Bảo Mật Dữ Liệu Lòng Bàn Tay (Palm)

HIKVISION

WISE SOLUTIONS
WISE.COM.VN

Thiết bị DS-KAB673-P của Hikvision là một mô-đun nhận dạng sinh trắc học hiện đại, sử dụng công nghệ quét lòng bàn tay để tăng cường bảo mật trong các hệ thống kiểm soát ra vào.

Tính năng chính của DS-KAB763-P

- Công nghệ nhận dạng lòng bàn tay kép: Thiết bị sử dụng cả **hoa văn bề mặt bàn tay** và **mạch máu dưới da** để xác thực danh tính. Công nghệ này đảm bảo mức độ bảo mật cao hơn vì các đặc điểm sinh trắc học bên trong cơ thể rất khó làm giả.
- Kết nối USB đơn giản: Thiết bị sử dụng cổng USB 2.0 với công nghệ **Plug-and-Play**, không cần cài đặt trình điều khiển, thuận tiện cho việc triển khai và tích hợp vào hệ thống hiện có.
- Hỗ trợ hệ điều hành Linux: Phù hợp cho các môi trường hệ thống kiểm soát an ninh dựa trên nền tảng Linux.

Ưu điểm của công nghệ quét mạch máu lòng bàn tay

1. Bảo mật vượt trội

- Mạch máu nằm **bên trong cơ thể** nên khó bị làm giả so với dấu vân tay hay nhận dạng khuôn mặt.
- Chỉ khi máu lưu thông trong mạch, hệ thống mới xác thực, chống giả mạo sinh trắc học.

2. Độ chính xác cao

   Xác thực qua mạch máu và hoa văn lòng bàn tay giúp giảm thiểu **tỷ lệ sai sót** (FAR - tỷ lệ chấp nhận sai và FRR - tỷ lệ từ chối sai) so với các công nghệ sinh trắc học khác.

3. Không tiếp xúc và đảm bảo vệ sinh

   Quét **không chạm trực tiếp**, phù hợp cho các môi trường đòi hỏi tiêu chuẩn vệ sinh cao như bệnh viện, nhà máy thực phẩm,...

4. Ít bị ảnh hưởng bởi yếu tố bên ngoài

   Không bị ảnh hưởng bởi các vấn đề **mồ hôi, vết thương, bụi bẩn** như quét vân tay.

5. Bảo vệ quyền riêng tư

Mạch máu dưới da **vô hình với mắt thường**, giảm nguy cơ bị chụp lén hoặc sao chép dữ liệu sinh trắc học.

Ứng dụng trong hệ thống an ninh

- Kiểm soát vào ra, kiểm soát an ninh: Đảm bảo chỉ những người được cấp phép với dữ liệu sinh trắc học hợp lệ mới có thể ra/vào khu vực được bảo vệ.
- Chấm công nhân viên: Giảm thiểu gian lận chấm công nhờ xác thực bằng dữ liệu sinh trắc học.
- Xác thực giao dịch tài chính: Đảm bảo độ an toàn cao trong các giao dịch yêu cầu bảo mật, như xác thực tại ngân hàng hoặc các trung tâm dữ liệu.

Công nghệ quét lòng bàn tay tiên tiến

Thiết bị **DS-KAB673-P** sử dụng công nghệ nhận dạng lòng bàn tay đa chiều, kết hợp:

- Quét cấu trúc tĩnh mạch lòng bàn tay: Áp dụng công nghệ **hồng ngoại gần (Near-Infrared)** để quét mạch máu dưới da, nhận diện qua dòng chảy máu. Cấu trúc mạch máu của mỗi người là **duy nhất** và không thay đổi theo thời gian, đảm bảo độ chính xác cao.
- Quét hoa văn bề mặt lòng bàn tay: Phân tích các đường vân và kết cấu bề mặt lòng bàn tay, tăng thêm một lớp bảo mật.
- Kết hợp dữ liệu sinh trắc học kép: Xác thực sử dụng **đồng thời** cả mạch máu và hoa văn lòng bàn tay, đảm bảo mức độ an ninh gấp đôi so với phương pháp sinh trắc học đơn lẻ.

Tính năng bảo mật vượt trội

- Chống giả mạo sinh trắc học: Công nghệ quét mạch máu lòng bàn tay chống lại việc làm giả do không thể nhìn thấy bằng mắt thường; chỉ nhận diện **mạch máu còn sống** (Blood Flow Detection), ngăn chặn các vật liệu mô phỏng.
- Mã hóa dữ liệu sinh trắc học: Dữ liệu lòng bàn tay được **mã hóa và lưu trữ** dưới dạng **mã hash không thể đảo ngược**, tránh bị sao chép hoặc đánh cắp. Hỗ trợ công nghệ **Save Model Data of Profile Picture Only**, lưu trữ dữ liệu dưới dạng mã hóa mà không hiển thị hình ảnh thực tế, tăng cường bảo mật thông tin cá nhân.
- Chỉ lưu trữ dữ liệu trên thiết bị cục bộ: Dữ liệu sinh trắc học không truyền qua mạng trừ khi có mã hóa nghiêm ngặt, giảm nguy cơ bị tấn công từ xa.

