm *ReLU* (Rectified Linear Unit) [61] cho kết quả tốt hơn ở các khía cạnh:

* tính toán đơn giản
* tạo ra tính thưa (sparsity) của các neuron ẩn. Ví dụ như sau bước khởi tạo ngẫu nhiên các trọng số, khoảng 50% các neuron ẩn được kích hoạt (có giá trị lớn hơn 0).
* quá trình huấn luyện nhanh hơn ngay cả khi không phải trải qua bước tiền huấn luyện (pre-training)

Hàm ReLU được áp dụng trên từng phần tử của ma trận trong quá trình biến đổi do đó số chiều không thay đổi:

Do đó một convolution layer là một hàm hợp của phép biến đổi convolution và cổng phi tuyến. Trong trường hợp sử dụng hàm phi tuyến ReLU ta có công thức biến đổi sau khi qua convolution layer như sau:

### Pooling

Pooling layer là một trong những thành phần tính toán quan trọng trong mạng CNN. Toán tử pooling được thực hiện độc lập trên mỗi kênh của ma trận để tổng hợp tất cả tín hiệu nằm trên một vùng cục bộ. Có thể kể đến các loại hàm pooling như *max-pooling*, *sum-pooling, L2-pooling*. Tuy nhiên dùng nhiều hơn cả trong các mạng CNN là phương pháp max-pooling được định nghĩa như sau:

trong đó, là kích thước của filter. Max-pooling xác định vị trí cho tín hiệu mạnh nhất khi áp dụng một loại filter. Điều này cũng tương tự như là một bộ lọc phát hiện vị trí đối tượng bằng filter. Kích thước của một pooler phụ thuộc mức độ bền vững trước các phép biến dạng. Kích thước càng lớn thì mức độ biến dạng càng lớn và ngược lại.

Ý nghĩa của tầng pooling là khi chúng ta khảo sát từng vùng trên ảnh để kiểm tra ảnh đó có tính chất cần tìm hay không, chúng ta có thể kết luận vùng đang khảo sát thỏa mãn tính chất này ngay khi xác định được có 1 điểm ảnh thỏa. Bên cạnh đó, nếu 1 đặc trưng được thể hiện ở 1 điểm ảnh, xác suất đặc trưng đó cũng thể hiện ở những điểm ảnh lân cận là thấp.

### Chuẩn hóa (Normalization)

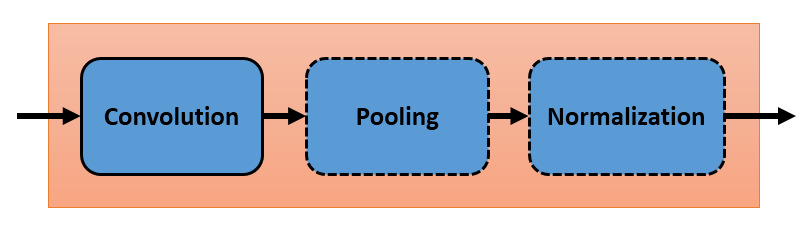
Chuẩn hóa các giá trị pixel được thực hiện trên từng kênh nhưng phạm vi ảnh hưởng của giá trị chuẩn hóa thì thuộc nhiều kênh lân cận. Công thức của phép chuẩn hóa giá trị pixel trên nhiều feature map (*local response normalization – cross map*) như sau:

trong đó, là hằng số cho biết số lượng kênh lân cận ảnh hưởng tới giá trị chuẩn hóa tại kênh đang xét. là các tham số khác của công thức chuẩn hóa. Trường hợp đặc biệt: ta có công thức chuẩn hóa dạng . Ưu điểm của việc chuẩn hóa các giá trị pixel đó là:

* Tăng tính bất biến (ví dụ: sự thay đổi môi trường sáng)
* Cải thiện quá trình tối ưu hóa kết quả huấn luyện
* Tăng độ thưa của các neuron. Ví dụ: giá trị của các pixel sau khi chuẩn hóa và qua hàm biến đổi ReLU sẽ có rất nhiều giá trị bằng 0.

### Kiến trúc mạng CNN

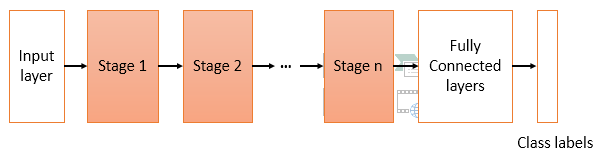
Mạng CNN là mạng gồm có nhiều pha (stage), trong đó mỗi pha gồm 3 thành phần cơ bản là convolution layer, pooling layer và normalization layer. Hình 4.6 minh họa cấu trúc của một pha trong mạng CNN.



Hình 4.6. Một pha trong mạng CNN

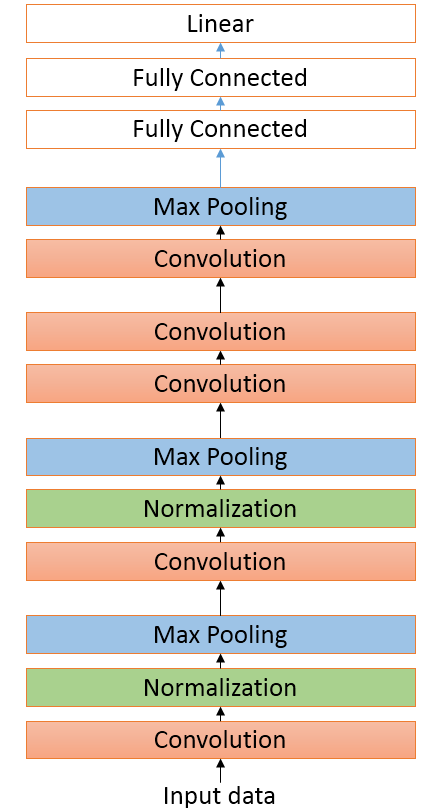
Lưu ý rằng, pooling layer và normalization layer được ký hiệu bằng đường đứt nét có tính tùy biến tùy theo mục đích bài toán và dữ liệu. Trong nhiều trường hợp chỉ có pooling mà không có Normalization và ngược lại. Ngoài ra, về thứ tự của hai layer này cũng có thể thay đổi. Về mặt khái niệm tổng quát, một pha đầu tiên của mạng CNN tương đương với bước tính đặc trưng cấp thấp như SIFT, HOG. Các đặc trưng này đều phải qua các bước biến đổi sử dụng các convolutional filter, chuẩn hóa và pooling. Tuy nhiên điểm khác biệt là các tham số của filter được thiết kế sẵn (hand crafted), trong khi mạng CNN với thuật toán học sẽ tự tìm ra các tham số của filter sao cho phù hợp với bài toán cần giải quyết.

Kiến trúc tổng quát của một mạng CNN sâu (Deep Convolutional Neural Network) bao gồm nhiều pha thành phần với các convolution, pooling và normalization layer. Hình 4.7 minh họa kiến trúc của một mạng DCNN cho bài toán phân loại đối tượng. Ngoài các stage có chứa convolution layer, mạng DCNN còn có các layer được kết nối đầy đủ với nhau (fully connected layers). Trong đó, mỗi neuron của lớp này sẽ kết nối với tất cả các neuron thuộc lớp lân cận. Để đảm bảo số lượng tham số cần ước lượng không quá lớn, thông thường các layer kết nối đầy đủ được đặt ở phần cuối của mạng và số lượng neuron còn lại không quá nhiều. Layer cuối cùng thể hiện thông tin output của bài toán cần giải, ví dụ vector chứa nhãn phân lớp đối với bài toán phân loại đối tượng. Về mặt khái niệm tổng quát, các pha của mạng CNN lần lượt thực hiện các công việc như tính đặc trưng cấp thấp (như SIFT, HOG,…), gom nhóm các đặc trưng (như K-mean), tổng hợp đặc trưng dựa trên thông tin vị trí (như Spatial Pooling)[54]. Các layer liên kết đầy đủ tương tự như một máy phân lớp (như SVM), sử dụng những đặc trưng từ các pha trước để phân loại. Ưu điểm của kiến trúc này là tất cả tham số của các bước xây dựng đặc trưng và máy phân lớp được huấn luyện để học tự động mà không cần phải thiết kế bằng tay.



Hình 4.7. Mạng CNN sâu bao gồm nhiều pha ở giữa và các layer kết nối đầy đủ ở những layer cuối cùng.

Mạng CNN có nhiều ứng dụng trong các bài toán khác nhau. Trong đó, đáng chú ý nhất là mạng CNN cho bài toán phân loại đối tượng được Krizhevsky và đồng sự xây vào năm 2012 [64]. Các tác giả đã xây dựng một mạng CNN gồm nhiều lớp sử dụng dữ liệu của ImageNet [55] để huấn luyện với số lượng lên đến hàng triệu ảnh và số lớp là 1000. Kiến trúc của mạng CNN của Krizhevsky sử dụng trong cuộc thi phân loại đối tượng được mô tả như trong Hình 4.8. Số lượng tham số của mạng này khoảng 60 triệu và thời gian huấn luyện trong khoảng hơn 1 tuần sử dụng chip xử lý song song GPU. Cuộc thi năm này đánh dấu sự thành công trong hướng tiếp cận deep learning vào các bài toán thuộc lĩnh vực thị giác máy tính. Trong những năm tiếp theo, deep learning chiếm áp đảo trong bảng xếp hạng các thuật toán cho kết quả tốt nhất thuộc nhiều bài toán khác nhau của ImageNet như: object classification, localization, object detection [56][57]. Không những vậy, deep learning còn được áp dụng rất thành công trong các lĩnh vực khác như: xử lý ngôn ngữ tự nhiên[53], xử lý tiếng nói[63]… Tháng 3 năm 2016, hệ thống chơi cờ vây AlphaGo sử dụng deep learning đã chiến thắng kì thủ vô địch thế giới Lee Sedol với tỉ số 4 – 1.



Hình 4.8. Kiến trúc mạng CNN được sử dụng trong cuộc thi ImageNet Classification 2012

## Phương pháp lan truyền ngược

Trong phần này trình bày các thành phần của một mạng CNN và kiến trúc tổng quát của một mạng CNN. Các tham số của mạng CNN được học dựa trên hàm mục tiêu . Việc huấn luyện được đề cập ở đây là huấn luyện có giám sát (supervised learning) dựa trên hai thành phần cho trước:

* Tập dữ liệu huấn luyện bao gồm các cặp  quan hệ input-output được gán nhãn trước: .
* *Hàm độ lỗi* (*loss function*) đánh giá mức độ chi phí (hoặc thiệt hại) khi dự đoán thay vì .

Hàm độ lỗi của mạng CNN cho trước tham số được tính bằng cách lấy trung bình cộng độ lỗi của tất cả các mẫu:

Trong nhiều trường hợp, hàm độ lỗi có thể được xem là một layer nữa của mạng CNN, hay còn gọi là *loss layer*. Do đó, về mặt ký hiệu, từ sau trở đi, hàm hợp của mạng CNN đã được tính bao gồm cả loss layer . Khi đó, ta xem đây là một ánh xạ từ không gian tập mẫu đến không gian số thực:. Hàm độ lỗi được sử dụng hiệu quả trong các mạng CNN được báo cáo gần đây là hàm *log-loss* kết hợp với hàm kích hoạt (activation function) *soft-max* cho layer kế cuối thay vì dùng hàm ReLU như các layer trước. Trong bài toán phân loại đối tượng, giả sử số lớp cần phân loại là , khi đó layer kế cuối sẽ gồm có phần tử nhưng có dạng ma trận kích thước . Điều này có ý nghĩa là với vị trí đầu tiên , kết quả trả về sau khi lan truyền thuận là giá trị tương ứng với mức độ giống với từng class. Các giá trị này sẽ được qua hàm kích hoạt soft-max có công thức như sau:

Công thức tính độ lỗi của hàm log-loss:

trong đó, là chỉ số lớp đối tượng của ground-truth tại vị trí . Trường hợp , độ lỗi . Ngược lại, nếu ta có khi .

Mục tiêu của quá trình huấn luyện là tìm bộ tham số tối ưu để tối thiểu hóa hàm độ lỗi của mạng CNN. Các bước chính của quá trình huấn luyện mạng CNN cũng tương tự như với các mạng NN truyền thống, bao gồm các bước:

* Bước 1: Lan truyền thuận (Forward propagation)
* Bước 2: Lan truyền nghịch (Back propagation)
* Bước 3: Cập nhật các tham số

Đối với mạng CNN có số lượng layer nhiều và dữ liệu huấn luyện rất lớn, thuật toán Stochastic Gradient Descent (SGD) với số lượng nhỏ mẫu (mini-batch) là một trong những phương pháp tốt nhất để huấn luyện. Phương pháp này giúp giảm chi phí tính toán khi cập nhật lại tham số đồng thời tận dụng được hiệu năng tính toán của GPU khi sử dụng các phép nhân ma trận với ma trận. Kích thước của mini-batch lớn thì hiệu quả càng cao (trong phạm vi cho phép của bộ nhớ lưu trữ). Để cập nhật tham số của mạng, ta dựa vào phương pháp *gradient descent*. Ý tưởng chính đơn giản như sau: tính gradient của hàm độ lỗi tại ma trận tham số tại thời điểm và cập nhật tham số tại thời điểm tiếp theo:

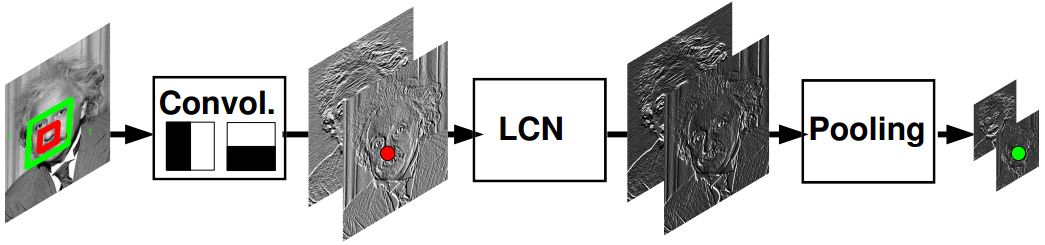
trong đó, là hệ số huấn luyện của thuật toán.

Đạo hàm của hàm hợp theo tham số tuân theo quy tắc chuỗi luật (*chain rule*) như sau:

Lưu ý, mỗi hàm thành phần trong mạng CNN là một ánh xạ từ mảng ba chiều kích thước sang ma trận ba chiều kích thước . Toán tử biến đổi các ma trận thành vector dạng cột (column vector) bằng cách nối các phần tử trên các cột vector lại với nhau. Kí hiệu biểu diễn công thức đạo hàm vector dạng cột của các biến output theo vector dạng dòng của các biến input. Giả sử rằng vector có phần tử, vector có phần tử, khi đó là một ma trận có kích thước .

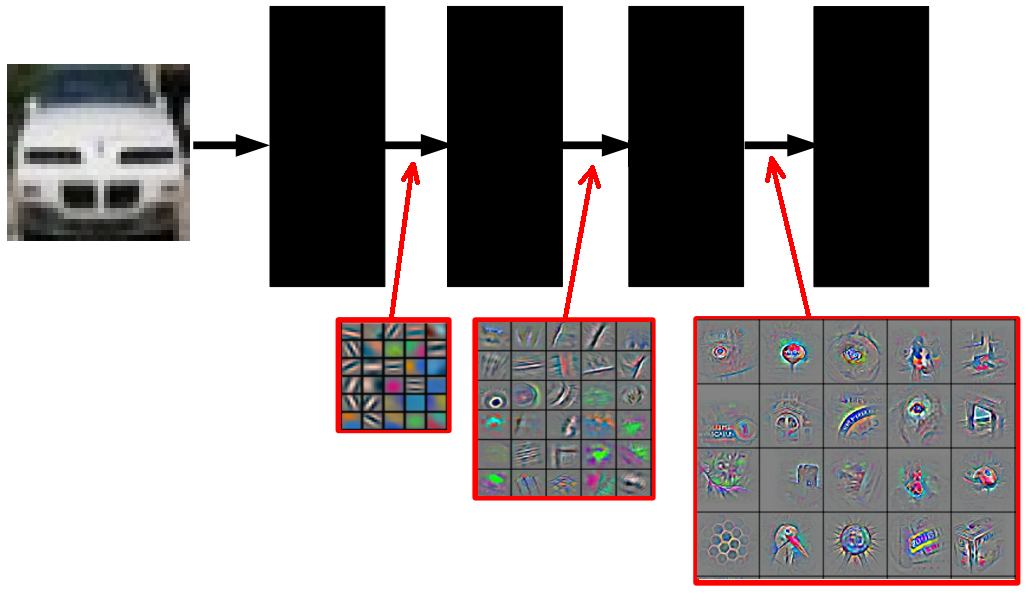
## Deep CNN là mạng học đặc trưng nhiều tầng

Mạng CNN bao gồm nhiều layer nối lại với nhau. Đây là một kiến trúc phức tạp và thường được nhiều người nhìn nhận dưới dạng một hộp đen (black box). Tuy nhiên, một số nghiên cứu gần đây tìm cách lý giải cho sự thành công của mô hình học theo chiều sâu bằng cách trực quan hóa (visualization) các tham số và kết quả trung gian trong quá trình huấn luyện [58]. Các nghiên cứu cho thấy, mạng CNN là một hệ thống cho phép huấn luyện và tìm ra các tham số tối ưu nhất nhằm tính toán các đặc trưng giúp phân biệt các lớp đối tượng với nhau. Hình 4.9 minh họa cho một pha đầu tiên của mạng CNN với hai loại filter đơn giản. Dấu chấm đỏ là một điểm trong không gian của feature map sau khi thực hiện biến đổi convolution. Điểm đặc trưng này chịu ảnh hưởng bởi những pixel nằm bên trong ô màu đỏ thuộc ảnh gốc. Sau khi thực hiện các biến đổi chuẩn hóa, pooling và giảm tỉ lệ kích thước (scale), điểm đặc trưng màu xanh lá cây thuộc feature map cuối cùng của pha chịu ảnh hưởng bởi những pixel nằm trong vùng màu xanh lá cây của ảnh gốc. Càng về những layer gần cuối của mạng CNN, phạm vi ảnh hưởng của mỗi điểm đặc trưng so với ảnh gốc càng lớn. Do đó, vector đặc trưng được học bởi mạng CNN được xem như là một vector mô tả toàn cục của tấm ảnh.



Hình 4.9. Phạm vi chịu ảnh hưởng của một điểm đặc trưng đối với ảnh đầu vào.

Ngoài ra, những đặc trưng được học trong những layer trung gian có thể được sử dụng cho những bài toán khác nếu như mạng CNN được học trên một tập dataset và số lượng phân lớp đủ lớn. Hình 4.10 trực quan hóa một số filter học được từ mạng CNN [58]. Feature map tại các bước trung gian của mạng CNN tuy theo độ sâu của các pha mà ta có các đặc trưng cấp thấp hay đặc trưng cấp cao. Layer càng sâu thì mức độ tác động của đặc trưng càng lớn và ngữ nghĩa càng cao hơn.



Hình 4.10. Ảnh trực quan hóa các layer của mạng CNN sau quá trình huần luyện.

## Một số vấn đề nâng cao về mạng CNN

Sau đây là một số vấn đề nâng cao trong việc xây dựng và huấn luyện mạng CNN.

### Dữ liệu huấn luyện

Mặc dù đã được giảm đáng kể, số lượng tham số của mạng CNN vẫn là một con số tương đối lớn, lên đến hàng triệu tham số. Để tránh hiện tượng các tham số quá khớp (over fitting) với dữ liệu, kích thước tập dữ liệu phải đủ lớn. Tuy nhiên, chi phí xây dựng dữ liệu huấn luyện lớn như vậy thường rất cao. Một trong những phương pháp hiệu quả để khắc phục việc này là phát sinh bộ dữ liệu mới từ một bộ dữ liệu đã gán nhãn cho trước. Mỗi ảnh đã được gán nhãn trước sẽ được biến đổi bằng các cách sau:

* Thêm nhiễu.
* Làm mờ.
* Thay đổi độ sáng.
* Biến đổi hình học: affine hoặc làm méo (distortion).
* Lật ngược hình theo trục *Ox*.
* Cắt ngẫu nhiên một vùng trong ảnh hoặc thay đổi tỉ lệ.
* Jittering: nối một phần ảnh huấn luyện với một phần nhỏ không liên quan tới ảnh huấn luyện khác. Phần đối tượng chính vẫn được chiếm phần lớn diện tích.

Mỗi phép biến đổi như vậy sẽ có một bộ tham số tương ứng. Do đó, số lượng tổ hợp các phép biến đổi khi thay đổi nhiều bộ tham số khác nhau sẽ rất lớn.

### Kiến trúc mạng

Một cách tổng quát, không có kiến trúc mạng CNN chung cho tất cả các bài toán. Tùy vào tính chất dữ liệu, loại bài toán cần giải quyết mà ta có những thiết kế mạng CNN cho phù hợp. Mẹo nhỏ trong việc thiết kế mạng CNN: khối lượng dữ liệu mẫu và số lượng phân lớp càng lớn thì ta cần xem xét tăng số lượng layer và số lượng neuron.

### Một số cải tiến trong việc huấn luyện

Để tránh hiện tượng quá khớp với dữ liệu, phương pháp cross-validation được áp dụng và tỏ ra khá hiệu quả. Ngoài thuật toán huấn luyện SGD được đề cập ở trên, để tăng tốc độ hội tụ về điểm tối ưu, phương pháp SGD với momentum được được đề xuất như sau:

Trong đó, là hằng số momentum và là hằng số huấn luyện. Hằng số momentum này thường được gán với giá trị . Nếu giá trị này gần với 1 thì tốc độ hội tụ sẽ càng chậm và xấp xỉ bằng phương pháp gradient descent thông thường. Ngoài ra để tăng tốc độ hội tụ, việc khởi tạo giá trị các tham số cũng rất quan trọng.

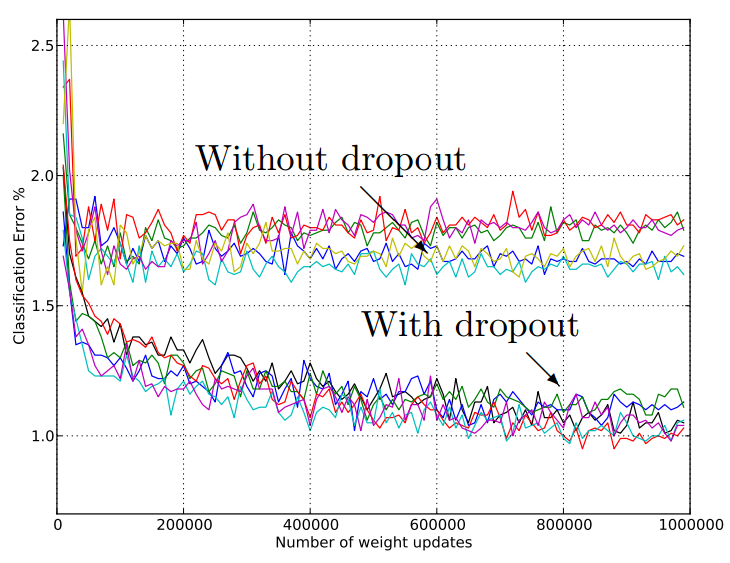
### Phương pháp Dropout

Để tránh hiện tượng mạng CNN quá khớp với dữ liệu huấn luyện, phương pháp *Dropout* được áp dụng [59]. Ý tưởng chính của phương pháp này là loại bỏ ngẫu nhiên một số neuron và những kết nối tương ứng của mạng CNN trong quá trình huấn luyện. Điều này giúp cho các neuron tránh hiện tượng thích nghi đồng thời (co-adaptation) với dữ liệu. Phương pháp đơn giản này giúp giảm một cách đáng kể hiện tượng overfitting và cho kết quả cao hơn so với các phương pháp *regularization* khác. Phương pháp regularization là phương pháp đưa các giá trị của các tham số trong mạng CNN vào trong hàm độ lỗi (hay hàm mục tiêu) để tránh hiện tượng các tham số có giá trị quá lớn dẫn đến chỉ thích nghi với nhiễu của ảnh.

**Thuật toán loan truyền ngược với Dropout:**

* Bước 1: Với mỗi mini-batch lấy ngẫu nhiên từ tập dữ liệu huấn luyện
  + Bước 1.1: Chọn ngẫu nhiên theo phân phối Bernoulli một số neuron để loại bỏ.
  + Bước 1.2: Sử dụng thuật toán lan truyền thuận và lan truyền ngược để tính gradient cho từng tham số. Những neuron bị loại bỏ thì các tham số kết nối với nó có gradient bằng 0.
* Bước 2: Cộng trung bình vector gradient của tất cả các tham số và cập nhật tham số mới.

