



TRƯỜNG ĐẠI HỌC  
BÁCH KHOA HÀ NỘI  
HANOI UNIVERSITY  
OF SCIENCE AND TECHNOLOGY

# HỆ MẬT SINH TRẮC DỰA TRÊN DẤU VÂN TAY VÀ MẬT MÃ

Sinh viên thực hiện: Hoàng Văn Thành

Giảng viên hướng dẫn: PGS. TS. Nguyễn Đình Hân

ONE LOVE. ONE FUTURE.

1. Bài toán định danh người dùng
2. Dữ liệu sinh trắc dấu vân tay
3. Hệ mật đa trị MAS
4. Hệ thống kết hợp mật mã và sinh trắc vân tay

# 1. Bài toán xác thực người dùng

- **Xác thực người dùng** là thủ tục gắn liền với giao tiếp giữa hai hoặc nhiều bên, trong đó một bên tiến hành xác minh bên kia là đối tượng thực sự hay giả mạo.



# 1. Bài toán xác thực người dùng

Các phương pháp xác thực người dùng:

- Dựa trên mật khẩu
- Dựa trên tri thức
- Dựa trên thách thức – đáp ứng
- Dựa trên dữ liệu sinh trắc học
- Dựa trên kết hợp nhiều phương pháp
- ...

## 2. Dữ liệu sinh trắc dấu vân tay








**Dấu vân tay:** là dấu vết của các đường vân trên bàn tay của con người khi chạm vào các bề mặt. Các đường vân tay là độc nhất và không thay đổi.



## 2. Dữ liệu sinh trắc dấu vân tay

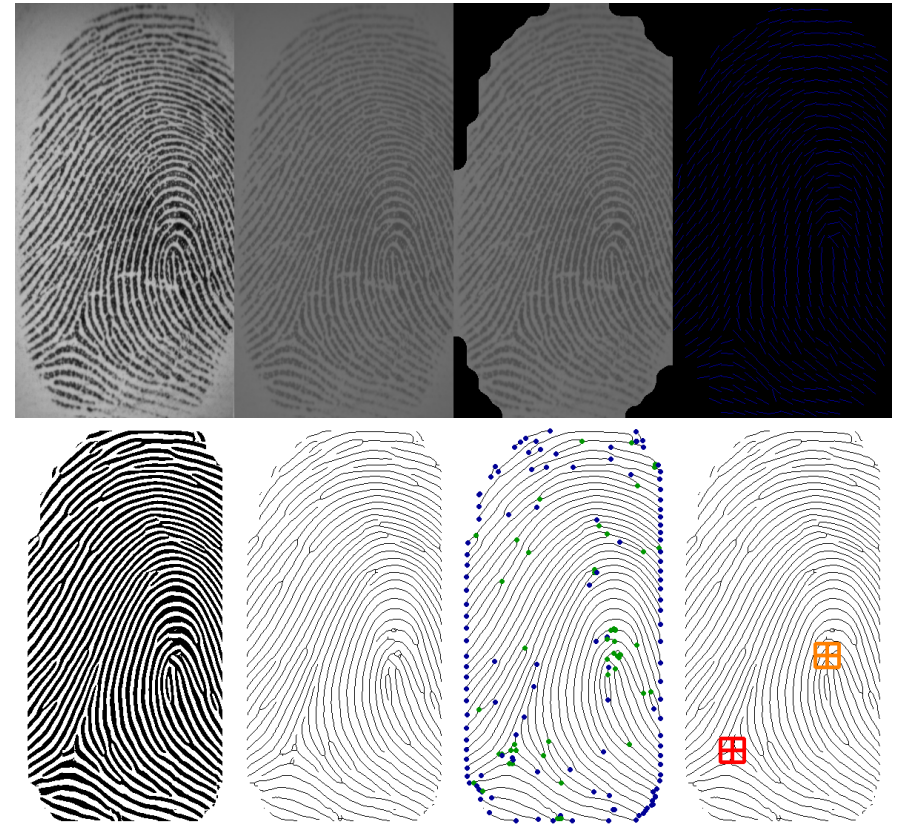
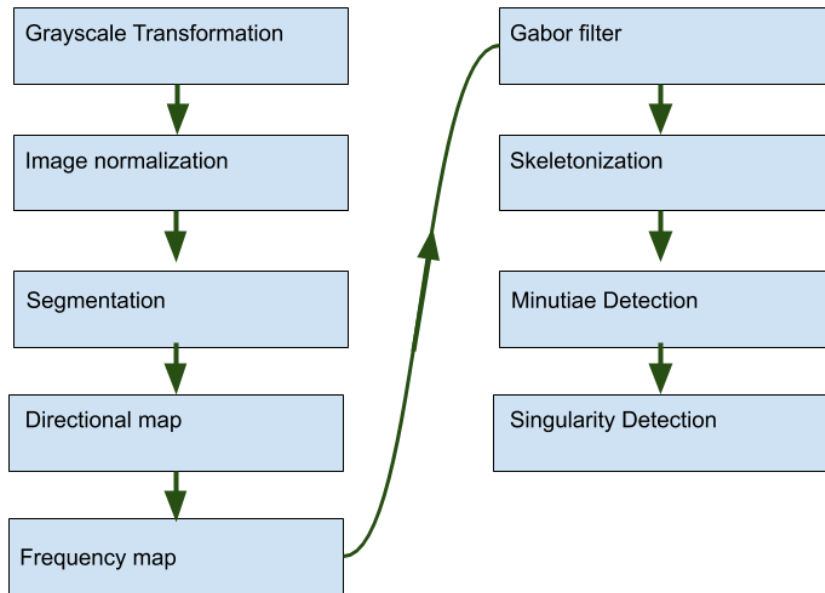
### Các đặc trưng của dấu vân tay:

- Điểm kết thúc đường vân
- Điểm rẽ nhánh đường vân
- Tâm của dấu vân tay

	Termination
	Bifurcation
	Lake
	Independent ridge
	Point or island
	Spur
	Crossover

## 2. Dữ liệu sinh trắc dấu vân tay

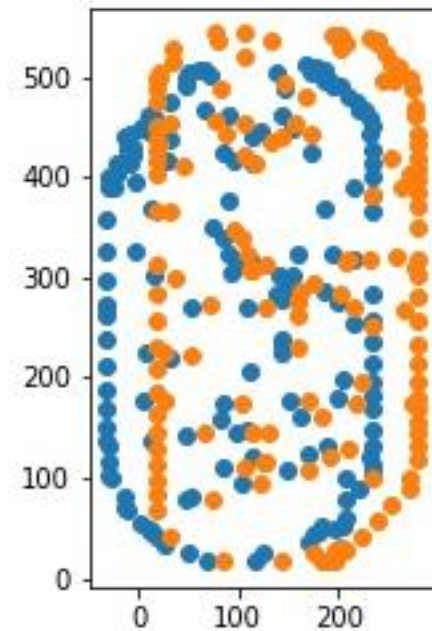
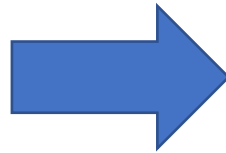
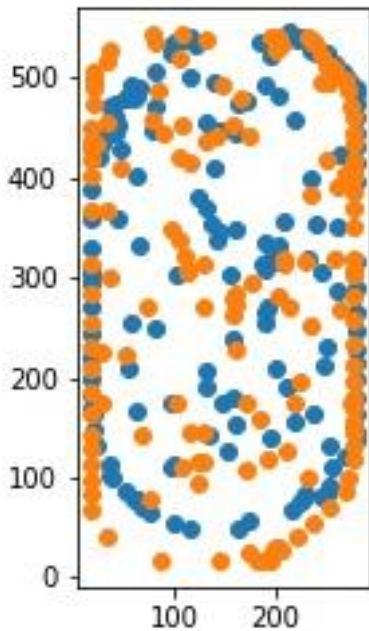
### Các bước trích xuất ra các điểm đặc trưng