Công nghệ Palm (xác thực lòng bàn tay) bảo mật hơn công nghệ Fingerprint (vân tay)

1. Phương thức xác sinh trắc học phức tạp hơn

- Công nghệ quét vân tay (Fingerprint): dựa trên hoa văn đường vân bề mặt ngón tay. Có thể bị làm giả bằng cách sử dụng dấu vân tay được in 3D hoặc chất liệu silicon, đặc biệt nếu bảo mật không đạt chuẩn cao.
- Công nghệ quét lòng bàn tay (Palm): dựa trên 2 lớp dữ liệu sinh trắc học hoa văn bề mặt lòng bàn tay, **cấu trúc tĩnh mạch dưới da** (Palm Vein Recognition) – quét bằng hồng ngoại gần (NIR). Cấu trúc mạch máu là **duy nhất** và chỉ nhận diện khi có **dòng máu đang lưu thông**, nên gần như không thể làm giả.
  Ưu điểm: **Ưu điểm:** Công nghệ lòng bàn tay quét cả **tĩnh mạch dưới da**, bảo mật vượt trội so với chỉ quét bề mặt như vân tay.

2. Khả năng chống giả mạo sinh trắc học

- Vân tay: Có thể bị làm giả bằng vật liệu như gelatin, silicon, in 3D. Dễ bị đánh cắp dấu vân tay từ các bề mặt đã tiếp xúc (cốc, tay nắm cửa...).
- Lòng bàn tay: Không thể sao chép vì tĩnh mạch không để lại dấu vết trên bề mặt tiếp xúc. Yêu cầu **mạch máu còn sống** (blood flow detection).
  Ưu điểm: Xác thực lòng bàn tay có khả năng chống làm giả vượt trội.

3. Độ bền và phù hợp với môi trường

- Vân tay: có thể bị ảnh hưởng do tay ướt, dính dầu, bụi bẩn, tổn thương da (sẹo, trầy xước).
- Lòng bàn tay: không cần tiếp xúc, không ảnh hưởng bởi mồ hôi, bụi bẩn. Phù hợp môi trường yêu cầu vệ sinh cao như y tế, thực phẩm, phòng sạch.
  Ưu điểm: Palm Vein bền bỉ hơn trong các môi trường hoạt động.

Mã hóa mẫu Palm (lòng bàn tay) trên hệ thống, phần mềm, thiết bị

Khi phần mềm thu thập mẫu vân tay hoặc lòng bàn tay, thay vì lưu trữ trực tiếp dưới dạng hình ảnh sinh trắc học, dữ liệu sẽ được xử lý và lưu trữ dưới dạng một chuỗi hash (hoặc bit) mã hóa. Đây là một tiêu chuẩn bảo mật quan trọng trong các hệ thống sinh trắc học và thường được thực hiện như sau:

1. Trích xuất đặc trưng (Feature Extraction)

Hệ thống chỉ trích xuất các đặc điểm sinh trắc học chính (như vị trí, góc và khoảng cách giữa các điểm đặc trưng trên lòng bàn tay).

2. Mã hóa thành chuỗi hash
   Các đặc trưng này sẽ được mã hóa thành một chuỗi hash hoặc dữ liệu nhị phân duy nhất (bit string). Chuỗi này là kết quả của các thuật toán băm một chiều (one-way hashing) như SHA-256 hoặc các thuật toán riêng biệt của nhà sản xuất.

3. Không thể khôi phục ảnh gốc
   Do tính chất của hàm băm một chiều, chuỗi hash này không thể đảo ngược để khôi phục lại hình ảnh vân tay/lòng bàn tay ban đầu, giúp giảm thiểu nguy cơ rò rỉ dữ liệu sinh trắc học.

4. So sánh hash, không phải ảnh gốc
   Khi xác thực, thiết bị sẽ trích xuất đặc trưng từ mẫu sinh trắc học mới, tạo một hash mới và so sánh với hash đã lưu trong cơ sở dữ liệu của thiết bị.

5. Kết luận
   Giảm nguy cơ lộ dữ liệu sinh trắc học: Không lưu trữ hình ảnh thô.
   Khó bị giả mạo: Chuỗi hash không thể đảo ngược thành ảnh gốc.
   Đáp ứng tiêu chuẩn bảo mật: Phù hợp với GDPR và các quy định bảo mật quốc tế.