Bản thân phương pháp Dropout đã cải tiến đáng kể so với các phương pháp huấn luyện truyền thống. Tuy nhiên, khi kết hợp Dropout với các phương pháp khác như momentum, weight decay, regularization, độ chính xác được đẩy lên một cách đáng kể hơn nữa. Hình 4.11 thể hiện sự cải tiến đáng kể khi áp dụng phương pháp Dropout với nhiều cấu hình mạng CNN khác nhau cho tập dataset MNIST. Trục ngang thể hiện số lần cập nhật tham số của mạng. Trục đứng là độ lỗi trong quá trình phân loại chữ số viết tay trên tập test. Không chỉ trên tập MNIST, phương pháp Dropout còn cho kết quả tốt hơn trên rất nhiều các dataset và loại dữ liệu khác nhau như: CIFAR-10, CIFAR-100 (nhận dạng số nhà), IMAGENET (phân loại đối tượng), TIMIT (nhận dạng tiếng nói) và các dataset thuộc lĩnh vực xử lý văn bản khác.



Hình 4.11. Hiệu quả của việc sử dụng phương pháp Dropout giúp làm giảm độ lỗi trong quá trình huấn luyện và phân loại đối tượng.

## MatConvNet

MatConvNet là một dạng cài đặt của nhiều mạng CNN bằng công cụ MATLAB. Thư viện này được thiết kế chú trọng vào sự đơn giản và khả năng hoạt động linh hoạt. Bên cạnh đó, thư viện cũng cung cấp các khối CNN bằng các hàm đơn giản trong MATLAB, cung cấp đoạn chương trình để tính toán các loại tầng phổ biến (đã giới thiệu ở phần trên). Do đó, MatConvNet cho phép xây dựng nhanh những cấu trúc của các CNN, cũng như cung cấp khả năng tính toán hiệu quả trên cả CPU và GPU cho việc huấn luyện trên các tập dữ liệu lớn như ImageNet ILSVRC.

Mỗi mạng CNN đều được xem là một hàm để biến đổi dữ liệu đầu vào thành đầu ra qua một hàm cài đặt . Hàm cài đặt này có thể coi là tổ hợp của một dãy các hàm giản đơn hơn hay còn gọi các khối tính toán (computation blocks). Các khối này có thể chuyển đổi một hình ảnh đầu vào với đặc trưng thành dữ liệu đầu ra bằng việc áp dụng các loại hàm đã được trình bày (như convolution, pooling, ReLU). Thư viện này cũng chứa những cài đặt cần thiết cho các tình huống sử dụng phổ biến nên có thể sử dụng trực tiếp hoặc chỉ gói gọn lại một cách đơn giản hơn. Vì các cấu trúc của các hàm là riêng biệt, việc tạo và kết nối với các khối tính toán mới với các khối tồn tại là hoàn toàn khả thi.

Trong thực tế, vấn đề tối ưu thường được quan tâm khi sử dụng những kiến trúc CNN phức tạp để huấn luyện số lượng mẫu từ hàng trăm nghìn đến hàng triệu mẫu. Thông thường, bài toán tối ưu này thường được giải bằng phương pháp stochastic gradient descent. MatConvNet có thể tính toán những quá trình dẫn xuất của toàn bộ các khối tính toán. Bên cạnh đó, thư viện cũng cung cấp những ví dụ về việc huấn luyện các mẫu dữ liệu lớn và nhỏ, cung cấp khả năng tùy chỉnh mở rộng. Thực tế, tuy các mạng CNN đều rất hiệu quả trong quá trình tính toán, quá trình huấn luyện đòi hủy phải lặp đi lặp lại nhiều lần với các dữ liệu mẫu. Vì thế, tốc độ tính toán là rất quan trọng. Với các mẫu dữ liệu lớn hơn, quá trình huấn luyện sẽ đòi hỏi nhiều tài nguyên hơn trong một giới hạn thời gian cho trước. Vì lí do này, MatConvNet đã tích hợp khả năng xử lý của đơn vị xử lý đồ họa (Graphics Processing Unit – GPU) dựa trên thư viện CUDA của nhà sản xuất NVIDIA và sự hỗ trợ của MATLAB.

Một cách tổng quan, MatConvNet có kiến trúc đơn giản. Thay vì phải bọc lại CNN với những tầng tính toán phức tạp, thư viện sẽ cung cấp những hàm để tính các khối CNN này, chẳng hạn như các toán tử convolution và ReLU. Những khối tính toán này sẽ kết hợp với nhau thành một mạng CNN hoàn chỉnh và cũng có thể sử dụng để cài đặt cho các thuật toán học sâu khác. Trong khi các thư viện khác cung cấp những kiến trúc CNN từ lớn đến nhỏ cùng với những quá trình huấn luyện có sẵn, thư viện MatConvNet cung cấp khả năng tự xây dựng một mạng lưới hoàn chỉnh, bằng cách sử dụng hiệu quả hơn các hàm thư viện trong MATLAB. Vì thế, đây chính là công cụ lý tưởng trong việc nghiên cứu và ứng dụng CNN. Công cụ MatConvNet cung cấp những toán tử tính toán sau:

* Khối tính toán CNN: tập hợp các phương thức tính toán cơ bản một cách tối ưu cho một convolutional neuron. Chẳng hạn, một khối convolution có thể được cài đặt thông qua các hàm có tham số đầu vào như là hình ảnh, filter và bias vector.
* Các khối bọc lại CNN: công cụ MatConvNet cung cấp những hàm cải tiến và tối ưu lại so với CNN, chẳng hạm như phương thức cài đặt CNN với kiến trúc liên kết tuyến tính (một chuỗi các khối tính toán). Phương thức này cho phép chạy hầu hết các mẫu dữ liệu cho việc nhận dạng hình ảnh. Bên cạnh đó, việc mở rộng cài đặt hàm này cũng giúp ích cho việc cài đặt những CNN phức tạp hơn.
* Ứng dụng mẫu: thư viện cung cấp tài liệu hướng dẫn việc sử dụng trên các đơn vị xử lý khác nhau.
* Mẫu dữ liệu huấn luyện trước: thư viện cũng cung cấp những dữ liệu đã được huấn luyện kỹ càng và có thể được tái sử dụng để nhận dạng hình ảnh mà không phải huấn luyện lại.

Các tính năng chính của MatConvNet:

* Tính linh hoạt: các tầng trong mạng neuron được cài đặt trực tiếp, thường là MATLAB code. Do đó, các tầng này có thể dễ dàng thay thế, mở rộng chỉnh sửa hay tích hợp với các tầng khác
* Tính mạnh mẽ: các cài đặt này có thể chạy được với những mẫu dữ liệu mới nhất, bao gồm DeCAF và Caffe hay từ Oxfor Visual Geometry Group. Các dữ liệu được huấn luyện cũng được cung cấp dễ dàng nhằm phục vụ cho các mục đích nghiên cứu khác nhau.
* Tính đóng gói: hầu hết các cài đặt của thư viện đều mang tính đóng gói cao, chỉ đòi hỏi MATLAB và trình biên dịch C/C++ tương ứng (hoặc CUDA nếu sử dụng GPU).

Thực tế, có rất nhiều thư viện cài đặt mã nguồn mở cho CNN. MatConvNet đã sử dụng lại các hàm convolution từ Caffe cũng như khả năng chạy được các mẫu của thư viện Caffe. Trong đó, thư viện Caffe là một thư viện C++ sử dụng CNN tùy chỉnh dựa trên Google Potocol Buffer. Do đó, cả hai thư viện này đều có thể sử dụng cho Cuda-Convnet, cho phép việc định nghĩa kiến trúc của CNN bằng cách sử dụng các tập tin cấu hình. Trong khi Caffe hay Cuda-Convnet đều có thể nhanh hơn MatConvNet, khả năng cung cấp các hàm tính toán CNN riêng lẻ cùng với việc tích hợp sâu vào việc hỗ trợ GPU của MATLAB đã giúp cho công cụ này dễ dàng để sử dụng. Bên cạnh đó, có một vài thư viện sử dụng trong việc huấn luyện và nhận dạng hình ảnh, nhưng lại không sử dụng dễ dàng trong MATLAB.

## Kết chương

Trong phần đầu chương này, chúng tôi trình bày sơ lược về neural network. Từ đó, chúng tôi tập trung trình bày các thành phần chính trong Convolutional Neural Network (CNN), một dạng đặc biệt của neural network được quan tâm nghiên cứu trong thời gian 5 năm gần đây. Từ dữ liệu đặc trưng đầu vào thô, việc sử dụng CNN với nhiều layer cho phép “học sâu” để tìm ra một dạng biểu diễn cấp cao hơn của đặc trưng, phục vụ việc phân lớp hay nhận biết đối tượng. Trong phần cuối chương này, chúng tôi cũng trình bày tóm tắt một công cụ cho phép cài đặt CNN được sử dụng trong đề tài này.

Dựa trên kiến trúc tổng quát và các thành phần thường sử dụng trong CNN, chúng tôi đã đề xuất một họ các CNN để rút trích đặc trưng và nhận biết người dùng thông qua đặc trưng dáng chuyển động, từ đó tiến hành thí nghiệm để chọn ra một thể hiện CNN hiệu quả cho bài toán này. Chi tiết về họ các CNN do chúng tôi đề nghị được trình bày trong Chương 5, và kết quả thử nghiệm trên các tập dữ liệu đặc trưng dáng đi được ghi nhận từ sensor chuyển động được trình bày trong Chương 6.

# 

# Dữ liệu và thử nghiệm nhận biết người dùng bằng đặc trưng dáng đi

**Tóm tắt chương:**

*✍ Nội dung Chương 6 trình bày về các tập dữ liệu được sử dụng để thử nghiệm việc nhận biết người dùng bằng đặc trưng dáng đi. Chúng tôi sử dụng 3 tập dữ liệu, trong đó có 2 tập dữ liệu có sẵn (OU-ISIR Gait Database, Inertial Sensor Dataset và tập dữ liệu Hoang et.al) và 1 tập dữ liệu thực tế do chúng tôi tự xây dựng để đánh giá phương pháp đề xuất.*

*Để tìm ra cấu hình phù hợp và huấn luyện cho convolutional neural network dùng cho việc rút trích và biểu diễn đặc trưng cấp cao cho dáng đi từ dữ liệu thô ghi nhận từ sensor chuyển động, chúng tôi sử dụng OU-ISIR Gait Database, Inertial Sensor Dataset do tập dữ liệu này có số lượng chủ thể khá lớn, đa dạng về độ tuổi và tỉ lệ đồng đều giữa nam và nữ. Việc thử nghiệm giải pháp nhận biết người dùng với Ensemble SVM sử dụng nhiều bộ phân lớp “yếu” SVM được tiến hành trên tập dữ liệu Huang et.al. và tập dữ liệu chúng tôi xây dựng.*

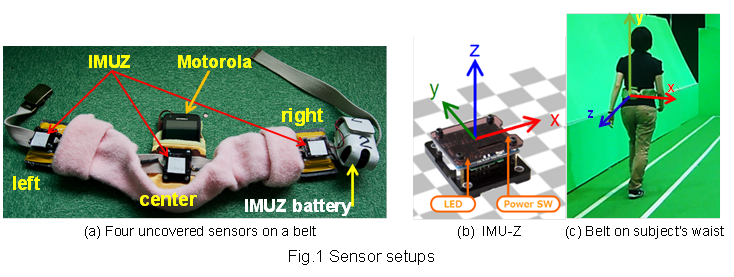
## Các tập dữ liệu thử nghiệm

Trong đề tài này, chúng tôi sử dụng 3 tập dữ liệu để thử nghiệm, bao gồm 2 tập dữ liệu đã được xây dựng sẵn và được công bố trong một số công trình nghiên cứu gần đây và 1 tập dữ liệu do chúng tôi tự xây dựng trong đề tài này.

### OU-ISIR Gait Database, Inertial Sensor Dataset

Tập dữ liệu OU-ISIR Gait Database, Inertial Sensor Dataset của Institute of Scientific and Industrial Research (ISIR), Đại học Osaka (OU). Tập dữ liệu này được công bố lần đầu trong công trình [70], sau đó được chính thức công bố trong công trình [71].

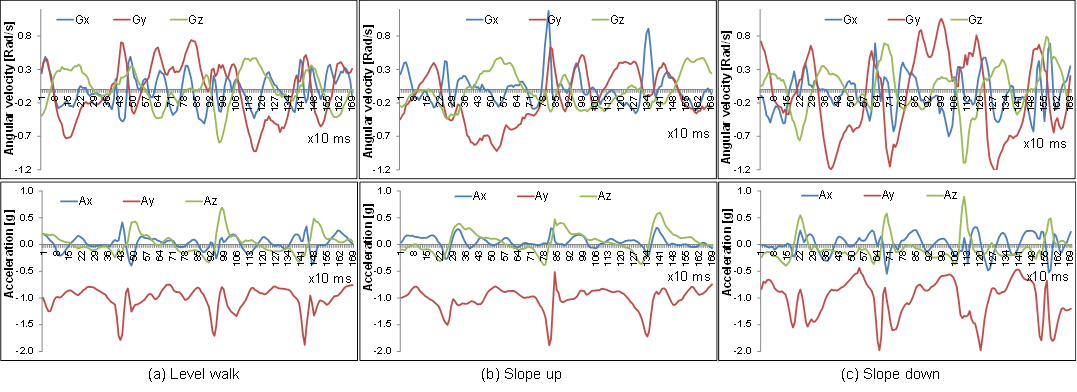
Tập dữ liệu này được xây dựng từ những người tham dự sự kiện 5 ngày được tổ chức tại Tokyo, Nhật Bản vào năm 2011. Sensor được gắn cố định ở phần thắt lưng của mỗi người, bao gồm 4 thiết bị ghi nhận thông tin chuyển động, bao gồm: 3 sensor IMUZ, mỗi sensor đều có gia tốc kế và con xoay hồi chuyển, và 1 smartphone Motorola ME860 chỉ có gia tốc kế (xem Hình 6.1). Một sensor IMUZ và smartphone Motorola được đặt ở chính giữa phía sau lưng của người tham gia thí nghiệm, hai sensor IMUZ còn lại được gắn ở hai bên hông.



Hình 6.1. Cách lắp đặt sensor để thu thập dữ liệu cho OU-ISIR Gait Database, Inertial Sensor Dataset

*(Nguồn:* [*http://www.am.sanken.osaka-u.ac.jp/BiometricDB/InertialGait.html*](http://www.am.sanken.osaka-u.ac.jp/BiometricDB/InertialGait.html)*)*

Các sensor ghi nhận dữ liệu với tần suất 100Hz (lấy mẫu 100 lần/giây). Mỗi người tham gia cung cấp thông tin sẽ di chuyển ở 3 chế độ: đi thẳng, lên dốc và xuống dốc (xem một số ví dụ trong Hình 6.2).



Hình 6.2. Một số ví dụ về dữ liệu ghi nhận trong OU-ISIR Gait Databasem Inertial Sensor Dataset

*(Nguồn:* [*http://www.am.sanken.osaka-u.ac.jp/BiometricDB/InertialGait.html*](http://www.am.sanken.osaka-u.ac.jp/BiometricDB/InertialGait.html)*)*

Trong tập dữ liệu gồm 744 chủ thể (389 nam và 355 nữ), bao gồm 6 độ tuổi: dưới 10 tuổi, từ 10-19 tuổi, từ 20 đến 29 tuổi, từ 30 đến 39 tuổi, từ 40 đến 49 tuổi và trên 50 tuổi. Có thể xem đây là tập dữ liệu ghi nhận từ IMU lớn nhất và có phân bố đều về tỉ lệ nam: nữ và độ tuổi của các chủ thể. Tuy nhiên, đây cũng là tập dữ liệu khó và việc đạt kết quả cao khi nhận biết chủ thể trên tập dữ liệu này là vấn đề đầy thử thách.

### Tập dữ liệu của Hoang et.al

Tập dữ liệu Hoang et.al [73] gồm gồm 38 chủ thể (28 nam và 10 nữ). Tập huấn luyện có 4329 mẫu và tập kiểm thử có 4453 mẫu. Mỗi mẫu có 288 đặc trưng đã được rút trích qua bước tiền xử lí. Dữ liệu được ghi nhận từ Smartphone HTC Google và Nexus One với tần suất lấy mẫu là 27Hz.

# Các hướng tiếp cận chính trong việc xây dựng quy trình chứng thực

**Tóm tắt chương:**

*✍ Trong chương này, chúng tôi sẽ tóm tắt một vài công trình liên quan đến việc xây dựng quy trình chứng thực. Bên cạnh đó, việc đánh giá và phân tích các hướng tiếp cận khác nhau trong những trường hợp khác nhau sẽ giúp chúng ta có được các kinh nghiệm quan trọng giúp ích cho việc đề xuất các cải tiến sau này.*

## Giới thiệu chung

Chứng thực người dùng là một trong những thao tác đầu tiên và quan trọng trong các dịch vụ mạng. Thiếu đi một qui trình chứng thực an toàn sẽ dẫn tới các kết quả tiêu cực cho cả người sử dụng và nhà cung cấp dịch vụ. Đã có rất nhiều công trình về vấn đề này nhằm nâng cao độ an toàn và hiệu quả trong quá trình chứng thực. Từ việc tận dụng định danh, mật khẩu, đặc trưng sinh trắc học cho tới áp dụng các phương pháp mã hóa, một số tồn tại đã hoàn toàn được giải quyết. Tuy nhiên, một vài kết quả chỉ đưa ra các ý tưởng mà chưa thực sự trình bày cụ thể các bước thực hiện; số khác chỉ giải quyết được một vài tình huống đặc biệt.

## Ứng dụng chứng thực

Với sự phát triển không ngừng của các công nghệ mạng, tốc độ truyền dẫn dữ liệu ngày càng được nâng cao và nhiều ứng dụng được triển khai trong các môi trường như thế cũng ngày càng gia tăng. Trong các dịch vụ mạng, cần phải đảm bảo được tính hợp lệ của người dùng trước khi cho họ truy cập vào các tài nguyên hệ thống. Vì vậy, một vài qui trình chứng thực đã được nghiên cứu để tích hợp vào các hệ thống để đảm bảo các giao dịch được an toàn.

***Mạng cảm biến không dây*** (Wireless sensor networks - WSNs) đã trở nên phổ biến rộng rãi vì nó có thể cung cấp các giải pháp kinh tế hơn trong nhiều lĩnh vực công nghiệp [75]. Vì vậy, nhiều nơi đã ứng dụng công nghệ này với nhiều mục tiêu khác nhau như, theo dõi điện áp từ xa trong các nhà máy điện, kiểm soát nhiệt độ và độ ẩm trong các nhà trưng bày và viện bảo tàng, theo vết sức khỏe bệnh nhân tại các trung tâm y tế [76], hoặc hệ thống điều khiển giao thông thời gian thực [77]. Do đó, việc ngăn ngừa thông tin trong các hệ thống này bị truy cập bất hợp pháp là điều rất cần thiết.

Không có một qui trình chứng thực đáng tin cậy, một vài kẻ tấn công có thể phá hủy hoặc khai thác lợi ích từ các thông tin này, ví dụ như những công ty bảo hiểm có thể mua thông tin sức khỏe của bệnh nhân. Bên cạnh độ an toàn, việc chứng thực cũng cần xem xét mức độ tiêu thụ điện năng từ các cảm biến (sensor-nodes) và năng lực tính toán của cổng ra vào (gateway-node) nhằm đáp ứng được càng nhiều người dùng càng tốt.

Bên cạnh mạng cảm biến không dây, các công nghệ giao tiếp như các hệ thống ***GSM, 3G, và 4G*** cũng ngày càng phát triển. Bởi thế, rất nhiều người dùng mong muốn các thiết bị di động của họ (ví dụ như điện thoại, đồng hồ, hoặc máy tính bảng...) có thể sử dụng các dịch vụ đã đăng ký tại quê nhà khi họ đang công tác nước ngoài. Tuy nhiên, nhu cầu này đã đặt ra nhiều vấn đề cần xem xét giải quyết nhằm đảm bảo quyền lợi cho khách hàng và nhà cung cấp dịch vụ. Hai vấn đề quan trọng cần được xem xét trước tiên đó là chứng minh sự hợp lệ định danh và cung cấp tính nặc danh người dùng [78]. Các nhà cung cấp dịch vụ phải cẩn thận kiểm tra định danh nhằm ngăn ngừa các truy cập không hợp lệ. Ngoài ra, việc ẩn đi thông tin định danh khách hàng cũng cần được xem xét thận trọng để bảo vệ quyền riêng tư cho họ. Các thiết bị di động đặc biệt các thiết bị đeo như đồng hồ, mắt kính... rất hạn chế về tài nguyên và năng lực tính toán, nên cần phải đưa ra thiết kế thật hợp lý nhằm cân bằng độ an toàn và tính hiệu quả trong quá trình chứng thực [79].

Trong thực tế, có rất nhiều dịch vụ phần lớn triển khai theo ***kiến trúc khách - chủ*** do tính đơn giản và tập trung. Các dịch vụ này rất đa dạng trong nhiều lĩnh vực như lưu trữ trực tuyến [Z6], ngân hàng internet, hay truyền hình di động trả tiền [123]. Việc chứng thực định danh trong các dịch vụ này là hết sức quan trọng bởi vì nó ảnh hưởng trực tiếp tới quyền lợi của các bên tham gia người dùng, và một thiếu sót nhỏ có thể dẫn tới thiệt hại về tài chính cũng như các hậu quả tiêu cực khác.

Cụ thể trong ***dịch vụ lưu trữ trực tuyến***, người dùng cần chứng minh tính hợp lệ định danh trước khi thực hiện việc lưu trữ hoặc truy cập các tài nguyên trên máy chủ. Do đó, chứng thực thất bại có thể tạo điều kiện cho kẻ mạo danh đánh cắp các tài liệu. Ngoài ra trong lĩnh vực ngân hàng, chứng thực người dùng là một trong những vấn đề đặc biệt được nghiên cứu thận trọng. Chứng thực an toàn cho phép các thủ tục sau đó như rút tiền hoặc chuyển khoản trở nên thuận tiện hơn. Trong dịch vụ truyền hình trả tiền, người dùng có thể xem các chương trình yêu thích bất kỳ thời điểm nào trên thiết bị di động của mình. Vì vậy, nhà cung cấp cần phải có được chính xác định danh người dùng để truyền đúng gói tin cũng như ngăn ngừa việc mạo danh từ bên thứ ba.

## Lưu trữ chứng thực

Có thể nói rằng bất kỳ dịch vụ nào triển khai dưới bất kỳ kiến trúc nào cũng cần đảm bảo kiểm tra được tính hợp lệ của định danh các bên tham gia. Các qui trình được thiết kế tốt thường quan tâm đến ba yếu tố cơ bản: kích thước gói tin trong quá trình chứng thực phải thực sự hợp lí, việc lưu trữ thông tin phục vụ việc kiểm tra định danh nên xem xét hậu quả nếu bị rò rỉ, và cần tính toán chính xác nhằm loại đi các thao tác không cần thiết trong quá trình xử lí thông tin đăng nhập. Trong ba yếu tố đó, yếu tố lưu trữ thông tin phục vụ việc kiểm tra định danh người dùng là quan trọng nhất vì nó liên quan tới tính an toàn của giao thức.

Nhìn chung, các công trình nghiên cứu thường lựa chọn ***thẻ thông minh*** hoặc thiết bị di động, thiết bị đeo để lưu trữ thông tin. Tuy nhiên, hai phương tiện này đều có lợi thế cũng như hạn chế của riêng nó. Trước tiên, chúng ta có thể thấy năng lực tính toán của chúng tương đối thấp. Do đó, các thiết kế qui trình nên hạn chế việc sử dụng các phép toán phức tạp tiêu tốn nhiều thời gian. Với thẻ thông minh, mặc dù một số tác giả đã chứng minh và đưa ra các phương pháp rút trích thông tin từ nó [124][125], nhưng chi phí thực hiện lại quá cao và không khả thi trong thực tế [80]. Vì thế, thông tin trong thẻ thông minh là thực sự an toàn và có một số ý kiến cho rằng với trình độ phát triển công nghệ hiện nay thì không nên quan tâm việc rò rỉ thông tin từ thẻ thông minh.

Ngược lại, dữ liệu lưu trữ trong các ***thiết bị di động*** lại dễ dàng bị đánh cắp do nhiều nguyên nhân khác nhau. Thế nên, nhiều công trình đã xem xét các kịch bản có thể xảy ra do vấn đề rò rỉ thông tin từ các thiết bị này nhằm mục đích bảo vệ an toàn thông tin cho người dùng. Do tính tiện lợi, phổ biến và có thể truy cập bất kỳ thời gian cũng như địa điểm của các thiết bị di động, nhiều dịch vụ đã được tính toán triển khai trên chúng xuất hiện ngày càng nhiều hơn.