## 2. Dữ liệu sinh trắc dấu vân tay

### So khớp hai dấu vân tay

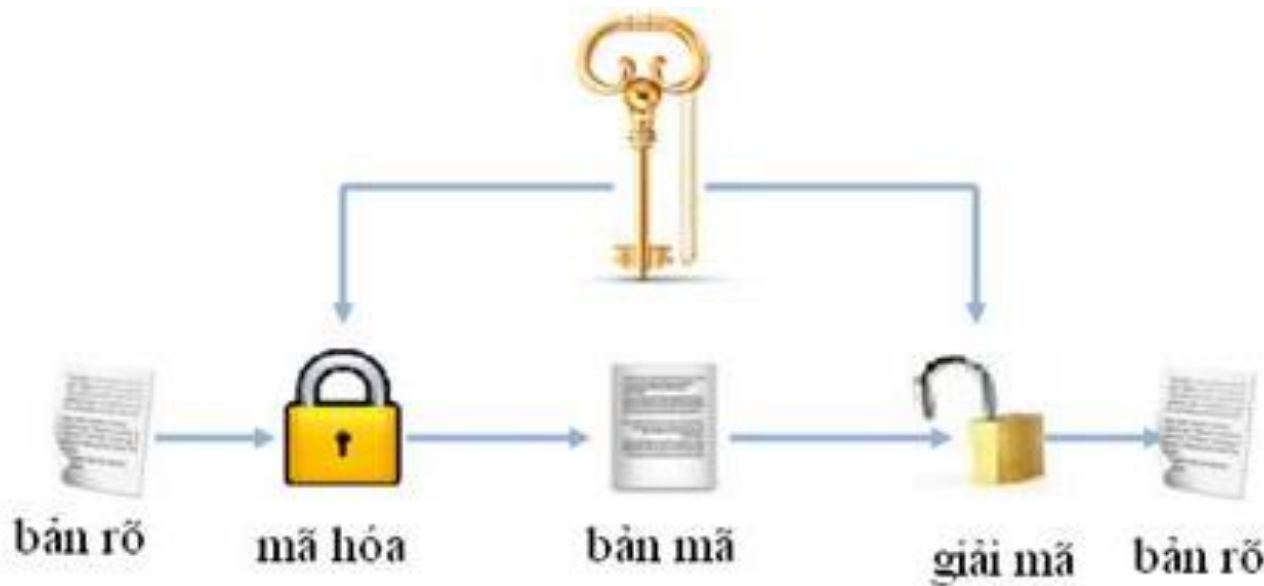
- Tính tiền đám mây điểm đặc trưng về đồng tâm
- Tính tỷ lệ khớp giữa các cặp điểm đặc trưng





### 3. Hệ mật đa trị MAS

**Hệ mật mã:** là các thuật toán biến đổi thông tin để có thể truyền tải an toàn.



### 3. Hệ mật đa trị MAS

Một hệ mật gồm năm thành phần  $(P, C, K, E, D)$

- **P**: tập hữu hạn các chữ cái của bản rõ
- **C**: tập hữu hạn các chữ cái của bản mã
- **K**: tập các khoá