Như đã phân tích thì nhu cầu giao tiếp của các dịch vụ mạng ngày càng phát triển. Trước khi cấp phép truy cập, các đối tác cần chứng minh được tính hợp lệ với nhau và secure socket layer (SSL/TLS) từ lâu đã trở thành một qui trình an toàn đáp ứng mục tiêu đó. Tuy vậy, việc triển khai qui trình này đòi hỏi có hạ tầng kỹ thuật cũng như chi phí tính toán cao, điều này sẽ làm giảm số lượng giao dịch của các nhà cung cấp mỗi khi cung cấp dịch vụ. Ý tưởng chính ở đây đó là chỉ sử dụng SSL/TLS một lần ở giai đoạn đăng kí, và sau đó dựa trên những thông tin đó để chứng thực ở giai đoạn cung cấp dịch vụ. Rõ ràng, nếu có một thiết kế hợp lí thì số lượng các giao dịch sẽ tăng lên rất nhiều so với việc áp dụng SSL/TLS trong tất cả các công đoạn.

## Phân loại chứng thực

### Chứng thực thông thường

Một trong những ý tưởng được áp dụng đầu tiên đó là sử dụng mật khẩu người dùng để chứng thực và vào năm 1981, Lamport [81] là người tiên phong hiện thực hóa điều này. Phương pháp chính của ông là sử dụng hàm băm mật mã nhiều lần với mật khẩu và điều này giúp che giấu đi mật khẩu thực sự. Tuy nhiên, kết quả này gặp phải hạn chế đó là việc lưu bảng thông tin kiểm tra phía máy chủ thực sự tạo nguy cơ rò rỉ. Bên cạnh đó, mật khẩu của người dùng thường rất dễ đoán dẫn tới việc qui trình thiếu đi tính an toàn.

Năm 1984, Shamir [82] là người đề xuất ý tưởng sử dụng định danh kết hợp với khóa chủ của nhà cung cấp dịch vụ nhằm tạo nên các khóa riêng cho từng khách hàng. Sự kết hợp này giúp cho việc kiểm tra thông tin đăng nhập của người dùng thực sự dễ dàng do chỉ cần thông tin định danh là đã có thể xác định sự hợp lệ, đồng thời ý tưởng này giúp giảm đi khối lượng tính toán trong trường hợp sử dụng chứng chỉ khóa công. Một số kết quả [83], [84], [85, [86] từ năm 2001 tới 2003 đã áp dụng ý tưởng này vào trong cơ chế của họ nhằm giảm sự phụ thuộc vào việc lưu bảng mật khẩu. Tuy nhiên, các kết quả đó thực hiện truyền định danh tĩnh vô tình tạo nguy cơ bị đánh cắp thông tin từ kẻ tấn công. Do đó, việc kết hợp mật khẩu giúp tăng tính cơ động thông tin ở mỗi lần đăng nhập là thực sự cần thiết. Ngoài ra, việc làm này cũng bảo vệ được tính nặc danh, phù hợp với một số ứng dụng không muốn công khai danh tính khách hàng của họ.

Năm 2004, Das và cộng sự [87] đã thực hiện loại thông tin định danh trong gói tin đăng nhập, thay vào đó họ đã thực hiện thao tác băm mật khẩu kết hợp với một số thông tin khác làm cho gói tin đăng nhập thay đổi mỗi lần truyền đến máy chủ. Với cách làm này thì thông tin định danh đã mất vai trò trong qui trình và khiến nó thực sự dễ bị tổn thương bởi một số hình thức tấn công như đoán mật khẩu, tấn công nội bộ... [88].

Gần đây, nhiều qui trình sử dụng thẻ thông minh như là một phương tiện lưu thông tin người dùng trong quá trình chứng thực, tuy nhiên một vài qui trình lại chưa quan tâm tới vấn đề rò rỉ thông tin từ thiết bị này dẫn tới việc chứng thực không an toàn. Năm 2006, Yoon [89] đề xuất một giải pháp sử dụng thẻ thông minh làm phương tiện cho việc chứng thực và không giống như những công trình trước đó, qui trình của tác giả thực hiện trả về cho người dùng hai khóa, một khóa chứng thực và một khóa mã thông tin mật khẩu. Ngoài ra, tác giả cũng sử dụng nhãn thời gian kết hợp với kỹ thuật bắt tay hai chiều nhằm chống lại hình thức tấn công lặp lại và một số biến thể của nó. Do đó, với cách làm như vậy nếu qui trình muốn áp dụng trong phạm vi lớn thì phải giải quyết vấn đề đồng bộ hóa thời gian. Điều quan trọng còn thiếu sót trong kết quả này là giữa người dùng và máy chủ chưa thống nhất được khóa phiên dành cho việc giao dịch sau khi chứng thực thành công.

Tuy vậy, ý tưởng của Yoon [89] cũng đã làm nền tảng cho nhiều công trình sau này. Năm 2011, Khan và cộng sự [90] cũng vận dụng các ý tưởng này trong qui trình của họ, tuy nhiên tương tự như qui trình trước, qui trình của tác giả cũng phân phối lượng thông tin chung cho mọi người dùng hợp lệ. Chính vì điều này mà thông tin định danh của một người dùng nào đó sẽ bị những người dùng khác tính toán được. Ngoài ra, do việc lưu thông tin khách hàng phía máy chủ mà chưa có một sự tính toán cẩn thận, nên dẫn tới nguy cơ dịch vụ sẽ bị tấn công từ chối dịch vụ do thông tin người dùng bị hiệu chỉnh phía máy chủ.

Năm 2011, Sood [91] cũng đề xuất qui trình chứng thực tương tự, tuy nhiên điểm tiến bộ đó là tác giả bắt đầu sử dụng lượng ngẫu nhiên vào trong khóa của người dùng và với cải tiến này thì các khóa của người dùng thực sự khác nhau tại những thời điểm khác nhau. Do đó, khả năng các hình thức tấn công nội bộ xuất hiện sẽ thấp hơn. Tuy vậy, trong thiết kế này thì vẫn phụ thuộc vào một khóa chung mà máy chủ cung cấp cho tất cả người dùng và điều này đã tạo cơ hội cho tình trạng mạo danh người dùng và máy chủ phát sinh.

Gần đây, Khan [92] đã đề xuất qui trình chứng thực có một vài ưu điểm, như hạn chế khả năng truy vết giao dịch của người dùng, hủy mối quan hệ giữa định danh người dùng và gói tin giao dịch... Tuy nhiên cũng giống như hầu hết các qui trình trước đó, cơ chế của Khan thực sự không an toàn nếu trong trường hợp thông tin định danh khách hàng bị đánh cắp vì về mặt lý thuyết thì khả năng định danh bị lộ ra ngoài là rất lớn nên các qui trình cần phải chuẩn bị kịch bản đối phó với tình huống này. Hơn nữa, qui trình cũng không cung cấp tính nặc danh mạnh như họ phát biểu do việc phát hiện hai gói tin của cùng một người là việc làm rất dễ dàng.

Có thể thấy rằng phần lớn các qui trình theo hướng tiếp cận sử dụng định danh và mật khẩu kết hợp với hàm băm mật mã làm nền tảng gặp một số hạn chế chung như phân phối thông tin chung cho mọi người dùng, sử dụng nhãn thời gian hoặc thiếu giai đoạn thống nhất khóa phiên sau khi chứng thực thành công.

### Chứng thực dựa trên sinh trắc học

Ngoài hướng tiếp cận đã trình bày, vẫn có rất nhiều công trình với nhiều hướng tiếp cận khác nhau nhằm gia tăng độ an toàn và hiệu quả cho bài toán chứng thực và một trong các phương pháp được nhiều tác giả quan tâm đó là sử dụng sinh trắc học như vân tay, mống mắt... Ta có thể thấy rõ ưu điểm của phương pháp này là tính duy nhất của đặc trưng sinh trắc học, ngoài ra thì người dùng cũng không cần phải ghi nhớ thông tin này vì vậy đặc biệt tiện dụng trong quá trình chứng thực. Tuy vậy, nhiều vấn đề như việc rút trích, so khớp và lưu trữ thông tin đặc trưng trong quá trình chứng thực phải được tính toán cẩn thận nhằm hạn chế việc rò rỉ cũng như giả mạo trong quá trình đăng nhập.

Đã có nhiều kết quả nghiên cứu tích hợp đặc trưng này, tiêu biểu năm 2002, Lee [93] là một trong những người đầu tiên đã đề xuất thiết kế sử dụng dấu vân tay, trong công trình này tác giả đã tận dụng đặc trưng sinh trắc học vào quá trình chứng thực. Tuy vậy, Lin [94] đã phân tích và phát hiện ra rằng kết quả của Lee dễ bị tổn thương với hình thức tấn công mạo danh, đồng thời tác giả cũng đề xuất cải tiến. Năm 2007, Khan [95] lại chứng minh được rằng trong kết quả của Lin, kẻ tấn công dễ dàng mạo danh máy chủ đánh lừa người dùng.

Năm 2010, Li và Hwang [96] đã đề xuất qui trình chứng thực sử dụng sinh trắc học kết hợp hàm băm mật mã và lượng ngẫu nhiên. Với thiết kế hợp lí, có thể nói công trình đã tránh được các hạn chế của nhiều đề xuất trước đó và vì vậy nó đã được nhiều tác giả quan tâm đánh giá. Năm 2011, Xiong – Li [97] đã chỉ ra được một số khiếm khuyết khá cơ bản trong thiết kế của Li và Hwang, điển hình là qui trình không có khả năng ngăn ngừa hình thức tấn công người trung gian (Man-in-the-middle [98]). Trong thiết kế này, kẻ thứ ba hoàn toàn có thể tận dụng lại các gói tin sẵn có trên đường truyền và thực hiện gửi riêng lẻ cho người dùng và nhà cung cấp. Ngoài ra một vấn đề cũng cần được xem xét đó là vấn đề đầu ra của hàm băm mật mã. Kết quả của Li và Hwang sử dụng hàm băm trực tiếp với đặc trưng sinh trắc học để so khớp trong quá trình đăng nhập, rõ ràng điều này hoàn toàn không khả thi do tính biến đổi của đặc trưng sinh trắc học dẫn tới việc đầu ra của hàm băm sẽ thay đổi, từ đó việc so khớp sẽ thất bại và đây là vấn đề quan trọng mà các tác giả chưa giải quyết được.

Trong thiết kế, Xiong – Li [97] sử dụng lượng ngẫu nhiên kết hợp kỹ thuật bắt tay hai chiều nhằm phòng ngừa các hình thức tấn công trung gian, lặp lại, nhưng giải pháp này rất khó thực hiện nếu như không nhận được gói tin xác nhận cuối cùng từ người dùng. Vì vậy, tác giả đã đề xuất việc lưu trữ lượng ngẫu nhiên trên máy chủ nhằm nhận biết được gói tin lặp lại. Tuy nhiên, đây là giải pháp không triệt để do kẻ tấn công hoàn toàn có thể chờ đủ lâu để thực hiện việc tấn công. Ngoài ra, việc so khớp với mẫu lưu trữ sẳn cũng là vấn đề mà tác giả chưa giải quyết rõ ràng. Việc mẫu so khớp được lưu trữ tại thẻ người dùng có thể bị đánh cắp, cộng với việc thuật toán so khớp mẫu cũng có thể khiến thời gian chứng thực bị kéo dài dẫn tới giảm số lượng người dùng mà một dịch vụ có khả năng đáp ứng.

Năm 2011, Chen [99] đề xuất qui trình sử dụng dấu vân tay cho thiết bị di động. Kết quả của tác giả có ưu điểm đơn giản rất phù hợp trên môi trường hạn chế về tài nguyên, tuy vậy qui trình không bảo vệ định danh của người dùng đồng thời không có cơ chế ngăn ngừa việc kẻ tấn công đánh cắp định danh thực hiện việc tái đăng ký và điều này dẫn tới các hệ quả tiêu cực. Bên cạnh đó trong quá trình chứng thực, nhà cung cấp dịch vụ hoàn toàn không khởi tạo lượng ngẫu nhiên thách thức tính hợp lệ người dùng và điều này cũng dẫn tới việc khách hàng dễ dàng bị mạo danh. Thêm vào đó cuối giai đoạn chứng thực, thiết bị khách hàng lại phải thay đổi lượng ngẫu nhiên gây lãng phí thời gian cũng như năng lực tính toán của thiết bị do việc thay đổi này hoàn toàn không đóng góp vào độ an toàn trong những lần chứng thực sau đó.

## Thuật toán chứng thực

Ngoài hàm băm mật mã, một số công trình cũng đã sử dụng khoá công làm nền tảng cho quá trình chứng thực, tiêu biểu là hệ thống mã khoá công (public key cryptography – PKC) của Rivest [100] và ElGamal [101]. Đặc trưng của các hệ mã truyền thống này là cần một hạ tầng quản lí các chứng chỉ khoá công của người dùng (Public Key Infrastructure), vì vậy khi số lượng khách hàng gia tăng thì dung lượng lưu trữ cũng như công việc bảo trì sẽ rất phức tạp. Ngoài ra, các hệ thống này sử dụng phép toán mũ lấy dư tiêu tốn nhiều thời gian, trong khi đó các thiết bị di động hoặc đeo tay lại hạn chế về tài nguyên và năng lực tính toán. Vì vậy, những hệ thống này hoàn toàn không phù hợp để triển khai thực tế.

Hệ mã khoá elliptic (Elliptic Curve Cryptography – ECC) lần đầu được đề xuất bởi Miller [102] và Kblitz [103] là một sự thay thế phù hợp bởi vì so với PKC trước đó, nó có thể đạt cùng độ an toàn với kích thước khoá nhỏ hơn, cụ thể 160-bit ECC có cùng cấp độ an toàn với 1024-bit RSA [104]. Tuy nhiên cũng tương tự như PKC, các ECC cũng cần một PKI để lưu trữ các chứng chỉ, do đó ECC cũng còn tồn tại hạn chế mà PKC gặp phải đó là quá trình chứng thực cần tiêu tốn một lượng tính toán cho các chứng chỉ khoá công, tiêu biểu có công trình của Tian [105].

Để giải quyết vấn đề này, Shamir [82] đã đề xuất hệ mã khoá công dựa trên định danh, đây là một ý tưởng rất hợp lí khi người dùng hoàn toàn có thể tận dụng những thông tin cá nhân (như địa chỉ, họ tên, email …) đại diện. Không còn chứng chỉ khoá công, các hệ thống ECC dựa trên định danh cũng không tốn lượng phép toán như các PKC và ECC trước đó và với ý tưởng này, đã có rất nhiều công trình liên tục được đề xuất cải tiến, tiêu biểu có Choie [106] và Wu [107]. Tuy nhiên, các kết quả này đều tận dụng bilinear pairing có chi phí rất cao và vì thế hoàn toàn không phù hợp với các thiết bị hạn chế tài nguyên và năng lực tính toán.

Gần đây, một số công trình [108], [109], [117], [118] đã tận dụng một số tính chất đặc biệt của đường cong elliptic, như vấn đề giai thừa, logarit rời rạc và bài toán Diffie – Hellman. Tiêu biểu vào 2009, Yang [108] đã đề xuất giải pháp tận dụng các tính chất trên, qui trình của tác giả đơn giản và rất hiệu quả về thời gian cũng như độ an toàn.

Tuy nhiên, do bản chất không bảo vệ định danh người dùng trong quá trình giao dịch, đồng thời lại không có cơ chế nào kiểm soát việc táiđăng kýnên không thể áp dụng vào thực tế và vào cùng năm, Yoon [109] đã đề xuất cải tiến dựa trên kết quả của Yang. Trong kết quả nghiên cứu của mình, Yoon đã phân tích và chứng minh rằng cơ chế của Yang không đáp ứng được nhu cầu chứng thực cũng như không sở hữu tính chất an toàn tiến đối với khoá phiên như đã công bố. Tuy vậy, các kết quả của hai tác giả này thực sự không đáp ứng được tính chất trên do trong thiết kế họ đã tận dụng tọa độ điểm để làm khoá phiên sau giai đoạn chứng thực.

Năm 2011, Islam [110] đã phân tích lại một số kết quả trước trong đó có hai công trình trên. Trong kết quả của mình, Islam nhận thấy phần lớn các kết quả sử dụng nhãn thời gian vì vậy sẽ gặp khó khăn trong quá trình đồng bộ hóa và do đó tác giả đã sử dụng lượng ngẫu nhiên kết hợp với kỹ thuật bắt tay ba chiều để tăng tính an toàn cũng như loại bỏ vấn đề đồng bộ hóa thời gian. Thế nhưng, một trong các hạn chế quan trọng trong công trình này là thiết kế phụ thuộc hoàn toàn vào lượng ngẫu nhiên, và vì thế khi thông tin này bị rò rỉ vì lí do nào đó thì các thông tin khoá sẽ bị lộ theo [112].

Ngoài ECC, một số công trình gần đây cũng tập trung áp dụng đa thức Chebyshev [119],[120]. Lợi thế lớn nhất của phương pháp này là các phép toán lượng giác cơ bản, vì vậy chi phí bỏ ra thật sự thấp hơn so với các hướng tiếp cận khoá công trước đó. Cũng như các PKC truyền thống hay ECC, một trong các tính chất quan trọng của đa thức Chebyshev được một số tác giả tận dụng đó là tính đồng nhất, các kết quả thường áp dụng điều này để thực hiện chia sẻ khoá phiên sau pha chứng thực, tiêu biểu vào năm 2003, Kocarev [112] đã đề xuất một hệ mã khóa công dựa trên phương pháp này. Tuy nhiên, Bergamo [113] đã chứng minh được rằng kết quả của Kocarev gặp phải hạn chế đó là kẻ tấn công hoàn toàn có thể truy ngược lại được thông điệp gốc từ thông điệp mã hóa.

Năm 2007 và 2008, Xiao [114] và Yoon [115] đã lần lượt đề xuất các cải tiến từ các phân tích của những kết quả trước đó, tuy vậy cả hai kết quả này đều sử dụng bảng mật khẩu để thực hiện việc kiểm tra người dùng. Điều này dẫn tới nguy cơ thông tin quan trọng rò rỉ sẽ gây ảnh hưởng lớn tới khách hàng cũng như nhà cung cấp dịch vụ.

Guo [116] đã sử dụng hướng tiếp cận này để xây dựng qui trình chứng thực cho dịch vụ giao tiếp không dây (Glomonet) giúp tăng tính hiệu quả về thời gian cho các dịch vụ triển khai trên nền tảng này. Tuy nhiên, kết quả này khó triển khai trong thực tế vì tác giả sử dụng nhãn thời gian nên sẽ gặp phải vấn đề đồng bộ hóa thời gian.

## Mô hình chứng thực

Qua những phân tích như trên, ta thấy mỗi qui trình đều có một số hạn chế nhất định dù có áp dụng những công cụ toán học và mật mã mạnh mẽ tới đâu. Thông qua phương pháp kiểm chứng dựa trên các tình huống tấn công cụ thể mà ta có thể xác định điểm yếu của các qui trình. Có thể nói đây là cách thức tự nhiên và trong tương lai sẽ còn phát triển mạnh. Phần lớn các qui trình cũng dựa vào phương pháp này mà được xây dựng lên. Tuy nhiên, nếu chỉ áp dụng điều này trong việc chứng minh tính an toàn của qui trình là không thể. Lí do đơn giản là tình huống tấn công sẽ thay đổi liên tục và trong tương lai rất có thể qui trình sẽ bị tổn thương bởi một kịch bản tấn công tinh vi nào đó. Như vậy, nhu cầu cần có một phương pháp chứng minh mang tính chất ổn định hơn xuất hiện.

Có rất nhiều mô hình đáp ứng được yêu cầu này và hình thành nên hai mục tiêu chứng minh rất rõ ràng. Thứ nhất là chứng minh tính chính xác của qui trình chứng thực vì thực sự có những qui trình hoàn toàn không chính xác trong các thao tác tính toán [121]. Thứ hai là chứng minh tính an toàn của qui trình chứng thực dựa vào xác suất. Trong yêu cầu tính chính xác, phần lớn mô hình BAN-logic [122] được sử dụng rộng rãi nhờ sử dụng các luật mệnh đề toán học để có thể xác định chính xác các thao tác thực hiện bên trong qui trình. Ý tưởng chính của phương pháp BAN-logic đó là các luật được cấu trúc gồm hai phần, giả thiết và kết luận. Nếu các thao tác của qui trình thỏa mãn yêu cầu của giả thiết này thì sẽ đạt được kết quả ở phần kết luận, nhờ đó mà tính chính xác của qui trình được chứng minh rất rõ ràng và dễ hiểu.

Về yêu cầu tính an toàn của qui trình, mô hình random oracle đang được nhiều tác giả xem xét áp dụng vào kết quả nghiên cứu của họ. Trong mô hình này, kẻ tấn công được cho phép có khả năng truy cập vào một số thủ tục bên trong qui trình thông qua hình thức hỏi đáp. Ngoài ra, mô hình này có hai tham số quan trọng đó là số lần mà kẻ tấn công được hỏi cũng như thời gian thực tế mà kẻ tấn công có thể duy trì. Do tính thực tế này mà rất nhiều tác giả sử dụng để chứng minh tính an toàn cho qui trình chứng thực.

Ý tưởng chính của mô hình random oracle đó là cho phép kẻ tấn công dùng bất kỳ kỹ thuật nào để khai thác điểm yếu của qui trình, miễn sao không vượt quá ngưỡng mà mô hình qui định. Nếu chứng minh được trong phạm vi cho phép mà qui trình vẫn an toàn với xác suất thấp thì tính an toàn đã được chứng minh. Câu hỏi đặt ra là làm sao có thể không quan tâm tới kỹ thuật cụ thể của kẻ tấn công nhưng vẫn đảm bảo tuyệt đối tính an toàn của qui trình. Một trong những phương pháp mà các tác giả thường sử dụng để vượt qua đó là kỹ thuật rút gọn (Reduction). Trong kỹ thuật này thì qui trình sẽ được rút gọn về một nền tảng toán học nào đó mà qui trình này dựa vào, từ đó cho thấy rằng khả năng để kẻ tấn công phá vỡ được nền tảng này là rất thấp từ đó kết luận được với năng lực thực tế thì qui trình hoàn toàn đứng vững được trước tất cả các cuộc tấn công. Vì vậy, tính đúng đắn của quá trình chứng minh hoàn toàn phụ thuộc vào bước rút gọn này, nếu quá trình rút gọn không chính xác sẽ dẫn tới việc ngộ nhận rằng qui trình an toàn trong khi thực tế qui trình có mối liên hệ không chặt chẽ với nền tảng bên dưới.

## Kết chương

Trong lĩnh vực chứng thực người dùng, chúng ta cần quan tâm tới các hướng tiếp cận dựa vào các nền tảng toán học vì đó là hướng tiếp cận đảm bảo cho qui trình được an toàn. Ngoài ra, việc thiết kế cũng cần phải hợp lí, chính xác và an toàn vừa đủ nhằm đảm bảo hiệu quả về mặt thời gian và năng lực tính toán của các thiết bị di động, thiết bị đeo. Khi công nghệ ngày càng phát triển thì những qui trình cũng cần ngày càng cải tiến và thay đổi để có khả năng đứng vững trước những cuộc tấn công trong tương lai.

# Quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc và hệ thống truy cập dịch vụ trực tuyến

**Tóm tắt chương:**

*✍ Trong Chương 8, chúng tôi đề xuất quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc, từ đó áp dụng để xây dựng hệ thống cho phép truy cập thông tin và các dịch vụ trực tuyến với chứng thực sử dụng thiết bị di động và đặc trưng dáng đi. Quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc được chúng tôi cải tiến từ quy trình chứng thực dựa trên đặc trưng vân tay của Khan* [146]. *Quy trình chứng thực cho hệ thống tương tác thông minh được xây dựng trên cơ sở điều chỉnh quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc và cải tiến quy trình chứng thực dựa trên sinh trắc học của Khan* [147] *để áp dụng vào hệ thống tương tác thông minh*.

## Chứng thực với sinh trắc học

Đặc trưng sinh trắc học là một đặc trưng có độ ngẫu nhiên (entropy) cao. Vì vậy, sử dụng đặc trưng này trong quá trình chứng thực và quản lý định danh có nhiều ưu điểm, ví dụ: (i) không thể bị mất hoặc quên; (ii) khó sao chép hay bị chia sẻ một cách bất hợp pháp; (iii) khó giả mạo; (iv) không thể đoán một cách dễ dàng [150].

Những phương pháp chứng thực dựa trên dữ liệu sinh trắc học như vân tay, móng mắt, giọng nói là những xu hướng phổ biến để khai thác đặc trưng sinh trắc của cơ thể con người cho mục đích xác định định danh.

Chúng tôi chọn đặc trưng vân tay làm nhân tố sinh trắc học và thiết kế một quy trình chứng thực phù hợp với hệ thống tương tác thông minh. Hệ thống của chúng tôi khai thác đặc trưng vân tay – đặc điểm nhận dạng phố biến và đã được hỗ trợ trong nhiều thiết bị để định danh và chứng thực người dùng. Bằng phương pháp này, người dùng không những có thể sử dụng những tiện ích trên hệ thống mà còn có thể truy cập những dịch vụ trực tuyến khác mà không cần phải đăng nhập nhiều lần.

Vân tay của người dùng là nhân tố quyết định tính an toàn của hệ thống mà chúng tôi xây dựng. Sử dụng chứng thực định danh dựa trên vân tay giảm đi những nguy cơ như khi dùng phương pháp chứng thực bằng mật khẩu, hoặc thẻ chứng thực như thẻ RFID, NFC, vì mật khẩu và thẻ có thể bị mất/quên hoặc bị đánh cắp.

## Đề xuất quy trình chứng thực hai chiều dựa trên đặc trưng sinh trắc

### Đề xuất quy trình chứng thực

Trong phần này, chúng tôi đề xuất một quy trình chứng thực mới, khắc phục những điểm yếu mà quy trình chứng thực do nhóm của Khan đề xuất còn gặp phải. Quy trình chứng thực của chúng tôi đề xuất kế thừa những ưu điểm trong quy trình chứng thực của Khan, đồng thời thay đổi những điểm thiết kế chưa chặt chẽ trong quy trình chứng thực của họ để tăng độ an toàn.

Trước khi đi vào chi tiết, chúng tôi trình bày ý tưởng chính của quy trình chứng thực mà chúng tôi đề xuất một cách tổng quan. Trong pha đăng ký, mục tiêu chính là cung cấp cho người dùng hai khóa bí mật h(IDS || e || x) và h(IDi || x || e || IDS ). Trong đó, giá trị ngẫu nhiên e để chống lại kiểu tấn công đăng ký lại, IDi được đưa vào hàm băm để chống người dùng trích thông tin đăng nhập của mình sau đó thay đổi ID để mạo danh người dùng khác. Trong pha đăng nhập và chứng thực, chúng tôi sử dụng hai giá trị ngẫu nhiên NU (được ẩn trong C1) và NS (được ẩn trong S1) để người dùng và máy chủ thử thách lẫn nhau. Ngoài ra, giá trị ngẫu nhiên NU còn có chức năng làm thay đổi định danh của người dùng mỗi lần đăng nhập. Sau khi chứng thực thành công, hai bên có thể thống nhất khóa phiên để mã hóa thông tin giao tiếp.

Quy trình chứng thực của chúng tôi cũng được chia làm bốn pha: đăng ký, đăng nhập, chứng thực hai phía và thay đổi mật khẩu. Tuy nhiên chúng tôi không trình bày giao pha thay đổi mật khẩu bởi vì pha này giống với pha thay đổi mật khẩu trong quy trình chứng thực của Khan đề xuất.

**A. Pha đăng ký**

Pha đăng ký có bốn yêu cầu cơ bản: kênh truyền giữa người dùng và máy chủ là kênh truyền an toàn; mật khẩu thật sự của người dùng phải được giữ bí mật, kể cả phía máy chủ cũng không được biết thông tin này; khóa bí mật máy chủ chia sẻ cho mỗi người dùng phải khác nhau; định danh phải được kết buộc bằng khóa bí mật của máy chủ. Từ những gì đã phân tích, quy trình chứng thực của Khan đảm bảo ba yêu cầu đầu tiên nhưng chưa đảm bảo được yêu cầu cuối cùng. Vì vậy, trong quy trình chứng thực đề xuất, chúng tôi sẽ sửa đổi điểm này để có được pha đăng ký tốt hơn.

|  |  |  |
| --- | --- | --- |
| **Người dùng Ui** |  | **Máy chủ S** |
| **Pha đăng ký** |  |  |
| Chọn IDi, PW |  |  |
| Quét vân tay Fi |  |  |
| Chọn lượng ngẫu nhiên N,  Tính hpw = h(PW || N || Fi) | {IDi, hpw, Fi} | Bi = h(hpw || Fi || IDi) ⊕ e  Ci = h(IDi || hpw || Fi) ⊕ h(IDS || h(e) || x) |
|  |  | Ei = h(Fi || hpw || IDi) ⊕ h(IDi || x || h(e) || IDS) |
|  | {Bi, Ci, Ei, Vi, h(.), hk(.)} | Vi = hh(IDi || x || h(e) || IDS)(hpw) |
| Lưu lại {Bi, Ci, Ei, Vi, h(.), hk(.)} và N vào thiết bị di động |  |  |

Hình 8‑1 - Pha đăng ký của quy trình chứng thực đề xuất

Khi muốn đăng ký với nhà cung cấp dịch vụ, người dùng phải chọn định danh IDi, quét vân tay qua thiết bị cảm biến, tính hpw = h(PW || N || Fi). Sau đó, người dùng gửi {IDi, hpw, N} cho máy chủ. Hình 8.1 mô tả các bước trong pha đăng ký.

* Bước 1: Khi nhận được yêu cầu đăng ký của người dùng, máy chủ S tạo giá trị ngẫu nhiên e. Giá trị ngẫu nhiên e để đảm bảo khóa bí mật của mỗi người dùng là khác nhau.
* Bước 2: Máy chủ tính Bi = h(hpw || Fi || IDi) ⊕ e, Ci = h(IDi || hpw || Fi) ⊕ h(IDS || h(e) || x), Ei = h(Fi || hpw || IDi) ⊕ h(IDi || x || h(e) || IDS), Vi = hh(IDi || x || h(e) || IDS)(hpw). Trong đó, Bi chứa giá trị ngẫu nhiên e, Ci và Ei chứa khóa bí mật máy chủ chia sẻ cho người dùng, Vi là thông tin kiểm tra mật khẩu khi người dùng đăng nhập.
* Bước 3: Máy chủ gửi {Bi, Ci, Ei, Vi, h(.), hk(.)} cho người dùng. Nhận được thông tin từ máy chủ, người dùng lưu toàn bộ thông tin này và N vào thiết bị di động.

**B. Pha đăng nhập**

Khi muốn đăng nhập với máy chủ, người dùng Ui nhập định danh IDi, mật khẩu PWi của mình và quét vân tay qua thiết bị cảm biến để đăng nhập. Sau đó, thiết bị di động của người dùng thực hiện các bước sau:

* Bước 1: Tính hpw = h(PW || N || Fi), Ai = h(Fi || hpw || IDi­) ⊕ Ei, so sánh hAi(hpw) với Vi. Nếu hai giá trị này không bằng nhau, thiết bị di động kết thúc phiên làm việc, ngược lại, người dùng được phép thực hiện bước tiếp theo.
* Bước 2: Thiết bị di động tạo lượng ngẫu nhiên NU và tính e = h(hpw || Fi || IDi) ⊕ Bi, C0 = h(IDi || hpw || Fi) ⊕ Ci ⊕ NU, C1 = hAi(NU), RCID = IDi ⊕ h(NU). Trong đó, RCID là định danh động, chứa định danh IDi của người dùng; C0 chứa lượng ngẫu nhiên NU và máy chủ tính lại được NU từ giá trị C0 này; C1 chứa thông tin khóa bí mật của người dùng kết hợp với lượng ngẫu nhiên để máy chủ kiểm tra tính hợp lệ của người dùng.
* Bước 3: Thiết bị di động gửi {h(e), RCID, C0, C1} lên cho máy chủ để yêu cầu đăng nhập.

**C. Pha chứng thực hai phía và thống nhất khóa phiên**

|  |  |  |  |
| --- | --- | --- | --- |
| **Người dùng Ui** |  | | **Máy chủ S** |
| **Pha đăng nhập** |  | | **Pha chứng thực** |
| Nhập IDi, PW và vân tay Fi |  | |  |
| hpwh(PW || N || Fi) |  | |  |
| Aih(Fi || hpw || IDi­) ⊕ Ei |  | |  |
| Kiểm tra nếu hAi(hpw) = Vi | {h(e), RCID, C0, C1} | |  |
| Nếu đúng,  eh(hpw || Fi || IDi) ⊕ Bi,  tạo lượng ngẫu nhiên N­U |  | | NU\*C0 ⊕ h(IDS || h(e) || x)  IDi\*RCID ⊕ h(NU\*)  Kiểm tra IDi\* |
| C0 h(IDi || hpw || Fi)⊕Ci⊕ NU  RCIDIDi ⊕ h(NU) |  | | Tính Ai\* = h(IDi\* || x || h(e) || IDS)) và so sánh C1 với hAi\*(NU\*) |
| C1hAi(NU) |  | | Nếu bằng nhau thì tạo lượng ngẫu nhiên NS, tính |
|  | {NS, S1} | | S1h( Ai\* || NU\* || NS || h(e) || IDi\*) |
|  |  | |  |
| So sánh S1 với  h(Ai || NU || NS || h(e) || IDi) | |  |  |
| Nếu bằng nhau,  S2 = h(NU || IDi || Ai || NS || h(e)) | {S2} | |  |
|  |  | | So sánh  S2 với h(NU\* || IDi\* || Ai\* || NS || h(e))  nếu bằng nhau |
| SK = h(NU ||NS|| h(e)|| IDi || h(Ai)) |  | | SK = h(NU\* || NS || h(e) || IDi\* || h(Ai\*)) |

Hình 8‑2 - Pha đăng nhập và chứng thực hai phía của quy trình chứng thực đề xuất

Trong pha này, chỉ có máy chủ có hai khóa bí mật x và IDS mới trích được lượng ngẫu nhiên NU của người dùng để đáp lại thử thách từ phía người dùng. Máy chủ không những phải kiểm tra tính hợp lệ của thông tin nhận được mà còn phải tạo lượng ngẫu nhiên N­S để thử thách lại người dùng. Sau khi chứng thực thành công, hai bên thống nhất được với nhau khóa phiên để làm việc.

Khi nhận được yêu cầu đăng nhập có chứa thông tin {e, RCID, C0, C1} từ phía người dùng, máy chủ S và thiết bị di động của người dùng Ui thực hiện các bước sau để chứng thực lẫn nhau. Hình 8.1 mô tả các bước trong pha chứng thực.

* Bước 1: Máy chủ S trích NU\* = C0 ⊕ h(IDS || h(e) || x), IDi\* = RCID ⊕ h(NU\*), sau đó S kiểm tra tính hợp lệ của định danh IDi\*. Nếu định danh hợp lệ, S tính Ai\* = h(IDi\* || x || h(e) || IDS)) và so sánh hAi(NU\*) với C1. Nếu hai giá trị này bằng nhau thì S tạo lượng ngẫu nhiên NS và tính S1 = h( Ai\* || NU\* || NS || h(e) || IDi\*) và gửi lại {NS, S1} cho người dùng.
* Bước 2: Khi thiết bị di động của người dùng nhận được {NS, S1} từ máy chủ, thiết bị di động tính và so sánh h(Ai || NU || NS || h(e) || IDi) vơi S1 nhận được. Nếu hai giá trị này bằng nhau, thiết bị di động tính tiếp S2 = h(NU || IDi || Ai || NS || h(e)) để đáp lại thử thách từ phía máy chủ.
* Bước 3: Khi nhận được S2 từ người dùng, máy chủ tính và so sánh h(NU\* || IDi\* || Ai\* || NS || h(e)) với S2. Nếu bằng nhau, máy chủ chấp nhận yêu cầu đăng nhập của người dùng. Máy chủ tính được khóa phiên SK = h(NU\* || NS || h(e) || IDi\* || h(Ai\*)). Thiết bị di động của người dùng tính được khóa phiên SK = h(NU || NS || h(e)|| IDi || h(Ai)).

### Chứng minh tính an toàn

Trong phần này, chúng tôi sẽ chứng minh rằng quy trình chứng thực mới đề xuất an toàn hơn quy trình chứng thực mà Khan đề xuất, đồng thời chống được nhiều kiểu tấn công phổ biến.

Một quy trình chứng thực an toàn không những phải chống được kẻ tấn công mạo danh mà còn phải bảo vệ thông tin của người dùng và máy chủ. Chúng tôi luôn giả định rằng tất cả thông tin được gửi xuống đường truyền không an toàn đều có thể bị kẻ tấn công thu thập. Hơn nữa, thông tin lưu trên thiết bị di động của người dùng có thể bị rò rỉ hay bị đánh cắp và kẻ tấn công có thể dùng những thông tin này để mạo danh máy chủ hay người dùng. Kẻ tấn công có thể kết hợp tất cả những thông tin mà mình thu thập được theo nhiều cách khác nhau và kết hợp nhiều kiểu tấn công để tấn công cùng một lúc. Vì vậy, trong khi thiết kế quy trình chứng thực, người thiết kể phải tính trước các trường hợp có thể xảy ra để có được một quy trình chứng thực an toàn. Trong phần này, chúng tôi sẽ giải thích thiết kế của quy trình chứng thực được đề xuất khác biệt và tốt hơn thiết kế của Khan như thế nào. Sau đó, chúng tôi thử áp dụng các kiểu tấn công mà quy trình chứng thực của Khan còn gặp phải cũng như một số kiểu tấn công phổ biến khác lên quy trình chứng thực đề xuất.

Trong các quy trình chứng thực, càng nhiều thông tin lưu lại trên thiết bị di động của người dùng sẽ cung cấp càng nhiều thông tin cho kẻ tấn công khi các thông tin này bị đánh cắp hay bị rò rỉ. Vì vậy, người thết kế quy trình chứng thực cần hạn chế tối đa việc lưu lại các giá trị dư thừa, không cần thiết trong thiết bị di động của người dùng. Trong quy trình chứng thực của Khan đề xuất, các thông tin lưu trên thiết bị di động của người dùng được tính toán chưa chặt chẽ. Việc lưu lại giá trị R­i trên thiết bị của người dùng là dư thừa vì người dùng có thể tự tính lại h(IDi ⊕ h(x || e || IDS)) bằng cách trích h(x || e || IDS) từ Ei sau đó kết hợp với ID­i của mình. Trong quy trình chứng thực đề xuất, chúng tôi loại bỏ giá trị Ri để tránh lưu lại giá trị dư thừa trên thiết bị di động của người dùng.

Điểm yếu tiếp theo trong thiết kế của Khan là tất cả những thông tin quan trọng do máy chủ chia sẻ với người dùng đều được ẩn bằng phép XOR với hpw. Với cách thiết kế này, kẻ tấn công chỉ cần thực hiện phép toán XOR giữa hai trong các giá trị Bi, Ci, Ei, Ri­ thì hpw sẽ mất đi và để lộ ra nhiều thông tin quan trọng mà kẻ tấn công có thể khai thác được. Trong quy trình chứng thực chúng tôi đề xuất, những thông tin máy chủ chia sẻ với người dùng được ẩn vào các giá trị khác nhau. Chúng tôi băm hpw kết hợp với IDi và Fi, thứ tự các giá trị này trong hàm băm được thay đổi để ẩn các giá trị khác nhau. Vì vậy, việc XOR hai giá trị bất kỳ chỉ đánh rối thêm nên không thể thu được những thông tin thực sự mà máy chủ chia sẻ cho người dùng.

Một thông tin được máy chủ chia sẻ cho tất cả người dùng là không an toàn. Cụ thể, quy trình chứng thực của Khan đề xuất lưu lại Ci = hpw ⊕ h(x || IDS). Trong đó, h(x || IDS) là thông tin được chia sẻ cố định cho mọi người dùng và được ẩn bằng phép XOR với hpw. Khi thông tin lưu trên thiết bị di động của người dùng bị rò rỉ, kẻ tấn công là một người dùng hợp lệ khác có thể trích hpw của Ui bằng cách XOR Ci với h(x || IDS) - trích từ thông tin máy chủ chia sẻ với mình. Như vậy, kẻ tấn công tính được hpw của người dùng mà không cần biết mật khẩu, vân tay và lượng ngẫu nhiên của người dùng. Sau đó, kẻ tấn công có thể trích toàn bộ những thông tin khác được ẩn bằng phép XOR với hpw trong Bi, Ci, Ei, Ri­ và dễ dàng mạo danh người dùng Ui. Trong quy trình chứng thực chúng tôi đề xuất, các thông tin máy chủ chia sẻ cho mỗi người dùng đều khác nhau. Hai giá trị bí mật x và IDS được kết hợp với giá trị ngẫu nhiên e để chia sẻ h(IDS || h(e) || x) thay vì chia sẻ h(x || IDS) như quy trình chứng thực của Khan. Vì vậy, kẻ tấn công không thể trích thông tin máy chủ chia sẻ cho mình để kết hợp với thông tin đánh cắp từ người dùng khác nhằm mục đích mạo danh.

Một điểm yếu nữa trong thiết kế của quy trình chứng thực mà Khan đề xuất là không kết buộc ID của người dùng với khóa bí mật của máy chủ, dẫn đến người dùng có thể tự thay đổi ID để mạo danh người dùng khác. Trong quy trình chứng thực chúng tôi đề xuất, giá trị Ei = h(Fi || hpw || IDi) ⊕ h(IDi || x || h(e) || IDS) là giá trị ẩn thông tin h(IDi || x || h(e) || IDS), người dùng phải có được h(IDi || x || h(e) || IDS) mới chứng thực được với máy chủ. Hơn nữa, người dùng không thể thay đổi ID vì không có x và IDS.

Tiếp theo, chúng tôi chứng minh quy trình chứng thực đề xuất chống được nhiều kiểu tấn công khác nhau. Trong đó, quy trình chứng thực đề xuất chống được những kiểu tấn công mà quy trình chứng thực của Khan chống được do kế thừa những ưu điểm từ quy trình chứng thực này. Đồng thời, quy trình chứng thực đề xuất có những cải tiến để chống lại những kiểu tấn công mà quy trình chứng thực của Khan còn gặp phải.

**1) Tấn công lặp lại:** Quy trình chứng thực của chúng tôi kế thừa từ quy trình chứng thực của Khan, sử dụng lượng ngẫu nhiên kết hợp kỹ thuật bắt tay ba bước để chống lại kiểu tấn công lăp lại. Ví dụ, kẻ tấn công A có thể gửi lại {e, RCID, C0, C1} cho máy chủ S. Sau đó, máy chủ gửi lại {NS, S1} cho A. Vì kẻ tấn công A không biết lượng ngẫu nhiên NU và h(IDi || x || h(e) || IDS) nên không thể tính được S2­ để gửi lại cho S. Vì vậy, S có thể nhận biết được có ai đó đang mạo danh người dùng Ui và kết thúc phiên làm việc.

**2) Tấn công mạo danh người dùng do rò rỉ định danh:** Quy trình chứng thực của chúng tôi chống được kiểu tấn công mạo danh người dùng do rò rỉ định danh. Khác với quy trình chứng thực của Khan, trong quy trình chứng thực được đề xuất, định danh IDi được đưa vào hàm băm với hai giá trị bí mật x và IDS của máy chủ và người dùng cần phải sử dụng giá trị băm này để chứng thực với máy chủ. Vì vậy, dù định danh người dùng bị lộ, kẻ tấn công cũng không tính được h(IDi || x || h(e) || IDS) do không có hai giá trị bí mật x và IDS nên không mạo danh được người dùng.

**3) Tấn công mạo danh người dùng và máy chủ khi có được gói tin đăng nhập và rò rỉ thông tin lưu trong thiết bị di động của người dùng:** Trong quy trình chứng thực đề xuất, các giá trị lưu trên thiết bị di động và thông điệp được gửi đi đã được tính toán trước. Không giống như quy trình chứng thực Khan đề xuất, các khóa bí mật máy chủ chia sẻ cho mỗi người dùng đều khác nhau và khi XOR từ hai giá trị trở lên với nhau chỉ làm rối thêm và không thể suy ra được khóa bí mật mà máy chủ chia sẻ với người dùng. Cụ thể trong quy trình chứng thực đề xuất, chúng tôi lưu lại {Bi, Ci, Ei, Vi, h(.), hk(.), N} trên thiết bị di động. Trong quá trình chứng thực, người dùng và máy chủ gửi cho nhau {e, RCID, C0, C1, NS, S1, S2}. Giả định rằng, kẻ tấn công có tất cả các thông tin trên, kẻ tấn công cũng không thể suy ra được thêm bất cứ thông tin gì khác của người dùng. Vì vậy, kẻ tấn công không thể mạo danh người dùng và máy chủ.

**4) Tấn công đoán mật khẩu:** Khan đề xuất sử dụng phép toán NOR để tránh kẻ tấn công trích được Fi từ hpw để đoán mật khẩu. Chúng tôi không sử dụng phép NOR nhưng thay vào đó, chúng tôi đưa Fi và trong hàm băm với PW. Với cách này, kẻ tấn công cũng không thể trích được Fi cũng như không có cơ sở để kiểm tra mật khẩu đoán được có đúng không và không trích được các thông tin quan trọng khác của người dùng. Vì vậy, quy trình chứng thực vẫn an toàn khi mật khẩu do người dùng đặt là mật khẩu yếu.

**5) Bảo vệ tính nặc danh của người dùng:** Người dùng gửi {e, RCID, C0, C1} cho máy chủ mỗi lần đăng nhập. Vì vậy, kẻ tấn công có thể bắt và phân tích gói tin đăng nhập. Kẻ tấn công không thể trích được ID­i nếu không có hai giá trị bí mật của máy chủ. Hơn nữa, thông điệp đăng nhập thay đổi mỗi lần người dùng đăng nhập do được kết hợp với lượng ngẫu nhiên NU. Vì vậy, kẻ tấn công không thể xác định được ai đang cố gắng đăng nhập với máy chủ. Nói theo cách khác, quy trình chứng thực chúng tôi đề xuất bảo vệ được tính nặc danh của người dùng.

**6) Chứng thực hai phía:** Trong pha đăng ký của quy trình chứng thực chúng tôi đề xuất, máy chủ S cung cấp cho người dùng hai khóa h(IDS || h(e) || x) và h(IDi || h(x) || e || IDS). Trong pha đăng nhập, người dùng ẩn lượng ngẫu nhiên NU vào khóa bí mật để chứng minh mình đang sở hữu khóa bí mật mà máy chủ chia sẻ. Đồng thời, máy chủ phải có hai giá trị bí mật mới trích được thông tin khác để kiểm chứng người đăng nhập. Sau đó, máy chủ thử thách lại người dùng bằng lượng ngẫu nhiên NS. Nếu người dùng hợp lệ, người dùng có thể tính được S2 để gửi lại cho S.

**7) Thống nhất khóa phiên:** Trong quy trình chứng thực chúng tôi đề xuất, sau khi chứng thực hai bên thành công, cả máy chủ và người dùng đều tính được khóa phiên SK để thiết lập phiên làm việc an toàn. Vì vậy, thông tin giao tiếp giữa người dùng và máy chủ sau pha chứng thực có thể được mã hóa để tránh kẻ tấn công đọc được nội dung.

Trong Bảng 8.1, chúng tôi so sánh giữa quy trình chứng thực được đề xuất và quy trình chứng thực của Khan về khả năng chống lại nhiều kiểu tấn công. Như đã phân tích, quy trình chứng thực của Khan không thể chống lại kiểu tấn công giả mạo người dùng và máy chủ, tấn công do rò rỉ định danh, tấn công sử dụng thông tin gói tin đăng nhập và thông tin trên thiết bị di động bị đánh cắp, tấn công do người dùng bên trong hệ thống. Có thể thấy rằng, quy trình chứng thực của chúng tôi an toàn hơn trước nhiều kiểu tấn công.

|  |  |  |
| --- | --- | --- |
| Kiểu tấn công | Quy trình chứng thực | |
| Của Khan | Của chúng tôi |
| Tấn công do rò rỉ định danh | Không | Có |
| Tấn công lặp lại | Có | Có |
| Tấn công giả mạo người dùng | Không | Có |
| Tấn công giả mạo máy chủ | Không | Có |
| Tấn công sử dụng gói tin đăng nhập | Không | Có |
| Tấn công do đánh cắp thiết bị di động | Không | Có |
| Tấn công đoán mật khẩu | Có | Có |
| Tấn công do người dùng bên trong hệ thống | Không | Có |

Bảng 8.1. So sánh về khả năng chống lại nhiều kiểu tấn công

### Phân tích hiệu quả của quy trình chứng thực

Trong phần này, chúng tôi chỉ ra rằng dù chi phí tính toán có tăng so với quy trình chứng thực của Khan, quy trình chứng thực mới đề xuất vẫn đảm bảo được tính hiệu quả và không tiêu tốn quá nhiều chi phí cũng như năng lực xử lý của thiết bị di động.

Để so sánh tính hiệu quả giữa quy trình chứng thực của chúng tôi và quy trình chứng thực của Khan đề xuất, chúng tôi sử dụng lại hướng tiếp cận của Khan, đó là tính số lượng phép băm một chiều được sử dụng. Thêm vào đó, tương tự với cách của Khan, chúng tôi bỏ qua phép toán XOR bởi vì phép toán này tiêu tốn rất ít chi phí. Trong Bảng 8.2, chúng tôi so sánh số phép băm một chiều được sử dụng trong quy trình chứng thực của chúng tôi và quy trình chứng thực do Khan đề xuất. Quy trình chứng thực của Khan cần 5h(.) trong pha đăng ký, 4h(.) trong pha đăng nhập và 9h(.) trong pha chứng thực. Quy trình chứng thực của chúng tôi đề xuất cần 8h(.) trong pha đăng ký, 8h(.) trong pha đăng nhập và 8h(.) trong pha chứng thực.

|  |  |  |  |
| --- | --- | --- | --- |
| Quy trình chứng thực | Pha đăng ký | Pha đăng nhập | Pha chứng thực |
| Quy trình chứng thực của Khan | 5h(.) | 4h(.) | 9h(.) |
| Quy trình chứng thực chúng tôi đề xuất | 8h(.) | 8h(.) | 8h(.) |

Bảng 8.2. So sánh chi phí tính toán

Có thể thấy quy trình chứng thực chúng tôi đề xuất cần nhiều chi phí tính toán hơn quy trình chứng thực của Khan đề xuất. Tuy nhiên, những chi phí tính toán này là cần thiết để bảo vệ tính nặc danh của người dùng, tránh trường hợp kẻ tấn công XOR các giá trị với nhau để suy ra thông tin khác và để thống nhất khóa phiên. Dựa vào bảng so sánh, chúng tôi nhận thấy quy trình chứng thực đề xuất không thêm quá nhiều phép băm một chiều so với quy trình chứng thực của Khan. Điều quan trọng là, quy trình chứng thực của chúng tôi đề xuất an toàn hơn quy trình chứng thực mà Khan đề xuất.