Thoả mãn

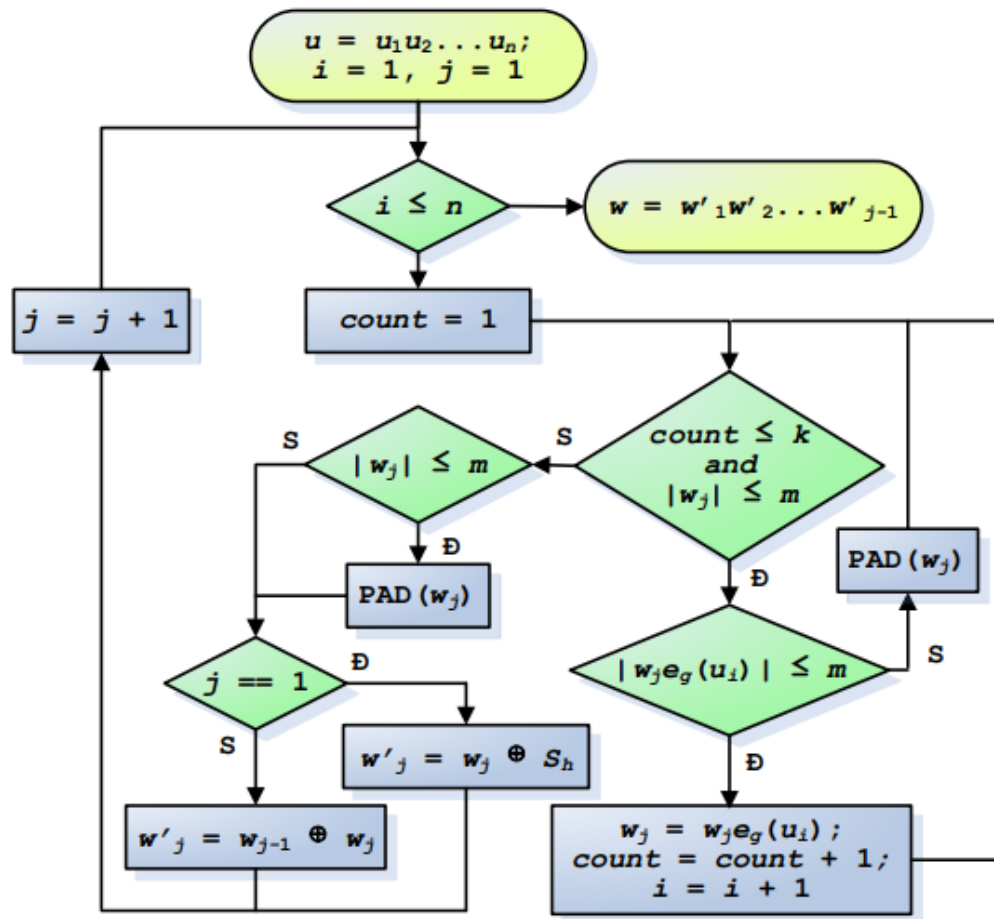
$$e_K: P \rightarrow C$$

$$d_K: C \rightarrow P$$

$$d_K(e_K(x)) = x \quad \forall x \in P$$

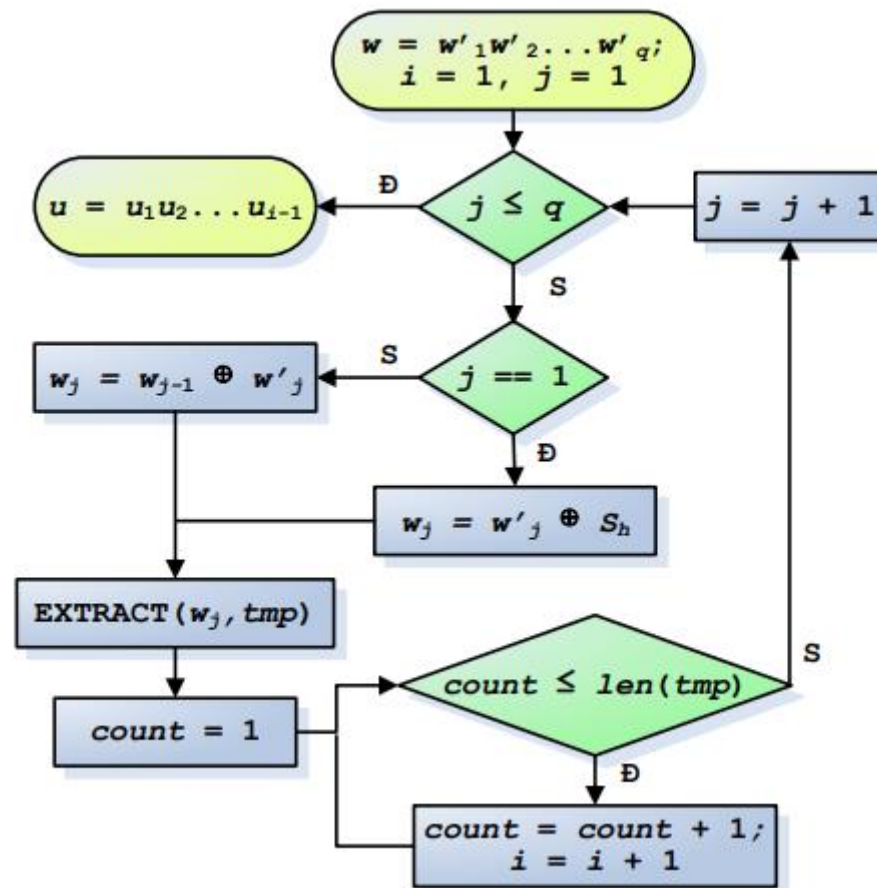
# 3. Hệ mật đa trị MAS

## Hệ mật MAS - Mã hoá



# 3. Hệ mật đa trị MAS

## Hệ mật MAS – Giải mã



## 4. Hệ thống xác thực bằng mật mã và vân tay

### Xây dựng bản rõ

Các đặc trưng của dấu vân tay:

- Điểm tâm:  $(x_0, y_0)$
- Các điểm kết thúc đường vân:  $\{(x_i, y_i) \mid i = 1, \dots, n\}$
- Các điểm rẽ đường vân:  $\{(x'_j, y'_j) \mid j = 1, \dots, m\}$

Bản tin nhắn cần mã hoá là:

$$msg = x_0 y_0 n m x_1 y_1 \dots x_n y_n x'_1 y'_1 \dots x'_m y'_m$$

# 4. Hệ thống xác thực bằng mật mã và vân tay

## Xây dựng hệ mật

- $0 = \{'a'; 'cgh'\}$
- $1 = \{'egm'; 'nmc'\}$
- $2 = \{'ig'; 'fce'\}$
- $3 = \{'jkd'\}$
- $4 = \{'bea'; 'mok'\}$
- $5 = \{'fno'; 'ihc'\}$
- $6 = \{'cei'\}$
- $7 = \{'demc'; 'khm'\}$
- $8 = \{'lbkh'\}$
- $9 = \{'kog'; 'dcef'\}$
- $k = 3$
- padding = 'p'
- Chuỗi **S** sinh từ mã PIN

# 4. Hệ thống xác thực bằng mật mã và vân tay

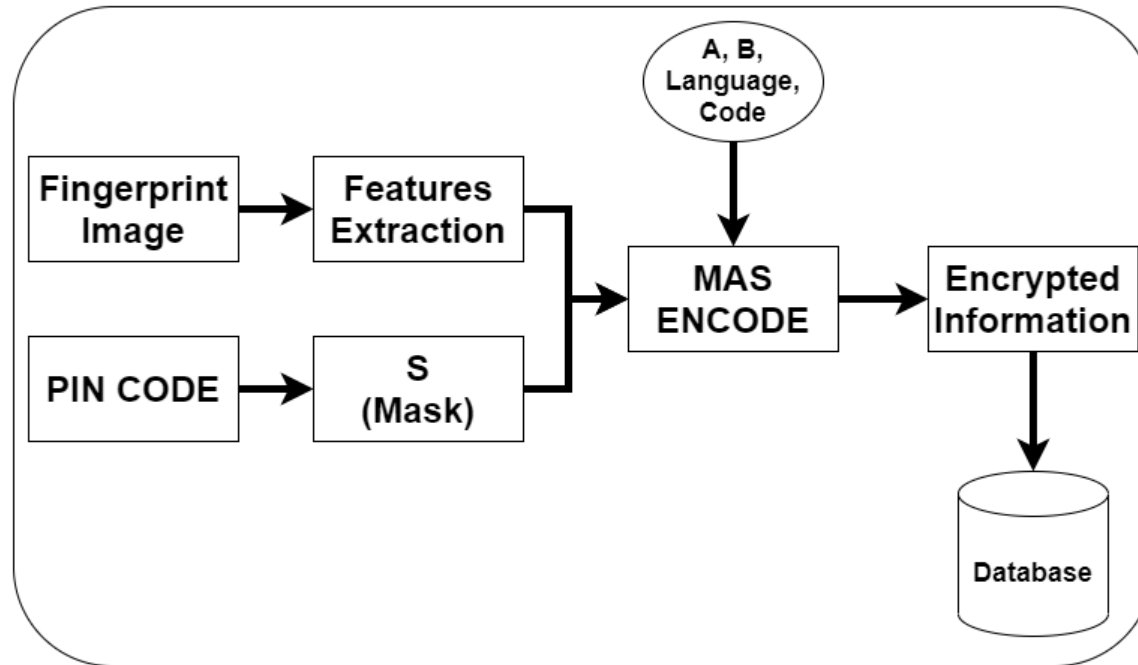
## Xây dựng hệ mật

- 'a': 1000
- 'b': 1110
- 'c': 0011
- 'd': 1111
- 'e': 1101
- 'f': 0010
- 'g': 1100
- 'h': 0101
- 'i': 1011
- 'j': 0000
- 'k': 1001
- 'l': 0111
- 'm': 0100
- 'n': 1010
- 'o': 0001
- 'p': 0110