Trong Bảng 8.3, chúng tôi so sánh giữa quy trình chứng thực được đề xuất và quy trình chứng thực của Khan về mặt các đặc tính thân thiện. Quy trình chứng thực của chúng tôi đề xuất không chững thỏa mãn toàn bộ những đặc tính mà quy trình chứng thực của Khan có mà còn cung cấp thêm đặc tính quan trọng mà quy trình chứng thực của họ không có, đó là bảo mật trên ba nhân tố chính.

Từ toàn bộ những so sánh đã nêu, chúng tôi thấy rằng việc tăng thêm một số lượng không đáng kể là 6 phép băm so với quy trình chứng thực của Khan, quy trình chứng thực đề xuất đã đạt được những đặc tính an toàn và thân thiện đáng kể.

|  |  |  |
| --- | --- | --- |
| Đặc tính | Quy trình chứng thực | |
| Của Khan | Của chúng tôi |
| Tính nặc danh người dùng | Có | Có |
| Chứng thực hai phía | Có | Có |
| Thống nhất khóa phiên | Có | Có |
| Không lưu bảng mật khẩu phía máy chủ | Có | Có |
| Phát hiện sai mật khẩu sớm | Có | Có |
| Thay đổi mật khẩu tự do | Có | Có |
| Bảo mật dựa trên ba nhân tố chính | Không | Có |

Bảng 8.3. So sánh về các đặc tính thân thiện

### Tổng kết phần đề xuất quy trình chứng thực dựa trên sinh trắc

Mục tiêu quan trọng nhất trong quá trình chứng thực chính là cần biết chính xác cả định danh của người dùng lẫn sự hợp lệ của máy chủ. Ngoài ra, việc đảm bảo tính toàn vẹn cho các gói tin trên đường truyền cũng là một yếu tố quan trọng. Để giải quyết được vấn đề này, chúng tôi đã sử dụng lượng ngẫu nhiên kết hợp với kĩ thuật bắt tay ba chiều cho cả hai phía tham gia. Với phương pháp này, cả người dùng và máy chủ đều có quyền bình đẳng trong việc chứng minh định danh của mình với đối phương.

Bên cạnh đó, dùng lượng ngẫu nhiên kết hợp thêm với thông tin bí mật chia sẻ trước đó cho phép bảo vệ được tính toàn vẹn của gói tin, đảm bảo phát hiện được các gói tin đã bị sửa đổi. Việc vận dụng kĩ thuật này giúp quy trình chứng thực có thể hạn chế các hình thức tấn công lặp lại, tấn công phản xạ và tấn công tạo phiên song song vì chỉ có người dùng và nhà cung cấp mới có khả năng tính toán ra được các đại lượng ngẫu nhiên này.

Trong thiết kế của quy trình chứng thực, không nên có thông tin chung được chia sẻ cho tất cả người dùng trong cùng một dịch vụ. Điều này sẽ dẫn tới việc quy trình chứng thực dễ bị tổn thương đối với một số hình thức tấn công từ bên trong do các thông tin chung sẽ bị kẻ tấn công nội bộ lợi dụng để tính toán ra các dữ liệu nhạy cảm khác của người dùng như khóa bí mật, định danh, mật khẩu. Để giải quyết vấn đề này, chúng tôi sử dụng phương pháp kết hợp khóa chủ và lượng ngẫu nhiên đặc trưng cho từng người dùng. Bằng cách này, mỗi người dùng chỉ thực sự sở hữu một khóa riêng biệt tại từng thời điểm khác nhau; do đó, độ an toàn thực sự được nâng cao. Áp dụng được kĩ thuật này giúp quy trình chứng thực phòng ngừa được các hình thức tấn công mạo danh từ phía máy chủ và người dùng vì lúc này mỗi người dùng đã có một đại lượng khóa riêng và kẻ tấn công không dễ dàng mạo danh để truy cập dịch vụ.

Việc thiết kế tuân thủ các lưu ý cũng như các giải pháp đã nêu có thể hạn chế một số hình thức tấn công phổ biến, ngoài ra giúp quy trình chứng thực có chi phí hợp lí tránh việc lưu trữ và truyền đi các thông tin thừa không tham gia trực tiếp vào quá trình chứng thực gây ra các nguy cơ tiềm ẩn. Từ đó đảm bảo được thiết kế thỏa mãn ngưỡng giữa độ an toàn và hiệu quả về thời gian.

Chúng tôi đã phân tích quy trình chứng thực hai chiều từ xa trên thiết bị di động dựa trên sinh trắc học do nhóm của Khan đề xuất. Mặt dù nhóm của Khan đề xuất nhiều ý tưởng mới, như sử dụng phép NOR để chống tấn công đoán mật khẩu của người dùng, sử dụng hai khóa bí mật để chống tấn công đoán khóa bí mật của máy chủ, quan tâm đến việc bảo vệ tính nặc danh mạnh mẽ của người dùng. Tuy nhiên, chúng tôi đã chứng minh thiết kế quy trình chứng thực của Khan vẫn chưa chặt chẽ và không thể chống được tấn công mạo danh người dùng và máy chủ, tấn công từ chối dịch vụ, tấn công dựa trên ba nhân tố chính. Hơn nữa, quy trình chứng thực do nhóm của Khan đề xuất không đảm bảo được tính nặc danh mạnh mẽ như họ trình bày. Vì vậy, chúng tôi đề xuất quy trình chứng thực mới để loại bỏ những vấn đề còn gặp phải.

So sánh với quy trình chứng thực của Khan, quy trình chứng thực do chúng tôi đề xuất có những điểm mạnh sau. (1) Quy trình chứng thực đề xuất bảo vệ được tính nặc danh của người dùng. (2) Quy trình chứng thực đề xuất được thiết kế chặt chẽ hơn, loại bỏ những điểm yếu trong thiết kế của Khan. Vì vậy, quy trình chứng thực do chúng tôi đề xuất an toàn hơn quy trình chứng thực Khan. Ngoài ra, quy trình chứng thực do chúng tôi đề xuất vẫn đảm bảo được tính hiệu quả về mặt chi phí khi so sánh với quy trình chứng thực của Khan.

## Đề xuất quy trình chứng thực cho hệ thống tương tác thông minh

Trong phần này, chúng tôi đề xuất quy trình chứng thực để phát triển một hệ thống tương tác thông minh đóng vai trò như hệ thống quản lý định danh và có khả năng tự động đăng nhập tất cả các dịch vụ đã đăng ký trước, sau khi chứng thực người dùng thành công. Định danh của người dùng cho các dịch vụ khác nhau được hệ thống xác định một cách tự động và trong suốt với người dùng. Để tăng tính bảo mật, chúng tôi đề xuất một quy trình chứng thực mới phù hợp với hệ thống tương tác thông minh, dựa trên đặc trưng dấu vân tay. Quy trình chứng thực đề xuất có thể chống lại nhiều kiểu tấn công, bao gồm cả tấn công dựa trên ba nhân tố chính.

Trong phần trước, chúng tôi đã nghiên cứu và phân tích tính an toàn của quy trình chứng thực dựa trên sinh trắc học do Khan đề xuất và chỉ ra rằng quy trình chứng thực này vẫn không thể chống được tấn công dựa trên ba nhân tố chính. Chính vì vậy, Chúng tôi đề xuất một quy trình chứng thực mới để loại bỏ điểm yếu này và áp dụng vào hệ thống tương tác thông minh. Theo đó, chúng tôi nhấn mạnh tính chất quan trọng của nhân tố sinh trắc học bởi vì nhân tố này vẫn chưa được quan tâm một cách thỏa đáng trong các quy trình chứng thực.

### Đề xuất quy trình chứng thực

Quy trình chứng thực của chúng tôi bao gồm bốn pha: pha đăng ký, pha đăng nhập, pha chứng thực hai phía và thống nhất khóa phiên, và pha thay đổi mật khẩu. Mỗi máy chủ () đóng vai trò một máy chủ quản lý định danh để kích để kích hoạt tất cả các dịch vụ khác một cách tự động. Các pha được mô tả chi tiết ngay tiếp theo đây.

**Pha đăng ký:** Khi người dùng muốn đăng kí với , chọn định danh, , lượng ngẫu nhiên và nhập vào dữ liệu sinh trắc học . Sau đó, gửi cho thông qua kênh truyền an toàn.

* Bước 1: Khi nhận được thông điệp đăng ký từ , tạo ra giá trị ngẫu nhiên để sinh ra những khóa bí mật khác nhau cho từng người dùng ở những lần đăng ký khác nhau.
* Bước 2: tính các giá trị sau:

Sau đó, R gửi cho thông qua kênh truyền an toàn.

* Bước 3: Thiết bị của người dùng tính:

,

Người dùng giấu định danh và mật khẩu của mình bằng cách tính: , .

Cuối cùng người dùng lưu vào thiết bị của mình.

**Pha đăng nhập:** Để thực hiện pha đăng nhập, thiết bị của người dùng tính lại của và tiến hành các bước sau:

* Bước 1: Tính lại và bằng cách tính: , , , và
* Bước 2: Thiết bị của người dùng tính và , và kiểm tra nếu hay không. Nếu thông tin này trùng khớp, Người dùng vượt qua được bước kiểm tra sinh trắc hoc; ngược lại thiết bị kết thúc phiên làm việc.
* Bước 3: Thiết bị của người dùng tạo lượng ngẫu nhiên và tính các giá trị sau: ,,,.
* Bước 4: Thiết bị của người dùng gửi gói tin đăng nhập cho .

**Pha chứng thực và thống nhất khóa phiên:** Khi nhận được thông điệp yêu cầu đăng nhập, máy chủ  và thiết bị di động của người dùng thực hiện các bước sau để chứng thực hai phía:

* Bươc 1: tính các giá trị sau:

, , và .

* Bước 2: kiểm tra định dạng của . Nếu hợp lệ, tính , sau đó kiểm tra nếu . Nếu hai giá trị bằng nhau, tạo lượng ngẫu nhiên và tính: ,. Sau đó, gửi thông điệp trả lời để chứng minh tính hợp lệ của bản thân máy chủ cũng như thử thách lại phía người dùng.
* Bước 3: Khi nhận được từ, thiết bị của người dùng tính . Sau đó, thiết bị di động kiểm tra nếu hay không. Nếu hai giá trị trùng khớp, thiết bị tính . Sau đó, thiết bị di động gửi thông điệp trả lời để chứng thực chính mình cho .
* Bước 4: Khi nhận được , máy chủ kiểm tra nếu hay không. Nếu hai giá trị bằng nhau, chấp nhận yêu cầu đăng nhập của .
* Bước 5: và tính giá trị của khóa phiên để mã hóa thông tin trao đổi sau khi chứng thực hai phía. tính khóa phiên , còn Tính khóa phiên .

**Pha đổi mật khẩu:** Khi người dùng muốn đổi mật khẩu của mình, người dùng và thiết bị của họ thực hiện các bước sau:

* Bước 1: Thiết bị của người dùng tính lại của sau đó khôi phục và bằng cách tính: , , và . Sau đó, thiết bị của người dùng tính ,, và so sánh nếu . Nếu hai giá trị này trùng khớp, Người dùng vượt qua được bước kiểm tra sinh trắc học; Ngược lại thiết bị chấm dứt phiên làm việc.
* Bước 2: Người dùng nhập mật khẩu mới .
* Bước 3: Thiết bị của người dùng cập nhật lại các giá trị sau:

.

### Phân tích độ an toàn

Trong phần này, chúng tôi chứng minh rằng quy trình chứng thực đề xuất an toàn hơn quy trình chứng thực của Khan do khai thác được sức mạnh của nhân tố sinh trắc học và có thể chống lại được nhiều kiểu tấn công khác nhau.

**Tấn công giả mạo người dùng:** Nếu muốn giả mạo người dừng hợp lệ để đăng nhập vào hệ thống, kẻ tấn công phải giả mạo thành công các giá trị . Tuy nhiên, kẻ tấn công không thể giả mạo được toàn bộ các giá trị này ngay cả khi có thể lấy được toàn bộ thông tin lưu trên thiết bị người dùng. Thậm chí từ những thông tin trên thiết bị, kẻ tấn công cũng không thể trích được và , bởi vì những giá trị này chỉ có thể khôi phục nếu sử dụng nhân tố sinh trắc học , giá trị này rất khó để sao chép và hầu như không thể giả mạo. Vì vậy quy trình chứng thực do chúng tôi đề xuất có thể chống lại tấn công giả mạo người dùng.

**Tấn công giả mạo máy chủ:** Nếu muốn giả mạo một máy chủ hợp lệ , kẻ tấn công phải giả mạo được các thông điệp . Tuy nhiên, do kẻ tấn công không thể có được hai khóa bí mật của máy chủ là và nên không thể tính được các giá trị , . Vì vậy, kẻ tấn công cũng không thể tính được các giá trị và . Từ những phấn tích này, chúng ta có thể thấy rằng kẻ tấn công không thể thực hiện tấn công giả mạo mấy chủ để đánh lừa người dùng.

**Tấn công đoán mật khẩu:** Giả sử rằng kẻ tấn công có thể đánh cắp được các giá trị bí mật lưu trên thiết bị người dùng là và cố gắng trích mật khẩu của người dùng từ những giá trị này dựa trên đặc tả của quy trình chứng thực. Trong quy trình chứng thực đề xuất, chúng tôi ẩn mật khẩu của người dùng bằng nhân tố sinh trắc học . Vì vậy, kẻ tấn công không thể lấy được nếu không có nhân tố sinh trắc học của người dùng. Hơn nữa, quy trình chứng thực do chúng tôi đề xuất không gửi bất kỳ thông tin nào chứa mật khẩu của người dùng qua đường truyền. Vì vậy, kẻ tấn công không thể suy diễn hay đoán được mật khẩu của người dùng.

**Tấn công lặp lại:**Trong kiểu tấn công này, kẻ tấn công đầu tiên sẽ thu thập các gói tin trao đổi giữa người dùng và máy chủ , sau đó cố gắng giả mạo người dùng để đăng nhập với máy chủ bằng cách gửi lại các gói tin đã thu thập. Quy trình chứng thực của chúng tôi sử dụng lượng ngẫu nhiên ở cả hai phía người dùng và máy chủ để thay đổi các giá trị một cách ngẫu nhiên ở mỗi phiên làm việc và để thử thách lẫn nhau. Vì vậy, thông điệp gửi lại có thể dễ dàng bị phát hiện và hủy bởi hay . Chính vì vậy, quy trình chứng thực đề xuất có khả năng phát hiện và chống được kiểu tấn công lặp lại.

**Tấn công do lộ thông tin cho máy chủ:** Trong pha đăng ký của quy trình chứng thực đề xuất, người dùng gửi thay vì gửi các giá trị và một cách riêng lẻ tới trung tâm đăng ký . Cho dù máy chủ có biết được giá trị lưu trên thiết bị của người dùng thì cũng không thể tính lại và . Lưu ý rằng người dùng có xu hướng dùng lại và cho nhiều ứng dụng khác nên việc bảo vệ bí mật thông tin này là cần thiết. Từ những phân tích trên, quy trình chứng thực đề xuất an toàn với kiểu tấn công này.

**Tấn công do đánh cắp thông tin chia sẻ bí mật**: Nếu kẻ tấn công có được các giá trị chia sẻ giữa người dùng và máy chủ, kẻ tấn công có thể muốn sử dụng thông tin này để đăng nhập với máy chủ. Nhưng để thực hiện được quá trình đăng nhập, kẻ tấn công buộc phải nhập thông tin sinh trắc học , giá trị này rất khó để sao chép và hầu như không thể giả mạo. Vì vậy kẻ tấn công không thể chứng thực thành công với máy chủ.

**Tấn công dựa trên ba nhân tố chính**: Trong kiểu tấn công này, chúng tôi giả sử kẻ tấn cong có được thông tin và mật khẩu cũng như định danh của người dùng . Bây giờ kẻ tấn công phải lấy được các giá trị , và sinh trắc học cùng một lúc. Điều này không thể thực hiện trong thời gian tuyến tính. Vì vậy, quy trình chứng thực của chúng tôi có khả năng chống được kiểu tấn công dựa trên ba nhân tố chính.

**So sánh độ an toàn:** Trong Bảng 8.4. , chúng tôi so sánh độ an toàn của phương pháp mới đề xuất với ba quy trình chứng thực của Khan [147], Sarvabhatla [149] và Wen [150]. Bên cạnh khả năng chông được các kiểu tấn công phổ biến, phương pháp của chúng tôi cũng có khả năng chống được kiểu tấn công dựa trên ba nhân tố chính, điều này chưa được xem xét trong quy trình chứng thực của Sarvabhatla cũng như Wen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Các đặc tính | Quy trình chứng thực của Khan [146] | Quy trình chứng thực của Sarvabhatla [148] | Quy trình chứng thực của Wen [149] | Quy trình chứng thực đề xuất |
| An toàn trước tấn công giả mạo người dùng | Không | Có | Có | Có |
| An toàn trước tấn công giả mạo máy chủ | Không | Có | Có | Có |
| An toàn trước tấn công đoán mật khẩu | Không | Có | Có | Có |
| An toàn trước tấn công do lộ thông tin trên thiết bị | Không | Có | Có | Có |
| Chứng thực hai phía | Không | Có | Có | Có |
| An toàn trước tấn công lặp lại | Có | Có | Có | Có |
| An toàn trước tân công do lộ thông tin người dùng cho máy chủ | Có | Có | Có | Có |
| An toàn trước tấn công dựa trên ba nhân tố chính | Không | Chưa xét | Chưa xét | Có |

Bảng 8.4. So sánh khả năng chống lại nhiều kiểu tấn công khác nhau

## Kết chương

Nội dung của chương này đã trình bày quy trình chứng thực được cải tiến từ hai quy trình chứng thực của Khan [146] [147]. Đặc điểm của quy trình chứng thực là sử dụng các phép tính toán đơn giản như hàm băm mật mã, lượng ngẫu nhiên, phép toán XOR trên bit.

Trong quy trình này, chúng tôi đã đề xuất tích hợp sử dụng chứng thực bằng đặc trưng dáng đi. Dựa trên quy trình này, chúng tôi đã đề xuất một ứng dụng minh họa là hệ thống cung cấp thông tin và dịch vụ trực tuyến dựa trên chứng thực với đặc trưng sinh trắc.

Một phần kết quả của chương này được công bố trong công trình [CT2]. Đây là kết quả bước đầu chúng tôi xây dựng. Các đề xuất, cải tiến trong quy trình chứng thực này có khả năng được mở rộng để xây dựng những quy trình chứng thực tốt hơn, ví dụ như tích hợp hướng tiếp cận mới trong xây dựng quy trình chứng thực an toàn với đa thức Chebysev (được trình bày trong Chương 9 và được chúng tôi công bố trong [CT1]).

# Quy trình chứng thực an toàn sử dụng đa thức Chebysev

**Tóm tắt chương:**

*✍ Tính chất an toàn tiến được xem là một chuẩn quan trọng để đánh giá một qui trình chứng thực mạnh. Đã có rất nhiều kết quả được nghiên cứu nhằm đạt được tính chất này mà không cần sử dụng các bài toán khó. Gần đây, công trình của Chang và các cộng sự đã đạt được một số bước tiến nhất định, như tính chính xác của cơ chế chứng thực được minh họa bằng mô hình BAN-logic và chi phí cài đặt được giảm bớt. Tuy nhiên, trong đề tài này, chúng tôi chứng minh rằng cơ chế của họ dễ bị tổn thương với hình thức tấn công mạo danh cũng như dễ bị rò rỉ khóa phiên. Để vượt qua các hạn chế này cũng như có được một kết quả thực tế hơn, chúng tôi sử dụng ý tưởng khác nhằm thực nghiệm và đề xuất ra một qui trình cải tiến hiệu quả về mặt thời gian.*

## Giới thiệu

Ngày nay, việc giao tiếp không dây là một nền tảng cần thiết cộng với sự phát triển không ngừng của các thiết bị cầm tay và thiết bị đeo, đã có nhiều các dịch vụ trực tuyến được triển khai trên internet. Khách hàng đòi hỏi một sự hồi đáp tức thời, tính riêng tư và bảo mật trong các giao dịch với nhà cung cấp dịch vụ. Bởi thế, việc tích hợp các kết quả toán học vào trong các thao tác chứng thực là một khuynh hướng tất yếu.

Chứng thực người dùng là nhiệm vụ đầu tiên mà bất kỳ dịch vụ trực tuyến nào cũng cần thực hiện. Có thể nói rằng hai chuẩn cơ bản một qui trình nên đạt được đó là độ an toàn và tính hiệu quả về thời gian. Tuy nhiên, đồng thời đạt được các mục tiêu này là một nhiệm vụ khó khăn. Về phần an toàn, có nhiều tiêu chuẩn và một trong số chúng là định danh người dùng một cách chính xác. Phương pháp cơ bản [126] là lưu trữ một bảng kiểm tra bao gồm các dòng có dạng “định danh / mật khẩu” trên máy chủ. Khi người dùng đăng nhập, thì máy chủ sẽ kiểm tra sự tồn tại bằng cách tra cứu trong bảng đã lưu. Tuy đơn giản, nhưng phương pháp này có nguy cơ bị đánh cắp bảng mật khẩu. Ngoài ra, việc cung cấp định danh tĩnh qua kênh truyền công khai hoàn toàn không phù hợp với một vài ứng dụng, ví dụ như truyền hình trả tiền [127] hoặc bầu trực tuyến. Để khắc phục các nhược điểm này, một vài tác giả đã đề xuất ý tưởng định danh động [128][129][141], nhưng các kết quả này vẫn có một số bất lợi như thông điệp đối xứng dễ bị tấn công lặp lại hoặc thiết kế kém dẫn tới bị tấn công chèn thông tin. Nhìn chung, phần lớn các qui trình sử dụng hàm băm mật mã cái không thể cho ra được một qui trình chứng thực với các thuộc tính mạnh mẽ. Để nâng cao độ an toàn, phương pháp sử dụng các bài toán khó ngày càng nhận được nhiều sự quan tâm. Tiêu biểu, RSA[142] là một trong những phương pháp phổ biến được tích hợp vào các qui trình chứng thực người dùng, nhưng phương pháp này thường đính kèm theo các chứng chỉ dẫn tới việc tăng thêm khối lượng lưu trữ và tính toán. Rõ ràng, điều này không thích hợp với các thiết bị có nguồn tài nguyên hạn chế. Một vài tác giả đã đề xuất kết quả [143][144][145] sử dụng đường cong elliptic làm nền tảng, và có thể nói đây là một hướng tiếp cận hợp lí về mặt chi phí và độ an toàn. Tuy nhiên, các công trình này đều đề cập tới việc sử dụng hàm băm MapToPoint, có chi phí không nhỏ ngoài ra cũng chưa được chuẩn hóa trong thực tế. Bên cạnh đó, đa thức Chebysev cũng nhận được nhiều sự quan tâm [130][131] và thuộc tính nửa nhóm của nó được áp dụng trong qui trình chứng thực cho môi trường mạng di động toàn cầu [132] hoặc làm nền cho các hệ thống dựa trên khóa công [133]. Cũng có một vài thuật toán [134] được dùng trong hệ thống khóa công dựa theo hướng tiếp cận này. Có thể nói chứng thực dựa trên đa thức Chebysev là một phương thức khác tốt hơn để cân bằng được ngưỡng an toàn và hiệu quả một cách hợp lí.

Năm 2013, Chang và các cộng sự đã đề xuất qui trình [135] hiệu quả dựa trên hàm băm mật mã. Bên cạnh đó, tính chính xác của qui trình cũng được chứng minh dùng mô hình BAN-logic [136]. Kết quả của họ thực sự đã có một vài thành công, ví dụ đã cung cấp được tính chứng thực hai chiều, đạt được pha thỏa hiệp khóa phiên sau chứng thực và không sử dụng cơ chế đồng bộ hóa thời gian. Tuy nhiên, hạn chế cơ bản của họ là việc thách thức chỉ xuất phát từ phía máy chủ cũng như việc phân phối thông tin chung cho tất cả các thành viên. Trong bài báo này, chúng tôi chứng minh rằng kết quả của Chang và các cộng sự dễ bị tổn thương với hình thức tấn công mạo danh và không bảo vệ được khóa phiên. Hơn nữa, nó không cung cấp tính nặc danh người dùng. Tiếp theo, chúng tôi sẽ áp dụng tính chất nửa nhóm của đa thức Chevbysev nhằm cân bằng ngưỡng cũng như bảo vệ khóa phiên trong môi trường khách-chủ nơi mà hướng tiếp cận này chưa được nghiên cứu. Ngoài ra, thiết kế của chúng tôi có các thách thức từ các bên tham gia, khách và chủ nhằm tạo nên tính công bằng trong các giao dịch. Chúng tôi cũng sử dụng mô hình BAN-logic nhằm chứng minh tính chính xác của qui trình. Có thể nói rằng kết quả của chúng tôi được nâng cao về độ an toàn cũng như có chi phí hợp lí về mặt thời gian.

Phần còn lại của bài báo này được tổ chức như sau: phần 2 trình bày lại qui trình của Chang và các cộng sự cũng như các thảo luận về những hạn chế. Sau đó, qui trình cải tiến được trình bày trong phần 3, trong khi phần 4 là các phân tích về thời gian và độ an toàn của nó. Cuối cùng, phần 5 là các kết luận luận của chúng tôi.

## Qui trình của Chang và các phân tích đánh giá

Trong phần này chúng tôi sẽ xem xét lại qui trình của Chang và các cộng sự [135] và cho thấy rằng kết quả của họ dễ bị tổn thương với hình thức tấn công mạo danh. Ngoài ra, nó không cung cấp tính nặc danh người dùng.

### Qui trình của Chang

Trong phần này, chúng tôi sẽ trình bày lại qui trình của Chang và các cộng sự. Qui trình của họ bao gồm 4 pha: pha đăng kí, pha chứng thực, pha thay đổi mật khẩu, và pha khôi phục thẻ. Bên dưới là một vài kí hiệu quan trọng trong qui trình này

|  |  |
| --- | --- |
| **Kí hiệu** | **Mô tả** |
| *U*i  *id*i  *pw*i  *S*  *id*S  *x*, *y*  *h*(.)  *sn*i  *SK*  *SC*  ⊕  || | Người dùng thứ *i*  Định danh của *U*i  Mật khẩu của *U*i  Máy chủ cung cấp dịch vụ  Định danh của máy chủ  Khóa bí mật của máy chủ  Hàm băm mật mã một chiều  Số thứ tự thẻ  Khóa phiên chung của *U*i và *S*  Thẻ thông minh/thiết bị di động/thiết bị đeo  Thao tác XOR hai chuỗi  Thao tác nối chuỗi |

Bảng 9.1. Các kí hiệu dùng trong qui trình

### Pha đăng kí

*U*i chọn định danh *id*i và *pw*i. Sau đó, *U*i phải đăng ký thông tin này với *S* thông qua kênh truyền an toàn. Khi nhận thông tin từ *U*i, *S* thực hiện các bước sau.

- *S* chọn ngẫu nhiên số nguyên *r*i kích thước 128-bit. Sau đó, *S* tính *R*1 = *h*(*id*i || *x* || *r*i), *R*2 = *g*xy mod *p*, ở đó *p* là số nguyên tố lớn và *g* là phần tử sinh trong Z\*p, và *R*3 = *h*(*id*i || *R*2) ⊕ *h*(*pw*i).

- *S* cấp *SC* với số *sn*i kích thước 32-bit, ở đó *sn*i có một định dạng cụ thể nào đó. Sau đó, *S* kết hợp *sn*i với *id*i của *U*i như sau *SID*i = (*id*i || *sn*i)

- Cuối cùng, *S* lưu *R*1, *R*2, *R*3, *SID*i và *h*(.) vào *SC* và gửi cho *U*i thông qua kênh truyền an toàn

Trong pha đăng kí, chúng ta thấy có một vài vấn đề: Bởi vì *U*i gửi *pw*i dạng thô cho *S*, nên *S* biết mật khẩu thực của *U*i và có thể sẽ cố gắng dùng nó trong các hệ thống khác ở đó *U*i là thành viên. Ngoài ra, sử dụng hai khóa *x* và *y* tuy có độ an toàn cao, tuy nhiên chúng tôi nhận thấy chỉ cần một khóa với độ hỗn loạn cao là đủ an toàn. Bởi thế, chúng tôi sẽ thay đổi những điều này trong phađăng kýcủa chúng tôi.

### Pha chứng thực

Khi *U*i truy cập *S*, *U*i đưa *SC* vào thiết bị trạm và cung cấp *id*i và *pw*i. Sau đó *SC* tính toán các bước sau.

- *SC* tính *C*1 = *R*3 ⊕ *h*(*pw*i) và *V*1 = *R*1 ⊕ *C*1.

- Kế tiếp, *SC* tạo ngẫu nhiên số *n*1 kích thước 160-bit, sau đó tính *DID*i = *h*(*R*2 || *n*1) ⊕ *SID*i

- Cuối cùng, *SC* gửi *m*1 = {*DID*i, *V*1, *n*1} tới *S* thông qua kênh truyền công cộng.

- Khi nhận *m*1 từ *U*i, *S* tính toán lại *SID*i = *DID*i ⊕ *h*((*g*xy mod *p*) || *n*1). Sau đó, *S* khôi phục *id*i và *sn*i và kiểm tra định dạng của chúng. Nếu chúng hợp lệ, *S* tiếp tục tính *R*\* = *V*1 ⊕ *h*(*id*i || (*g*xy mod *p*)) và tạo ngẫu nhiên số nguyên *n*2 kích thước 160-bit.

- Kế tiếp, *S* tính *V*2 = *h*(*R*\*1 || *id*S || *n*1), *V*3 = *h*(*h*(*id*i || (*g*xy mod *p*)) || *n*1) ⊕ *n*2 và gửi *m*2 = {*id*S, *V*2, *V*3} tới *U*i thông qua kênh truyền công cộng.

- Khi nhận được *m*2 từ *S*, *SC* tính *V*\*2 = *h*(*R*1 || *id*S || *n*1) và kiểm tra *V*\*2 ?= *V*2. Nếu điều này thỏa, *S* được chứng thực thành công; ngược lại kết nối sẽ bị ngắt.

- *SC* thu giá trị ngẫu nhiên *n*2 = *V*3 ⊕ *h*(*C*1 || *n*1) và tạo *SK* = *h*(*n*1 || *SID*i || *R*2 || *n*2).

- Cuối cùng, *SC* tính *V*4 = *h*(*SK* || (*n*2 + 1)) và gửi *m*4 = {*V*4} tới *S* thông qua kênh truyền công cộng.

- Sau khi nhận được *m*4 từ *U*i, *S* tính *SK* = *h*(*n*1 || *SID*i || (*g*xy mod *p*) || *n*2) và *V*\*4 = *h*(*SK* || (*n*2 + 1)). Kế tiếp, *S* kiểm tra *V*\*4 ?= *V*4. Nếu điều này thỏa, *U*i được chứng thực thành công. Ngược lại, kết nối sẽ bị ngắt.

Trong pha chứng thực của họ, chúng ta thấy rằng chỉ *S* khởi tạo giá trị ngẫu nhiên *n*2 để thách thức *U*i, trong khi giá trị *n*1 của *U*i là công khai trong kênh truyền công cộng. Thiết kế này sẽ hạn chế sức mạnh của các giá trị ngẫu nhiên trong qui trình. Ngoài ra, định danh của người dùng có thể bị rò rỉ bởi vì qui trình của họ phân phối *g*xy mod *p* tới tất cả các thành viên. Chúng tôi sẽ phân tích rõ hơn trong phần kế tiếp.

### Pha thay đổi mật khẩu

Khi *U*i muốn thay đổi *pw*i, *U*i có thể thực hiện các bước sau.

- *U*i đưa *SC* vào một trạm thiết bị nào đó và nhập *id*i, *pw*i.

- *SC* tính *Q*1 = *h*(*id*i || *R*2) và *Q*\*1 = *R*3 ⊕ *h*(*pw*i) và so sánh với nhau. Nếu *Q*1 = *Q*\*1, *SC* tiếp tục các bước kế; ngược lại, thủ tục sẽ bị ngắt.

- *SC* tính *R*’3 = *h*(*id*i || *R*2) ⊕ *h*(*pw*i) ⊕ *h*(*pw*’i) và thay *R*3 bằng *R*’3.

Trong pha thay đổi mật khẩu, chúng ta thấy rằng việc cập nhật mật khẩu được thực hiện mà không cần tương tác với *S*. Qui trình cùa chúng tôi sẽ kế thừa ý tưởng này từ [135].

### Pha khôi phục thẻ

Khi *U*i phát hiện ra thông tin trong *SC* bị rò rỉ, *U*i có thể yêu cầu *S* cấp lại *SC* thông qua kênh truyền an toàn. Khi nhận được yêu cầu khôi phục, *S* kiểm tra *U*i bằng các thông tin cá nhân. Sau khi kiểm tra thành công, *S* lưu *sn*i của *SC* cũ trong cơ sở dữ liệu và cấp *SC* mới với *sn*’i mới cho *U*i. Cuối cùng, *U*i chọn một *pw*i mới tương tự như các bước trong pha đăng kí.

## Phân tích đánh giá qui trình Chang và các cộng sự

Trong phần này, chúng tôi trình bày các kết quả phân tích trên qui trình của Chang. Chúng tôi chứng minh rằng qui trình dễ bị tổn thương với hình thức tấn công mạo danh và đánh cắp khóa phiên. Ngoài ra, nó cũng không cung cấp tính nặc danh người dùng.

### Không cung cấp tính nặc danh người dùng

Trong qui trình của Chang, chúng ta thấy một người dùng nào đó gửi *m*1 = {*DID*i, *V*1, *n*1}. Tuy nhiên, thông tin quan trọng (*g*xy mod *p*) được phân phối tới tất cả các thành viên khác. Do đó, bất kỳ ai là người dùng hợp lệ có thể đánh cắp định danh của người dùng khác bằng các bước sau:

- Kẻ tấn công bắt gói tin *m*1 = {*DID*i, *V*1, *n*1}

- Kế tiếp, kẻ tấn công thu *SID*i = *DID*i ⊕ *h*((*g*xy mod *p*) || *n*1).

- Cuối cùng, kẻ tấn công trích *id*i và *sn*i từ *SID*i và biết ai đang chứng thực với *S.*

Rõ ràng, qui trình của Chang không bảo vệ được định danh cho người dùng chống lại kẻ tấn công.

### Tấn công mạo danh

Bởi vì thiết kế không hợp lí, qui trình của Chang dễ bị tổn thương với hình thức tấn công mạo danh từ cả hai phía, người dùng và máy chủ. Trước tiên, chúng tôi sẽ trình bày các bước mà một kẻ tấn công thực hiện để mạo danh máy chủ:

- Tương tự như các bước trong việc đánh cắp định danh, kẻ tấn công thu *id*i và *sn*i của một người dùng nào đó.

- Với *id*i, kẻ tấn công tính *R*\*1 = *V*1 ⊕ (*id*i || (*g*xy mod *p*)) and *V*\*2 = *h*(*R*\*1 || *id*S || *n*1), trong đó *V*1 và *n*1 thuộc về *m*1 = {*DID*i, *V*1, *n*1}.

- Kế tiếp, kẻ tấn công tạo một giá trị ngẫu nhiên *n*\*2 và tính *V*\*3 = *h*(*h*(*id*i || (*g*xy mod *p*)) || *n*1) ⊕ *n*\*2.

- Cuối cùng, kẻ tấn công gửi *m*\*2 = {*id*S, *V*\*2, *V*\*3} cho *U*i.

Khi nhận *m*\*2, *U*i tính toán lại *V*2 = *h*(*R*1 || *id*S || *n*1) và so sánh nó với *V*\*2. Rõ ràng, chúng hoàn toàn khớp nhau và kẻ tấn công đã mạo danh thành công *S*. Ngoài ra, kẻ tấn công có thể mạo danh *U*i nào đó đang chứng thực với *S*. Sau đây là một vài bước mạo danh người dùng.

- Kẻ tấn công bắt gói tin *m*1 = {*DID*i, *V*1, *n*1}, sau đó trích *SID*i bằng cách *SID*i = *DID*i ⊕ *h*(*R*2 || *n*1), ở đó *R*2 là thông tin của *SC* trong thẻ/thiết bị của kẻ tấn công.

- Sau đó, kẻ tấn công tạo một giá trị ngẫu nhiên *n*\*1 và tính toán *DID*\*i = *h*(*R*2 || *n*\*1) ⊕ *SID*i.

- Kế tiếp, kẻ tấn công gửi *m*\*1 = {*DID*\*i, *V*1, *n*1} cho *S*.

- Sau khi nhận *m*\*1, *S* tính và gửi lại *m*2 = {*id*S, *V*2, *V*3} cho kẻ tấn công. Trong lúc này, kẻ tấn công tính *n*2 = *V*3 ⊕ *h*(*h*(*id*i || *R*2) || *n*\*1), trong đó *id*i đã được kẻ tấn công tính ra.

- Với *n*2, kẻ tấn công tính *SK*\* = *h*(*n*\*1 || *SID*i || *R*2 || *n*2) và *V*\*4 = *h*(*SK*\* || (*n*2 + 1)).

- Cuối cùng kẻ tấn công gửi *m*\*3 = {*V*\*4} cho *S*.

Sau khi nhận *m*\*3, *S* tính *V*4 và so sánh nó với *V*\*4. Rõ ràng, chúng hoàn toàn khớp nhau và kẻ tấn công đã mạo danh người dùng thành công.

### Tấn công khóa phiên

Một người dùng hợp lệ nào đó có thể quan sát và tính toán *SK* bằng cách thưc hiện một số bước sau:

- Trước tiên, kẻ tấn công bắt 3 gói tin *m*1, *m*2 và *m*3 trên kênh truyền công cộng.

- Kế tiếp, kẻ tấn công tính *SID*i = *DID*i ⊕ *h*((*g*xy mod *p*) || *n*1) và trích ra *id*i.

- Sau đó, kẻ tấn công có được *n*2 bằng cách *n*2 = *V*3 ⊕ *h*((*id*i || *R*2) || *n*1).

- Cuối cùng, kẻ tấn công tính *SK* = *h*(*n*1 || *SID*i|| *R*2 || *n*2).

Rõ ràng, tất cả dữ liệu được mã hóa với *SK* này sẽ bị lộ hoàn toàn.

## Qui trình đề xuất

Trước tiên, chúng tôi mô tả đa thức Chebysev [131][137][138] mà chúng tôi dùng làm nền tảng an toàn trong qui trình. Đa thức Chebysev *T*n(*x*): (-∞, ∞) → [-1, 1] có dạng:

*T*n(*x*) = (2 \* *x* \* *T*n-1(*x*) – *T*n-2(*x*)) mod *p*

Trong đó *n* ≥ 2 là một bậc số nguyên, *x* ∈ (-∞, ∞) và *p* là số nguyên tố lớn. Ngoài ra, qui trình đề xuất tận dụng thuộc tính nửa nhóm của đa thức

*T*q(*T*w(*x*)) = *T*w(*T*q(*x*)), ∀*q*,*w* ∈ N và *x* ∈ (-∞, ∞).

Tiếp theo chúng tôi đề xuất qui trình cải tiến nhằm loại bỏ các vấn đề an toàn đã đề cập. Trước khi trình bày mỗi pha, chúng tôi mô tả các ý tưởng tổng quan trong qui trình. Trong pha đăng kí, mục tiêu chính bao gồm cung cấp khóa chứng thực *h*(*X*S || *e*) và lưu *h*(*id*i) ⊕ *X*S ở cơ sở dữ liệu phía máy chủ để kiểm tra tính hợp lệ định danh. Đặc biệt, giá trị ngẫu nhiên *e* giúp tạo các khóa khác nhau ở những thời điểm khác nhau. Trong pha đăng nhập và chứng thực, chúng tôi dùng hai giá trị ngẫu nhiên *R*U và *R*S kết hợp với đa thức Chebysev hỗ trợ việc thách thức. Ngoài ra, chúng tôi áp dụng kỹ thuật bắt tay hồi đáp thách thức ba chiều để chống lại hình thức tấn công lặp lại và mạo danh tốt hơn [145]. Cuối cùng, cần phải đạt được *SK* nhằm mã hóa dữ liệu giữa người dùng và máy chủ sau pha chứng thực thành công. Qui trình của chúng tôi được chia thành năm pha, gồm pha đăng kí, pha đăng nhập, pha chứng thực, pha cập nhật mật khẩu và pha khôi phục thẻ.

### Pha đăng kí

Trước khi trình bày chi tiết, chúng tôi đề nghị ba điều kiện mà một phađăng kýnên thỏa mãn: thứ nhất, mật khẩu của người dùng không nên lộ ra cho máy chủ. Trong qui trình đề xuất, mặt dù máy chủ khởi tạo mật khẩu cho người dùng, tuy nhiên người dùng sẽ phải thay đổi mật khẩu sau khi nhận nó từ phía máy chủ. Thứ hai, máy chủ phải cung cấp khóa chứng thực khác nhau ở từng thời điểm khác nhau. Thứ ba, máy chủ nên lưu định danh người dùng theo cách an toàn nhằm phục vụ cho việc kiểm tra tính hợp lệ trong các pha sau. Qui trình đề xuất được thiết kế để đạt được các điều cơ bản nêu trên.

Khi *U*iđăng kývới *S*, *U*i phải đưa *id*i tới cho *S* thông qua kênh truyền an toàn. *S* sẽ thực hiện các bước sau:

1. *S* tạo *pw*i và giá trị ngẫu nhiên *e*.

2. Kế tiếp, *S* tính khóa chứng thực *K* = *h*(*X*S || *e*), khóa phụ *M* = *K* ⊕ *h*(*id*i || *pw*i) và thông tin xác nhận *L* = *h*(*K* || *id*i || *pw*i), trong đó *X*S là khóa chủ của *S*.

3. Sau đó, *S* lưu *h*(*id*i) ⊕ *X*S trong cơ sở dữ liệu của *S*.

4. Cuối cùng, *S* gửi {*pw*i, *SC*(*M*, *L*, *e*, *h*(.), *T*S(*x*))} thông qua kênh truyền an toàn, trong đó {*x*, *T*S(*x*)} là thông tin công khai của *S*.

Sau khi nhận *SC* và *pw*i, *U*i cập nhật *pw*i thông qua pha cập nhật mật khẩu.

### Pha đăng nhập

Trong pha đăng nhập, việc kiểm tra định danh và mật khẩu người dùng phải được thực hiện ở phía người dùng nhằm ngăn ngừa những trường hợp máy chủ phải xử lí những trường hợp vô tình cung cấp những thông tin sai lệch từ phía người dùng. Ngoài ra, thông điệp đăng nhập nên thay đổi ở từng thời điểm khác nhau nhằm bảo vệ thông tin người dùng đặc biệt là định danh. Pha đăng nhập trong qui trình đề xuất cũng được thiết kế để thỏa mãn ba yêu cầu này.

Khi *U*i nhập thông tin *id*i và *pw*i để đăng nhập *S*, *SC* thực hiện:

1. *SC* tính *K* = *M* ⊕ *h*(*id*i || *pw*i) và *L*\* = *h*(*K* || *id*i || *pw*i).

2. Kế tiếp, nó so sánh *L*\* với *L*. Nếu chúng bằng nhau, thì *id*i và *pw*i là chính xác và *SC* tiếp tục các bước kế; ngược lại nó sẽ ngắt phiên làm việc.

3. Sau đó, *SC* tạo một giá trị nguyên lớn *r*U, tính *R*U = *T*rU(*x*), *DID*i = *id*i ⊕ *h*(*R*U || *K*) và *R*2 = *h*(*K* || *id*i || *R*U).

4. Cuối cùng, nó gửi {*e*, *R*U, *R*2, *DID*i} tới *S* thông qua kênh truyền công cộng.

### Pha chứng thực và thỏa hiệp khóa

Trong pha chứng thực, cả người dùng và máy chủ phải thách thức lẫn nhau để chứng minh tính hợp lệ của mình. Ngoài ra, cả hai bên nên thống nhất một khóa phiên chung sau khi chứng thực thành công. Pha chứng thực của qui trình đề xuất đạt được hai tiêu chí này. Trong phần này, sau khi nhận {*e*, *R*U, *R*2, *DID*i} từ *U*i trong pha đăng nhập, *S* thực hiện các bước sau để chứng thực *U*i.

1. *S* tính *h*(*X*S || *e*) và trích *id*i = *DID*i ⊕ *h*(*R*U || *h*(*X*S || *e*)).

2. Kế tiếp, *S* kiểm tra *id*i bằng cách thực hiện *h*(*id*i) ⊕ *X*S, và tìm kiếm sự tồn tại của nó trong cơ sở dữ liệu. Nếu tìm thấy, *id*i là hợp lệ; ngược lại, *S* ngắt phiên làm việc.

3. Sau đó, *S* tính *R*\*2 = *h*(*h*(*X*S || *e*) || *id*i || *R*U) và so sánh *R*\*2 với *R*2. Nếu chúng bằng nhau, *S* tiếp tục các bước kế tiếp; ngược lại, *S* ngắt phiên làm việc.

4. *S* tạo *r*S, tính *R*S = *T*rS(*x*), *SK* = *h*(*T*rS(*R*U) || *h*(*X*S || *e*) || *id*i) và *R*4 = *h*(*h*(*X*S || *e*) || *id*i || *SK*).

5. Cuối cùng, *S* gửi {*R*S, *R*4} tới *U*i thông qua kênh truyền công cộng.

6. Sau khi nhận {*R*S, *R*4} từ *S*, *U*i tính toán lại *SK* = *h*(*T*rU(*R*S) || *K* || *id*i), *R*\*4 = *h*(*K* || *id*i || *SK*) và so sánh *R*\*4 với *R*4. Nếu chúng bằng nhau, *U*i chứng thực thành công với *S*.

7. *U*i tính *R*5 = *h*(*SK*) và gửi tới *S* thông qua kênh truyền công cộng.

8. Sau khi nhận {*R*5} của *U*i, *S* tính lại *R*\*5 = *h*(*SK*) và so sánh nó với *R*5. Nếu chúng bằng nhau, *S* chứng thực thành công *U*i.

### Pha cập nhật mật khẩu

Khi *U*i muốn thay đổi *pw*i, *U*i thực hiện:

1. *U*i đưa *SC* vào trạm thiết bị và nhập *id*i, *pw*i.

2. Kế tiếp, *SC* tính *K* = *M* ⊕ *h*(*id*i || *pw*i) và *L*\* = *h*(*K* || *id*i || *pw*i).

3. Sau đó, *SC* so sánh *L*\* với *L* lưu bên trong. Nếu chúng bằng nhau, *SC* chấp nhận yêu cầu của người dùng; ngược lại, nó ngắt phiên làm việc.

4. *U*i nhập mật khẩu mới *pw*inew. Sau đó, *SC* tính *M*new = *K* ⊕ *h*(*id*i || *pw*inew) và *L*new = *h*(*K* || *id*i || *pw*inew).

5. Cuối cùng, *SC* thay *L*, *M* bằng *L*new và *M*new.

### Pha khôi phục thẻ

Nếu *U*i mất *SC*, *U*i phải thông báo cho *S*. Sau đó, *S* sẽ cấp lại *SC* mới với định danh cũ cho *U*i.

1. *U*i cung cấp lại *id*i và yêu cầu cấp lại thẻ/cài đặt trên thiết bị di động/thiết bị đeo tới *S* thông qua kênh truyền an toàn.

2. Sau khi nhận yêu cầu từ *U*i, *S* tính *h*(*id*i) ⊕ *X*S và tìm sự tồn tại của nó trong cơ sở dữ liệu. Nếu tồn tại, *S* chấp nhận yêu cầu của *U*i; ngược lại *S* ngắt phiên làm việc.

3. Kế tiếp *S* tạo một giá trị ngẩu nhiên mới *e*new và thực hiện các bước giống như trong pha đăng kí. Cuối cùng, *S* cấp lại *SC* mới cho *U*i thông qua kênh truyền an toàn.

## Các phân tích độ an toàn và tính hiệu quả

Trong phần này, chúng tôi phân tích qui trình đề xuất trên hai phương diện: độ an toàn và tính hiệu quả. Trước khi đi sâu vào quá trình đánh giá, chúng tôi giới thiệu ba giả thiết cơ bản mà qui trình sử dụng, đó là giả thiết một chiều hàm băm mật mã [135] và hai bài toán logarit rời rạc và Diffie-Hellman trên đa thức Chebysev [131][138].

- Vấn đề logarit rời rạc trên đa thức Chebysev (CDLP): Cho trước *y* và *x* sao cho *y* = *T*u(*x*), rất khó tìm ra được *u* thỏa mãn biểu thức trên, trong đó *u*, *v* ∈ N và *x* ∈ (-∞, ∞).