# 4. Hệ thống xác thực bằng mật mã và vân tay

## Tổng quan hệ thống

### Mã hoá và lưu thông tin về vân tay

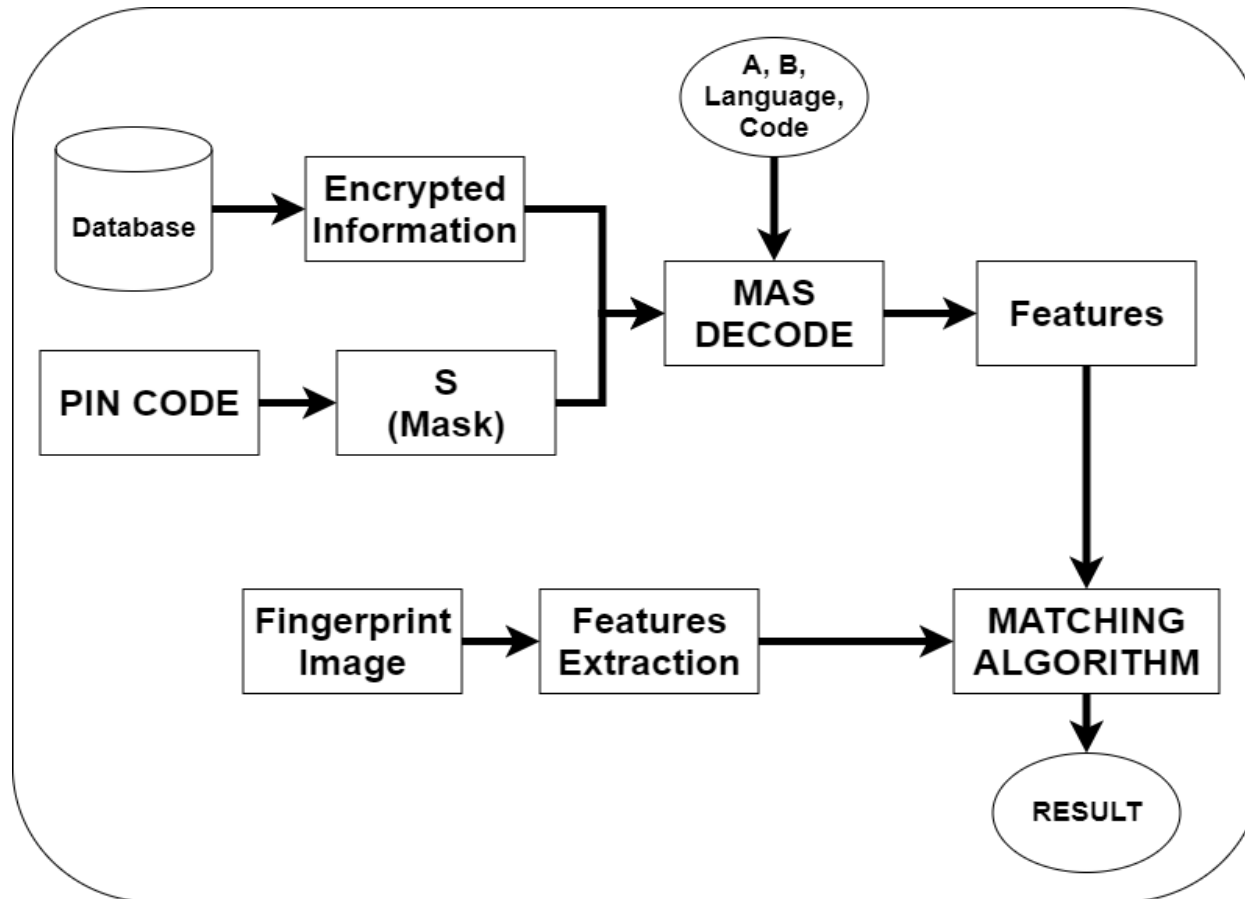




# 4. Hệ thống xác thực bằng mật mã và vân tay

## Tổng quan hệ thống

### Xác thực một dấu vân tay



# Chạy thử hệ thống

A large, stylized graphic on the left side of the slide. It consists of a red background with a circular pattern of white dots of varying sizes, creating a sense of depth and movement. The word "HUST" is written in white, bold, sans-serif capital letters in the center of this graphic.

**HUST**

**THANK YOU !**