- Vấn đề Diffie-Hellman (CDHP): Cho trước *x*, *T*u(*x*) và *T*v(*x*), rất khó có thể tính được giá trị *T*u\*v(*x*), trong đó *u*, *v* ∈ N và *x* ∈ (-∞, ∞).

### Chứng minh độ chính xác

Để đánh giá chính xác về qui trình cải tiến, chúng tôi sử dụng BAN-logic [136] do Burrows đề xuất. Chúng tôi giới thiệu một vài kí hiệu cơ bản được dùng trong phương pháp này: kí hiệu *P* và *Q* đại diện cho các bên tham gia, *X* và *Y* là các thông điệp và *K* là khóa bí mật. Sau đây, chúng tôi sẽ dùng BAN-logic để chứng minh qui trình đã đạt được tính chứng thực hai chiều và thỏa hiệp khóa một cách chuẩn xác. Thay vì dùng *P* và *Q*, chúng tôi sẽ thế bằng *U*i và *S* đại diện cho người dùng và máy chủ. Ngoài ra, chúng tôi chuẩn hóa tám mục tiêu được kí hiệu bằng *G*j, ∀*j* ∈ [1, 8]:

|  |  |
| --- | --- |
| *G*1. *U*i |≡ *U*i*S*  *G*2. *U*i |≡ *S* |≡ *U*i*S*  *G*3. *S* |≡ *U*i*S*  *G*4. *S* |≡ *U*i |≡ *U*i*S* | *G*5. *U*i |≡ *U*i*S*  *G*6. *U*i |≡ *S* |≡ *S**U*i  *G*7. *S* |≡ *S**U*i  *G*8. *S* |≡ *U*i |≡ *U*i*S* |

Bảng 2: Các mục tiêu trong mô hình

Sau đó, chúng tôi sẽ chuẩn hóa qui trình đề xuất như sau:

- *DID*i = <*U*i*S*, *T*rU, *U*i*S*>

- *R*2 = <*U*i*S*, *U*i*S*, *T*rU>

- *R*4 = <*U*i*S*, *U*i*S*, *U*i*S*>

- *R*5 = <*T*rS(*R*U), *U*i*S*, *U*i*S*>

Kế tiếp chúng tôi sẽ đưa ra một vài giả thiết (kí hiệu là *A*t, ∀*t* ∈ [1, 8]) về các trạng thái đầu tiên của qui trình:

|  |  |
| --- | --- |
| *A*1. *U*i |≡ *U*i*S*  *A*2. *U*i |≡ *U*i*S*  *A*3. *U*i |≡ *S* ⇒ *U*i*S*  *A*4. *S* |≡ *U*i ⇒ *U*i*S* | *A*5. *S* |≡ *U*i ⇒ *U*i*S*  *A*6. *S* |≡ *S**U*i  *A*7. *U*i |≡ #(*T*rS)  *A*8. *S* |≡ #(*T*rU) |

Bảng 3: Các giả thiết trong mô hình

Cuối cùng với *A*t và các định đề trong mô hình BAN-logic, chúng tôi sẽ chứng minh qui trình đạt được tất cả tám *G*j, ∀*j* ∈ [1, 8].

- *U*iđăng ký*id*i với *S*, vậy chúng ta đạt được *G*1: *U*i |≡ *U*i*S*

- Với *A*6 và *DID*i, áp dụng luật message-meaning ta có

(1)

- Với *A*8 và áp dụng luật freshness ta suy ra  (2)

- Với (1) và (2), áp dụng luật nonce-verification ta có  (3)

- Với (3), ta áp dụng luật believe để có (*G*4)

- Với *G*4 và *A*4, ta áp dụng luật jurisdiction ta được (*G*3)

- Với *A*2 và *R*4, áp dụng luật message-meaning ta có

(4)

- Với (4) và *A*7, áp dụng luật freshness ta có (5)

- Với (4) và (5), áp dụng luật nonce-verification để có

(6)

- Với (6) áp dụng luật believe ta có (*G*2)

Với *G*1, *G*2, *G*3 và *G*4, ta đã chứng minh *U*i và *S* có thể chứng thực lẫn nhau với định danh động. Kế tiếp ta minh họa *U*i và *S* chia sẻ chung một khóa phiên *SK* như sau:

- Với *R*4 và *A*2, ta áp dụng luật message-meaning để có ds

(7)

- Với *R*4 và *A*7, áp dụng luật freshness ta có (8)

- Với (7) và (8), áp dụng luật nonce-verification ta có

(9)

- Với (9), áp dụng luật believe ta có (*G*6)

- Với *A*3 và *G*6, ta áp dụng luật jurisdiction để được (*G*5)

- Với *R*5 và *A*6, ta áp dụng luật message-meaning để được

(10)

- Với *R*5 và *A*8, áp dụng luật freshness ta có (11)

- Với (10) và (11), áp dụng luật nonce-verification ta có

(12)

- Với (12) và *A*6, áp dụng luật believe ta có (*G*8)

- Với (12) và A5, áp dụng luật message-meaning ta có (13)

- Với (13), áp dụng luật believe ta có (*G*7)

Với *G*5, *G*6, *G*7 và *G*8 ta đã chứng minh cả *S* và *U*i đều tin rằng đối phương sẽ tin *SK* đã được chia sẻ chính xác. Bên dưới là các hình thức tấn công phổ biến mà qui trình đề xuất có khả năng chống lại.

### Phân tích các hình thức tấn công phổ biến

Trong phần này, chúng tôi sẽ chứng minh qui trình đề xuất có thể ngăn chặn nhiều hình thức tấn công phổ biến dựa trên hai giả thiết. Ngữ cảnh chúng tôi đặt ra là cả máy chủ và người dùng đang chứng thực lẫn nhau trong một kênh truyền công cộng. Do đó, bất kỳ ai cũng có khả năng nghe trộm tất cả các thông điệp được truyền giữa các bên tham gia. Ngoài ra, chúng tôi giả sử rằng bất kỳ ai cũng có thể đánh cắp được các thông tin trong thẻ thành viên/thiết bị di động hay thiết bị đeo của người dùng.

**Tấn công lặp lại**

Trong hình thức tấn công này, kẻ tấn công sẽ đánh cắp các thông điệp cũ của người dùng để tấn công giao dịch kế tiếp. Tuy nhiên, điều này rất khó thực hiện trong qui trình đề xuất. Ví dụ khi kẻ tấn công gửi lại gói tin {*e*, *R*U, *R*2, *DID*i} ở một phiên nào đó để đánh lừa máy chủ, kẻ tấn công cần gửi lại *R*5 ở cuối phiên. Rõ ràng, việc biết *r*U, *id*i và *h*(*X*S || *e*) của *U*i cùng một lúc là không thể đối với kẻ tấn công. Có thể nói rằng qui trình đề xuất có khả năng chống lại hình thức tấn công này.

**Mạo danh người dùng và máy chủ**

Trong hình thức tấn công này, kẻ tấn công có hai lựa chọn đó là mạo danh người dùng hoặc mạo danh máy chủ. Trước tiên, chúng ta xét trường hợp mạo danh người dùng. Trong thông điệp đăng nhập của người dùng, chỉ có hai thông điệp mà kẻ tấn công có thể giả mạo là *e* và *R*U = *T*rU(*x*) bởi vì chúng không bao gồm thông tin định danh. Bởi thế, kẻ tấn công sẽ chọn ngẫu nhiên *r*\*U để tính *R*\*U = *T*r\*U(*x*), trong đó *e*\* là giá trị ngẫu nhiên của chính kẻ tấn công. Cuối cùng, kẻ tấn công gửi {*e*\*, *R*\*U, *R*2, *DID*i} cho máy chủ. Khi nhận được thông tin này, máy chủ tính *h*(*X*S || *e*\*) và trích *id*i bằng cách tính *DID*i ⊕ *h*(*R*\*U || *h*(*X*S || *e*\*)) = *id*i ⊕ *h*(*R*U || *h*(*X*S || *e*)) ⊕ *h*(*R*\*U || *h*(*X*S || *e*\*)). Rõ ràng máy chủ sẽ phát hiện và ngắt phiên làm việc. Thứ hai, chúng ta xét trường hợp mạo danh máy chủ. Chúng ta thấy rằng kẻ tấn công cần tính thành công {*R*S, *R*4} và điều này là không thể bởi vì *R*4 = *h*(*h*(*X*S || *e*) || *id*i || *SK*\*), trong đó *SK*\* là khóa phiên ngẫu nhiên được tính từ giá trị ngẫu nhiên *r*\*S của kẻ tấn công. Do đó, kẻ tấn công cần *h*(*X*S || *e*) và *id*i của *U*i. Tóm lại, qui trình đề xuất có khả năng chống lại hình thức tấn công mạo danh từ hai phía.

**Tính nặc danh người dùng**

Trong hình thức tấn công này, kẻ tấn công muốn biết ai là chủ nhân của giao dịch cụ thể nào đó. Bởi thế, kẻ tấn công sẽ tìm ra cách trích định danh từ *DID*i. Chúng ta thấy rằng định danh của người dùng được kết hợp giữa giá trị ngẫu nhiên *R*U và khóa *K* = *h*(*X*S || *e*). Với hai đại lượng này, kẻ tấn công không có cơ hội trích định danh thực sự của người dùng. Đặc biệt, *DID*i sẽ khác nhau ở những phiên khác nhau do tính ngẫu nhiên của *R*U. Cũng như vậy, kẻ tấn công không biết liệu *DID*i và *DID*’i có cùng thuộc về một người hay không. Do đó, qui trình đề xuất cung cấp được tính chất nặc danh người dùng.

**Tính chất an toàn tiến**

Trong hình thức tấn công này, ta giả sử các khóa chính của máy chủ và tất cả các khóa chứng thực của người dùng bị rò rỉ, hay nói cách khác đó là hệ thống hoàn toàn bị sụp đỗ. Tuy nhiên, các giao dịch trong quá khứ nên vẫn an toàn bí mật. Trong qui trình đề xuất, trường hợp rò rỉ *X*S của *S* và *h*(*X*S || *e*) của *U*i, kẻ tấn công có được *R*U = *T*rU(*x*), *R*S = *T*rS(*x*) và *id*i. Tuy nhiên, việc tính *T*rS\*rU(*x*) là không thể do gặp phải vấn đề tính toán Diffie-Hellman (CDHP). Có thể nói rằng qui trình đề xuất đạt được tính an toàn tiến dựa trên vấn đề CDHP.

Qui trình đề xuất thừa hưởng các ý tưởng tích cực của Chang và cộng sự. Ví dụ, không sử dụng mật khẩu hoặc bảng trạng thái giúp hạn chế gia tăng lượng tính toán cũng như những nguy cơ đánh cắp, hoặc dùng lượng ngẫu nhiên để loại bỏ chi phí đồng bộ hóa thời gian. Tương tự, việc dùng hàm băm mật mã cho phép người dùng tự do chọn lựa các mật khẩu mà không lo lắng về giá trị độ dài của chúng. Tóm lại, những tính chất đó hoàn toàn tồn tại trong qui trình đề xuất. Bảng 9.2 tóm tắt những khía cạnh an toàn mà qui trình cần xem xét.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất/kiểu tấn công** | **Wang [140]** | **Das [139]** | **Chang [135]** | **Qui trình đề xuất** |
| Chứng thực hai chiều | ✓ | 🗶 | ✓ | ✓ |
| Mật khẩu tự do | 🗶 | ✓ | ✓ | ✓ |
| Nặc danh người dùng | 🗶 | ✓ | 🗶 | ✓ |
| Không có bảng đăng kí | ✓ | ✓ | ✓ | ✓ |
| Tấn công mạo danh | 🗶 | 🗶 | 🗶 | ✓ |
| Không có cơ chế đồng bộ hóa thời gian | 🗶 | 🗶 | ✓ | ✓ |
| Pha thỏa hiệp khóa phiên | 🗶 | 🗶 | ✓ | ✓ |
| An toàn tiến | 🗶\* | 🗶\* | 🗶 | ✓ |
| \* Không cung cấp pha thỏa hiệp khóa phiên | | | | |

Bảng 9.2. So sánh độ an toàn giữa các qui trình

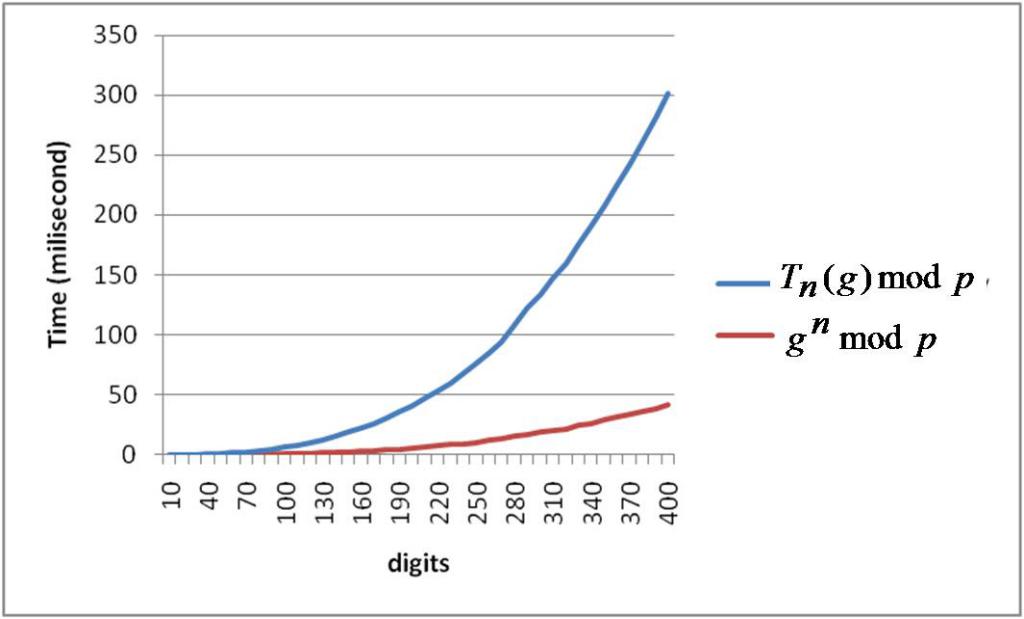
### Phân tích tính hiệu quả

Để so sánh tính hiệu quả giữa qui trình đề xuất với các qui trình trước đó, chúng tôi đặt H là thao tác băm, ↑ là thao tác lấy mũ modulo, ⊕ là thao tác XOR bit và T là thao tác tính đa thức. Ở pha đăng kí, qui trình của Das cần 1×⊕, 2×H; qui trình của Wang cần 2×⊕, 2×H; qui trình của Chang cần 1×⊕, 3×H, 1×↑; qui trình đề xuất cần 2×⊕,4×H. Ở pha đăng nhập và chứng thực, qui trình của Das cần 14×⊕, 7×H; qui trình của Wang cần 14×⊕, 6×H; qui trình của Chang cần 7×⊕, 10×H, 1×↑; qui trình đề xuất cần 4×⊕, 14×H, 4×T. So với các qui trình trước, chi phí tính toán của qui trình đề xuất gia tăng rõ rệt. Tuy nhiên, điều này là cần thiết vì sự nâng cao độ an toàn. Ngoài ra theo [134], chúng tôi tin rằng nếu được cài đặt thực tế, qui trình đề xuất vẫn đủ độ hiệu quả. Bảng 9.3 tóm tắt chi phí tính toán trong các qui trình.

|  |  |  |  |
| --- | --- | --- | --- |
| **Qui trình** | **Pha chứng thực** | **Pha đăng nhập** | **Pha đăng kí** |
| Das [139] | 3×H, 7×⊕ | 4×H, 7×⊕ | 2×H, 1×⊕ |
| Wang [140] | 4×H, 10×⊕ | 2×H, 4×⊕ | 2×H, 2×⊕ |
| Chang [135] | 8×H, 4×⊕, 1×↑ | 2×H, 3×⊕ | 3×H, 1×⊕, 1×↑ |
| Qui trình đề xuất | 10×H, 2×⊕, 3×T | 4×H, 2×⊕, 1×T | 4×H, 2×⊕ |

Bảng 9.3. So sánh chi phí tính toán

Ta đặt tH, t⊕, tT, t↑ đại diện cho thời gian chạy tương ứng với mỗi thao tác H, ⊕, T, ↑. Chúng tôi thấy rằng t⊕ << tH << t↑ << tT, vì vậy chúng tôi chỉ so sánh giữa hai thuật toán, lấy mũ modulo và thao tác tính đa thức Chebysev, những thao tác được qui trình đề xuất và qui trình của Chang sử dụng. Để so sánh tương đối, chúng tôi cài đặt lại *T*n(*g*) mod *p* sử dụng lớp BigInteger trong Java. Tương tự, chúng tôi sử dụng lại hàm “ModPow” trong Java để đại diện cho thao tác *g*n mod *p*. Thí nghiệm của chúng tôi được xây dựng trên máy tính cá nhân Core 2 Quad CPU 2.66GHz. Bằng cách đo thời gian chạy giữa hai thuật toán với các số nguyên tố từ 10 tới 400 kí số, chúng tôi đề xuất sử dụng số nguyên tố 512-bit để đảm bảo tính hiệu quả về thời gian (≈ 150ms) và vẫn giữ được độ an toàn vì không gian nghiệm lên tới 2512 khi gặp phải vấn đề CDLP. Mặc dù, thời gian chạy giữa thao tác *g*n mod *p* và *T*n(*g*) mod *p* có sự khác biệt, tuy nhiên thời gian chạy của qui trình đề xuất khoảng ≈ 0.6s khi dùng số nguyên tố hợp lí. Vì vậy, có thể nói rằng qui trình đề xuất vẫn đủ hiệu quả khi cài đặt thực tế. Kết quả thí nghiệm với các số nguyên tố khác nhau được trình bày trong hình 4.3.1.



Hình 9.1. So sánh chi phí thời gian giữa *T*n(*g*) mod *p* và *g*n mod *p*

## Kết chương

Trong chương này, chúng tôi tập trung khảo sát qui trình của Chang và các cộng sự. Mặc dù qui trình của họ có một vài ý tưởng tích cực, tuy nhiên nó vẫn dễ bị tổn thương đối với một số hình thức tấn công phổ biến như mạo danh từ các bên tham gia. Ngoài ra nó cũng không có tính chất an toàn tiến và không cung cấp tính nặc danh người dùng, một trong những thuộc tính riêng tư quan trọng trong nhiều ứng dụng trực tuyến. Do đó, chúng tôi đề xuất một qui trình cải tiến với hướng tiếp cận dùng đa thức Chebysev để khắc phục những nhược điểm trên. So với những qui trình trước, qui trình chúng tôi có một số lợi thế sau; (1) Người dùng không cần chọn mật khẩu trước. (2) Qui trình cung cấp tính nặc danh người dùng. (3) Qui trình không lưu bảng kiểm tra. (4) Qui trình cung cấp tính chất an toàn tiến. Trong tương lai, chúng tôi sẽ nghiên cứu kết hợp đặc trưng sinh trắc học vào các qui trình chứng thực dựa trên đa thức Chebysev để gia tăng độ an toàn cũng như tiện dụng cho người dùng.

# 

# Tài liệu tham khảo

[1] A. K. Jain, A. Ross, S. Prabhakar, “An Introduction to Biometric Recognition”, in IEEE Transaction on Circuits and System for Video Technology, Vol. 14, No. 1, 2004.

[2] M. O.Derawi, C. Nickely, P. Bour, C. Busc, “Unobtrusive User-Authentication on Mobile Phone susing Biometric Gait”, Proceedings of 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, tr. 306-311, 2010.

[3] Jennifer R. Kwapisz, Gary M. Weiss, and Samuel A. Moore, “Cell Phone-Based Biometric Identification”, Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS 2010), tr. 1-7, 2010.

[4] D. Gafurov, “Performance and security analysis of gait-based user authentication,” PhD dissertation, Faculty of Mathematical and Natural Science, University of Oslo, 2008.

[5] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S. M. Mäkelä, H. Ailisto, “Identifying Users of Portable Devices From Gait Pattern With Accelerometers”, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05), tr. 973-976, 2005

[6] H. W. Reese, D. Rodeheaver, “Age-related declinces in motor control,” Handbook of the Psychology of Aging, 5th ed., C. J. Ketcharn and G. E. Stelmach, Eds., USA, tr. 333–335, 2001

[7] S. Mondal, A. Nandy, P. Chakraborty, G.C Nandi, "Gait Based Personal Identification System Using Rotation Sensor", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 3, tr. 395-402, 03/2012.

[8] H. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjounaite, S.M. Makela, "Identifying People from Gait Pattern with Accelerometers", Proceeding of SPIE 5779, Biometric Technology for Human Identification II, tr. 7-14, 2005.

[9] S. Terada, Y. Enomoto, D. Hanawa, K. Oguchi, “Performance of gait authentication using an acceleration sensor”, 34th International Conference on Telecommunications and Signal Processing (TSP 2011), tr. 34-36, 2011

[10] G. Pan, Y. Zhang and Z. Wu, "Accelerometer-based gait recognition via voting by signature points", IET Electronic Letters Vol. 45, No. 22, tr. 1116-1118, 10/2009.

[11] P. Bours, R. Shrestha, "Eigensteps: A giant leap for gait recognition", The 2nd International Workshop on Security and Communication Networks (IWSCN 2010), tr. 1-6, 2010

[12] F. Frank, S. Mannor, D. Precup, “Activity and Gait Recognition with Time-Delay Embeddings”, The 24th AAAI Conference on Artificial Intelligence (AAAI 2010), tr. 1581-1586, 2010.

[13] Ngo, T.T.; Makihara, Y.; Nagahara, H.; Mukaigawa, Y.; Yagi, Y. Similar gait action recognition using an inertial sensor. Pattern Recognit. 2015, 48, 1289–1301.

[14] Öberg, T.; Karsznia, A.; Öberg, K. Basic gait parameters: Reference data for normal subjects, 10–79 years of age. J. Rehabil. Res. Dev. 1993, 30, 210–216.

[15] Cutting, J.E.; Kozlowski, L.T. Recognizing friends by their walk: Gait perception without familiarity cues. Bull. Psychon. Soc. 1977, 9, 353–356.

[16] Wang, L.; Tan, T.; Ning, H.; Hu, W. Silhouette analysis-based gait recognition for human identification. IEEE Trans. Pattern Anal. Mach. Intell. 2003, 25, 1505–1518.

[17] Gafurov, D. A survey of biometric gait recognition: Approaches, security and challenges. In Proceedings of the Annual Norwegian Computer Science Conference, Oslo, Norway, 19–21 November 2007; pp. 19–21.

[18] Ailisto, H.J.; Lindholm, M.; Mantyjarvi, J.; Vildjiounaite, E.; Makela, S.M. Identifying people from gait pattern with accelerometers. Proc. SPIE 2005, 5779, 7–14.

[19] Mantyjarvi, J.; Lindholm, M.; Vildjiounaite, E.; Makela, S.M.; Ailisto, H.A. Identifying users of portable devices from gait pattern with accelerometers. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Philadelphia, PA, USA, 18–23 March 2005; pp. 973–976.

[20] Gafurov, D.; Helkala, K.; Søndrol, T. Biometric gait authentication using accelerometer sensor, J. Comput. 2006, 1, 51–59.

[21] Ngo, T.T.; Makihara, Y.; Nagahara, H.; Mukaigawa, Y.; Yagi, Y. The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication. Pattern Recognit. 2014, 47, 228–237.

[22] Ngo, T.T.; Makihara, Y.; Nagahara, H.; Mukaigawa, Y.; Yasushi, Y. Orientation-compensative signal registration for owner authentication using an accelerometer. IEICE Trans. Inf. Syst. 2014, 97, 541–553.

[23] Zhang, Y.; Pan, G.; Jia, K.; Lu, M.; Wang, Y.; Wu, Z. Accelerometer-Based Gait Recognition by Sparse Representation of Signature PointsWith Clusters. IEEE Trans. Cybern. 2014

[24] Sprager, S.; Zazula, D. A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine. WSEAS Trans. Signal Proc. 2009, 5, 369–378.

[25] Derawi, M.O.; Nickel, C.; Bours, P.; Busch, C. Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. In Proceedings of the Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Darmstadt, Germany, 15–17 October 2010; pp. 306–311.

[26] Frank, J.; Mannor, S.; Precup, D. Activity and Gait Recognition with Time-Delay Embeddings. In Proceedings of the AAAI, Atlanta, GA, USA, 11–15 July 2010.

[27] Kwapisz, J.R.; Weiss, G.M.; Moore, S.A. Cell phone-based biometric identification. In Proceedings of the Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; pp. 1–7.

[28] Lu, H.; Huang, J.; Saha, T.; Nachman, L. Unobtrusive gait verification for mobile phones. In Proceedings of the 2014 ACM International Symposium on Wearable Computers, Seattle, WA, USA, 13–17 September 2014; pp. 91–98.

[29] Rong, L.; Zhiguo, D.; Jianzhong, Z.; Ming, L. Identification of individual walking patterns

using gait acceleration. In Proceedings of the 1st International Conference on Bioinformatics and Biomedical Engineering (ICBBE), Wuhan, China, 6–8 July 2007; pp. 543–546.

[30] Rong, L.; Jianzhong, Z.; Ming, L.; Xiangfeng, H. A wearable acceleration sensor system for gait recognition. In Proceedings of the 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA), Harbin, China, 23–25 May 2007; pp. 2654–2659.

[31] Trung, N.T.; Makihara, Y.; Nagahara, H.; Sagawa, R.; Mukaigawa, Y.; Yagi, Y. Phase registration in a gallery improving gait authentication. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–7.

[32] Sun, H.; Yuao, T. Curve aligning approach for gait authentication based on a wearable accelerometer. Physiol. Meas. 2012, 33, 1111–1120.

[33] Frank, J.; Mannor, S.; Pineau, J.; Precup, D. Time Series Analysis Using Geometric Template Matching. IEEE Trans. Pattern Anal. Mach. Intell. 2013, 35, 740–754.

[34] Zhong, Y.; Deng, Y. Sensor orientation invariant mobile gait biometrics. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Clearwater, FL, USA, 29 September–2 October 2014; pp. 1–8.

[35] Sprager, S.; Juric, M.B. An efficient HOS-based gait authentication of accelerometer data. IEEE Trans. Inf. Forensics Secur. 2015, 10, doi:10.1109/TIFS.2015.2415753 .

[36] Subramanian, R.; Sarkar, S.; Labrador, M.; Contino, K.; Eggert, C.; Javed, O.; Zhu, J.; Cheng, H. Orientation invariant gait matching algorithm based on the Kabsch alignment. In Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), Hong Kong, China, 23–25 March 2015; pp. 1–8.

[37] Trivino, G.; Alvarez-Alvarez, A.; Bailador, G. Application of the computational theory of perceptions to human gait pattern recognition. Pattern Recognit. 2010, 43, 2572–2581.

[38] Derawi, M.; Bours, P. Gait and activity recognition using commercial phones. Comput. Secur. 2013, 39, 137–144.

[39] Nickel, C.; Busch, C. Classifying accelerometer data via hidden markov models to authenticate people by the way they walk. IEEE Aeros. Electron. Syst. Mag. 2013, 28, 29–35.

[40] Ren, Y.; Chen, Y.; Chuah, M.C.; Yang, J. User Verification Leveraging Gait Recognition for Smartphone Enabled Mobile Healthcare Systems. IEEE Trans. Mob. Comput. 2014

[41] Sun, B.; Wang, Y.; Banda, J. Gait Characteristic Analysis and Identification Based on the iPhone’s Accelerometer and Gyrometer. Sensors 2014, 14, 17037–17054.

[42] Hoang, T.; Choi, D.; Nguyen, T. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Int. J. Inf. Secur. 2015, 1–12.

[43] Primo, A.; Phoha, V.V.; Kumar, R.; Serwadda, A. Context-Aware Active Authentication Using Smartphone Accelerometer Measurements. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Columbus, OH, USA, 23–28 June 2014; pp. 98–105.

[44] Hoang, T.; Choi, D. Secure and Privacy Enhanced Gait Authentication on Smart Phone. Sci. World J. 2014, 2014, 1–8.

[45] Muaaz, M.; Mayrhofer, R. Orientation Independent Cell Phone Based Gait Authentication. In Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, Kaohsiung, Taiwan, 8–10 December 2014; pp. 161–164.

[46] Muaaz, M.; Mayrhofer, R. An analysis of different approaches to gait recognition using cell phone based accelerometers. In Proceedings of the International Conference on Advances in Mobile Computing & Multimedia, Vienna, Austria, 2–4 December 2013; pp. 293.

[47] Juefei-Xu, F.; Bhagavatula, C.; Jaech, A.; Prasad, U.; Savvides, M. Gait-ID on the move: Pace independent human identification using cell phone accelerometer dynamics. In Proceedings of the IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 23–27 September 2012; pp. 8–15.

[48] Ren, Y.; Chen, Y.; Chuah, M.C.; Yang, J. Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), New Orleans, LA, USA, 24–27 June 2013; pp. 149–157.

[49] Nickel, C.; Derawi, M.O.; Bours, P.; Busch, C. Scenario test of accelerometer-based biometric gait recognition. In Proceedings of the Third International Workshop on Security and Communication Networks (IWSCN), Gjovik, Norway, 18–20 May 2011; pp. 15–21.

[50] Nickel, C.; Busch, C. Does a cycle-based segmentation improve accelerometer-based biometric gait recognition? In Proceedings of the 11th International Conference on Information Science, Signal Processing and their Applications (ISSPA), Montreal, QC, Canada, 2–5 July 2012; pp. 746–751.

[51] Youn, I.H.; Choi, S.; Le May, R.; Bertelsen, D.; Youn, J.H. New gait metrics for biometric authentication using a 3-axis acceleration. In Proceedings of the IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2014; pp. 596–601.

[52] Bours, P.; Shrestha, R. Eigensteps: A giant leap for gait recognition. In Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN), Karlstad, Sweden, 26–28 May 2010; pp. 1–6.

[53] R. Sarikaya, G. Hinton, and A. Deoras, Application of Deep Belief Networks for Natural Language Understanding, IEEE Transactions on Audio Speech and Language Processing, 2014

[54] S. Lazebnik, C. Schmid, and J. Ponce, Beyond Bags of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories, CVPR, 2006

[55] Large Scale Visual Recognition Challenge 2012 (ILSVRC2012): http://www.image-net.org/challenges/LSVRC/2012/, 2012

[56] Large Scale Visual Recognition Challenge 2014 (ILSVRC2014) Results: http://image-net.org/challenges/LSVRC/2014/results.php

[57] Large Scale Visual Recognition Challenge 2013 (ILSVRC2013) Results: http://www.image-net.org/challenges/LSVRC/2013/results.php

[58] M. D. Zeiler and R. Fergus, Visualizing and Understanding Convolutional Networks, ECCV 2014, Lecture Notes in Computer Science, vol. 8689, , pp. 818-833, 2014

[59] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever and R. Salakhutdinov, Dropout: A Simple Way to Prevent Neural Networks from Overfitting, The Journal of Machine Learning Research,15(1), pp. 1929-1958, 2014

[60] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, Caffe: Convolutional Architecture for Fast Feature Embedding, in Proceedings of the ACM International Conference on Multimedia (MM’14), pp. 675-678, 2014.

[61] M. D. Zeiler, M. Ranzato, R. Monga, M. Mao, K. Yang, Q. V. Le, P. Nguyen, A. Senior, V. Vanhoucke, J. Dean, G. E. Hinton, On Rectified Linear Units for Speech Processing, 38th International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013.

[62] M. A. Nielsen, Neural Networks and Deep Learning, Determination Press, 2015.

[63] A. Mohamed, G. E. Dahl, and G. Hinton, Acoustic Modeling Using Deep Belief Networks, Trans. Audio, Speech and Lang. Proc., 20(1), pp. 14-22, 2010

[64] A. Krizhevsky, S. Ilya, and Geoffrey E. Hinton, ImageNet Classification with Deep Convolutional Neural Networks, Advances in Neural Information Processing Systems (NIPS), pp. 1097-1105, 2012

[65] A. Ng, J. Ngiam and C. Y. Foo, "Deep Learning Tutorial," Stanford University,[Online] . Available: http://ufldl.stanford.edu/tutorial/.[Accessed 22 7 2015] .

[66] Chat\_eld, K., Simonyan, K., Vedaldi, A., Zisserman, A.: Return of the devil in the details: Delving deep into convolutional nets. In: British Machine Vision Conference, BMVC 2014 (2014)

[67] Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. Computing Research Repository - CoRR abs/1409.1556 (2014)

[68] Srivastava, N., Hinton, G.E., Krizhevsky, A., Sutskever, I., Salakhutdinov, R.: Dropout: a simple way to prevent neural networks from over\_tting. Journal of Machine Learning Research 15(1), 1929\_1958 (2014)

[69] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Van-houcke, V., Rabinovich, A.: Going deeper with convolutions. Computing Research Repository-CoRR abs/1409.4842 (2014)

[70] [N. T. Trung](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.N.%20T.%20Trung.QT.&newsearch=true), [Y. Makihara](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Y.%20Makihara.QT.&newsearch=true) ; [H. Nagahara](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.H.%20Nagahara.QT.&newsearch=true) ; [Y. Mukaigawa](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Y.%20Mukaigawa.QT.&newsearch=true), Y. Yagi, “Performance Evaluation of Gait Recognition using the Largest Inertial Sensor-based Gait Database,” The [5th IAPR International Conference on Biometrics (ICB 2012)](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6195082), pp. 360-366, 2012.

[71] [N. T. Trung](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.N.%20T.%20Trung.QT.&newsearch=true), [Y. Makihara](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Y.%20Makihara.QT.&newsearch=true) ; [H. Nagahara](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.H.%20Nagahara.QT.&newsearch=true) ; [Y. Mukaigawa](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Y.%20Mukaigawa.QT.&newsearch=true), Y. Yagi,, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," Pattern Recognition Vol.47 (1), pp. 222-231, 2014

[72] Sebastijan Sprager, Matjaz B. Juric, “Inertial Sensor-Based Gait Recognition: A Review,” Sensors, Vol 15, pp. 22089-22127, MDPI, 2015.

[73] Hoang, T., Choi, D., Vo, V., Nguyen, A., Nguyen, T.: “A lightweight gait authentication on mobile phone regardless of installation error,” In: Security and Privacy Protection in Information Processing Systems, pp. 83–101. Springer, Berlin (2013).

[74] N. Trung, Y.Makihara, H.Nagahara, R.Sagawa, Y.Mukaigawa, Y.Yagi, “Phase registration in a gallery improving gait authentication,” in:International Joint Conference on Biometrics(IJCB2011),IEEE and IAPR, 2011, pp.1–7

[75] Chafika Benzaida, Karim Lounisa, Ameer Al-Nemratb, Nadjib Badachea, Mamoun Alazab: Fast authentication in wireless sensor networks. Future Generation Computer Systems, Volume 55, February 2016, Pages 362–375

[76] Hande Alemdar, Cem Ersoy: Wireless sensor networks for healthcare: A survey. Computer Networks, Volume 54, Issue 15, 28 October 2010, Pages 2688–2710.

[77] Bushra Rashid, Mubashir Husain Rehmani: Applications of wireless sensor networks for urban areas: A survey. Journal of Network and Computer Applications, Volume 60, January 2016, Pages 192–219.

[78] Ding Wang, Ping Wang: On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Computer Networks, Volume 73, 14 November 2014, Pages 41–57.

[79] Vanga Odelua, Ashok Kumar Dasb, Adrijit Goswami: An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. Journal of Information Security and Applications, Volume 21, April 2015, Pages 1–19.

[Z6] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun, Kouichi Sakurai: Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications, Volume 61, February 2016, Pages 59–80.

[80] He Debiao, Chen Jianhua, Hu Jin: An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security. Information Fusion 13 (3) (July 2012), 223–230.

[81] Lamport, L., Password authentication with insecure communication. Communications of the ACM 1981; 24(11): 770 – 772.

[82] Shamir, A., 1984. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO’84 on Advances in Cryptology. Springer-Verlag, New York, USA, pp. 47–53.

[83] Hwang, M.S., Lee, C.C., Tang, Y.L.: A Simple Remote User Authentication Scheme. Mathematical and Computer Modelling. Vol. 36 (2002)103-107.

[84] Lee, C.C., Hwang, M.S., Yang, W.P.: Flexible Remote User Authentication Scheme Using Smart Cards. ACM Operating Systems Review. Vol. 36. No. 3 (2002) 46-52.

[85] Li, L.H., Lin, I.C., Hwang, M.S.: A Remote Password Authentication Scheme for Multi server Architecture Using Neural Networks. IEEE Transactions on Neural Networks. Vol.12. No. 6 (2001) 1498-1504.

[86] Shen, J.J., Lin, C.W., Hwang, M.S.: A Modified Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics. Vol.49. No. 2 (2003) 414-416.

[87] Das, M.L., Saxena, A., Gulati, V.P.: A Dynamic ID-based Remote User Authentication Scheme. IEEE Transactions on Consumer Electronics. Vol. 50. No. 2 (2004) 629-631.

[88] Liao, I.E., Lee, C.C., Hwang, M.S.: Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme. IEEE Computer Society. Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP 2005). (2005) 437-440.

[89] Yoon E.J., Yoo K.Y.: Improving the Dynamic ID-based Remote Mutual Authentication Scheme. Springer Verlag Berlin Heidelberg. OTM Workshops 2006. LNCS 4277, pp. 499 – 507.

[90] Muhammad Khurram Khan, Soo-Kyun Kimb, Khaled Alghathbar: Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme’. Computer Communications Volume 34, Issue 3, 15 March 2011, Pages 305–309.

[91] Sandeep K. Sood, Anil K. Sarje, Kuldip Singh: A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications 34 (2011) 609–618.

[92] Muhammad Khurram Khan, Saru Kumari, Mridul K. Gupta: More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing (2013) DOI 10.1007/s00607-013-0308-2.

[93] Lee J-K, Ryu S-R, Yoo K-Y: Fingerprint-based remote user authentication scheme using smart cards. Electronics Letters 2002; 38 (12): 554–5.

[94] Lin I-C, Hwang M-S, Li L-H: A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems 2003; 19 (1): 13–22.

[95] Khan M-K, Zhang J-S: Improving the security of ‘a flexible biometrics remote user authentication scheme’. Computer Standards & Interfaces 2007; 29 (1): 82–5.

[96] Li C-T, Hwang M-S: An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 2010; 33 (1): 1–5.

[97] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, Cheng-Lian Liu: Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 34 (2011) 73–79.

[98] Jian-Zhu Lu, Jipeng Zhou: Preventing delegation-based mobile authentications from man-in-the-middle attacks. Computer Standards & Interfaces, Volume 34, Issue 3, March 2012, Pages 314–326.

[99] C.-L. Chen, C.-C. Lee, and C.-Y. Hsu: Mobile device integration of a ﬁngerprint biometric remote authentication scheme. International Journalof Communication Systems 25 (2011) 585 – 597.

[100] Rivest RL, Shamir A, Adleman L: A method for obtaining digital signatures and publickey cryptosystems. Communications of the ACM 1978; 21(2): 120–6.

[101] El Gamal T: A publickey cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information 1985; IT-31: 469–72.

[102] Miller VS: Use of elliptic curves in cryptography. Advances in cryptology, proceedings of CRYPTO’85, LNCS, Springer-Verlag 218 (1986). 417–26.

[103] Koblitz N: Elliptic curvecrypto system. Mathematics of Computation 48 (1987). 203–209.

[104] Hankerson D, Menezes A, Vanstone S: Guide to elliptic curve cryptography. NewYork, USA: LNCS, Springer-Verlag; 2004.

[105] Tian X, Wong DS, Zhu RW: Analysis and improvement of authenticated key exchange protocol for sensor networks. IEEE Communications Letters 2005; 9(11): 970–972.

[106] Choie YJ, Jeong E, Lee E: Efficient identity-based authenticated key agreement protocol from pairings. Applied Mathematics and Computation 2005; 162: 179–88.

[107] Wu ST, Chiu JH, Chieu BC: ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography. Proceedings of IEEE international conference on electro information technology; 2005.

[108] Jen-Ho Yang, Chin-Chen Chang: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers & security 28 (2009) 138–143.

[109] E.-J. Yoon and K.-Y. Yoo: Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc. Computational Science and Engineering, IEEE International Conferenceon, vol.2, pp. 633–640, 2009.

[110] S.H. Islam and G.P. Biswas: A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software, vol.84, no.11, pp.1892–1898, 2011.

[111] Canetti, R, Krawczyk, H: Analysis of Key Exchange Schemes and Their Use for Building Secure Channels. Advances in Cryptology-Eurocrypt ‘01, 2045 Springer-Verlag, Berlin, Germany, pp. 451–472 (LNCS, May 6–10).

[112] L. Kocarev and Z. Tasev: Public-key encryption based on Chebyshev maps. Proceedings of the International Symposium on Circuits and Systems (ISCAS’03), vol.3, May 2003, pp. III-28-III-31.

[113] P. Bergamo, P.D’Arco, A. Santis, and L. Kocarev: Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Transactions on Circuits and Systems-I, vol. 52, no. 7, Jul. 2005, pp. 1382-1393.

[114] D. Xiao, X. Liao, and S. Deng: A novel key agreement protocol based on chaotic maps. Information Sciences, vol. 177, no. 4, Feb. 2007, pp. 1136-1142.

[115] E.J. Yoon and K.Y. Yoo: A new key agreement protocol based on chaotic maps. Proceedings of The Second KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA’08), Mar. 2008, pp. 897-906.

[116] Cheng Guo, Chin-Chen Chang, Chin-Yu Sun: Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Communications. Journal of Information Hiding and Multimedia Signal Processing. Volume 4 (2), 2013, 99 - 109.

[117] Ding Wang, Chun-guang Ma: Cryptanalysis of a remote user authentication scheme for mobile client–server environment based on ECC. Information Fusion. Volume 14 (4), 2013, 498 – 503.

[118] Yi-Pin Liao, Chih-Ming Hsiao: A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Networks. Volume 18, 2014, 133 – 146.

[119] Han-Yu Lin: Improved chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation. Volume 20 (2), 2015, 482 – 488.

[120] Tian-Fu Lee: An Efficient Chaotic Maps-Based Authenticationand Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems. Journal of Medical Systems. Volume 37 (6): 9985, 2013.

[121] Kuo-Hui Yeh: A Provably Secure Multi-server Based Authentication Scheme. Wireless Personal Communications. Volume 79 (3), 2014, 1621 – 1634.

[122] M. Burrows, M. Abadi, and R. Needham: A logic of authentication, ACM Transactions on Computer System. Volume 8, 1990, 18 – 36.

[123] Tien-Ho Chen, Yen-Chiu Chen, Wei-Kuan Shih, Hsin-Wen Wei: An efficient anonymous authentication protocol for mobile pay-TV. Journal of Network and Computer Applications 34 (2011) 1131–1137

[124] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proceedings of Advances in Cryptology–Crypto’99, Santa Barbara, USA (1999), 388–397.

[125] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smartcard security under the threat of power analysis attacks, IEEE Transactions on Computers 51 (5) (2002), 541–552.

[126] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, tập. 24, số. 11, trang. 770-772, 1981.

[127] T.H. Chen, Y.C. Chen, W.K. Shih, and H.W. Wei, “An efficient anonymous authentication protocol for mobile pay-tv,” Journal of Network and Computer Applications, tập. 34, số. 4, trang. 1131-1137, 2011.

[128] S. Shin, K. Kim, K.H. Kim, and H. Yeh, “A remote user authentication scheme with anonymity for mobile devices,” International Journal of Advanced Robotic Systems, tập. 9, số. 13, trang. 1-7, 2012.

[129] I.E. Liao, C.C. Lee, and M.S. Hwang, “Security enhancement for a dynamic id-based remote user authentication scheme,” International Conference on Next Generation Web Services Practices, tập. 6, số. 2, trang. 517-522, 2005.

[130] K. Wang, W.J. Pei, L.H. Zou, Y.M. Cheung, and Z.Y. HE, “Security of public key encryption technique based on multiple chaotic system,” Journal of Physics Letters A, tập. 360, số.2, trang. 259-262, 2006.

[131] L. Zhang, “Cryptanalysis of the public key encryption based on multiple chaotic systems,” Journal of Chaos, Solitons & Fractals, tập. 37, số. 3, trang. 669-674, 2008.

[132] C. Guo, C.C. Chang, and C.Y. Sun, “Chaotic maps-based mutual authentication and key agreement using smartcards for wireless communications,” Journal of Information Hiding and Multimedia Signal Processing, tập. 4, số. 2, trang. 99-109, 2013.

[133] K. Prasadh, K. Ramar, and R. Gnanajeyaraman, “Public key cryptosystems based on chaotic chebyshev polynomials,” Journal of Engineering and Technology Research, tập. 1, số. 7, trang. 122-128, 2009.

[134] L. Zhi-hui, C. Yi-dong, and X. Hui-min, “Fast algorithms of publickey cryptosystem based on chebyshev polynomials over finite field,” The Journal of China Universities of Posts and Telecommunications, tập. 18, số. 2, trang. 86-93, 2010.

[135] C.C. Chang and C.Y. Lee, “A smartcard-based authentication scheme using user identify cryptography,” International Journal of Network Security, tập. 15, số. 2, trang. 139-147, 2013.

[136] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” ACM Transactions on Computer System, tập. 8, trang. 18-36, 1990.

[137] D. Xiao, X. Liao, and K. Wong, “An efficient entire chaos-based scheme for deniable authentication,” Journal of Chaos, Solitons & Fractals, tập. 23, số. 4, trang. 1327-1331, 2005.

[138] P. Bergamo, P. Arco, A. Santis, and L. Kocarev, “Security of public key encryption technique based on multiple chaotic system,” IEEE Transactions on Circuits and Systems I, tập. 52, số. 7, trang. 1382-1393, 2005.

[139] M.L. Das, A. Saxena, and V.P. Gulati, “A dynamic id-based remote user authentication scheme,” IEEE Transactions on Consumer Electronics, tập. 50, số. 2, trang. 629-631, 2004.

[140] Y.Y. Wang, J.Y. Kiu, F.X. Xiao, and J. Dan, “A more efficient and secure dynamic id-based remote user authentication scheme,” Computer Communications, tập. 32, số. 4, trang. 583-585, 2009.

[141] E.J. Yoon and K.Y. Yoo, “Improving the dynamic id-based remote mutual authentication scheme,” First International Workshop on Information Security, tập. 4277, trang. 499-507, 2006.

[142] R.L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and publickey cryptosystems,” Communications of the ACM, tập. 21, số. 2, trang. 120-126, 1978.

[143] J.H. Yang and C.C. Chang, “An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Computers and Security, tập. 28, số. 3-4, trang. 138-143, 2009.

[144] E.J. Yoon and K.Y. Yoo, “Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc,” IEEE International Conference on Computational Science and Engineering, tập. 2, trang. 633-640, 2009.

[145] S.H. Islam and G.P. Biswas, “A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Journal of Systems and Software, tập. 84, số. 11, trang. 1892-1898, 2011.

[146] Khan, M. K., Kumari, S., Gupta, M. K.: More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing, vol 96, pp. 793-816. 2013.

[147] Khan, M. K., Kumari, S.: An improved biometrics-based remote user authentication scheme with user anonymity. Journal of Biomedicine and Biotechnology, Vol. 2013 (2013).

[148] RU Rehman(2008). Get Ready for OpenID. Conformix Technologies Inc.

[149] Sarvabhatla, M., Giri, M., Vorugunti, C.S.: A secure biometrics-based remote user authen-tication scheme for secure data exchange. Embedded Systems 2014. pp.110-115 (2014)

[150] Wen, F., Susilo, W., Yang, G.: Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards. Journal of Wireless Personal Communi-cations, Volume 80, Issue 4, pp. 1747-1760 (2014)

[CT1] Toan-Thinh Truong[,](mailto:ttthinh@fit.hcmus.edu.vn) Minh-Triet Tran, Anh-Duc Duong, Isao Echizen, “Chaotic Chebyshev polynomials based remote user authentication scheme in client-server environment,” International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2015), May 26–28, 2015, Hamburg, Đức, Volume 455, IFIP Advances in Information and Communication Technology, tr. 479-494, Springer

[CT2] Duong-Tien Phan, Nhan Nguyen-Trong Dam, Minh-Phuc Nguyen, Minh-Triet Tran, Toan-Thinh Truong, “Smart Kiosk with Gait-Based Continuous Authentication,” Third International Conference on Distributed, Ambient, and Pervasive Interactions (DAPI 2015), August 2-7, 2015, Los Angeles, CA, Mỹ, Volume 9189, Lecture Notes in Computer Science, tr. 188-200, Springer.

[CT3] Nhan Nguyen-Trong Dam, [Vinh-Tiep Nguyen](http://dblp.uni-trier.de/pers/hd/n/Nguyen:Vinh=Tiep), [Minh N. Do](http://dblp.uni-trier.de/pers/hd/d/Do:Minh_N=), [Anh Duc Duong](http://dblp.uni-trier.de/pers/hd/d/Duong:Anh_Duc), Minh-Triet Tran, “Realtime Face Verification with Lightweight Convolutional Neural Networks,” 11th International Symposium on Advances in Visual Computing (ISVC 2015), Las Vegas, NV, USA, December 14-16, 2015, Volume 9475, Lecture Notes in Computer Science, tr. 420-430, Springer.

[CT4] Duong-Tien Phan, Toan-Thinh Truong, Minh-Triet Tran, Anh-Duc Duong, “Two-way Biometrics-based Authentication Scheme on Mobile Devices”, Proceedings of The 1st International Conference on Future Data and Security Engineering, November 19-21, 2014, Lecture Notes in Computer Science (LNCS) Vol 8860, tr. 117-130, Springer 2014