

Curso de Tecnologia em Redes de Computadores
Disciplina: Tópicos Avançados II – 5º período
Professor: José Maurício S. Pinheiro

AULA 7: Sistemas Biométricos

1. Sistema Biométrico Típico

Qualquer que seja a característica biométrica utilizada, ela deve estar enquadrada em um sistema biométrico. Um sistema biométrico pode ser encarado como o conjunto de *hardware* e *software* para o reconhecimento de padrões de propósito específico, que opera através da aquisição automática de uma coleção de informações biométricas do indivíduo, extraindo um modelo a partir dessas informações e comparando esse modelo com um conjunto de outros modelos armazenados em uma base de dados.

Um modelo conceitual simples considera os dados e processos básicos comuns a qualquer sistema biométrico (Fig. 1), onde o usuário é previamente registrado (aquisição) e seu perfil biométrico (exemplar) fica armazenado. Quando da utilização posterior do sistema, o processo de extração obtém da característica biométrica apresentada os atributos necessários para análise e o modelo biométrico extraído (perfil) é comparado com os modelos armazenados na base de dados. O processo de comparação decide se os dados apresentados são suficientemente similares (limiar) ao perfil registrado, permitindo (ou não) a autenticação do usuário no sistema.



Figura 1 – Modelo conceitual simples de um sistema biométrico

1.1. Aquisição e Exemplar

O processo de aquisição ou apresentação é o processo de obtenção dos dados da característica biométrica apresentada ao sistema. Os dispositivos de aquisição das características biométricas obtêm os dados através de sensores especiais e utilizam um software que converte cada informação em um modelo digital que será armazenado no Banco de Dados (Database) do sistema para posterior comparação.

Normalmente, a dificuldade deste processo é balancear adequadamente a qualidade da amostra sem causar incômodo para o indivíduo. Neste módulo normalmente é adicionado um controle da qualidade da amostra adquirida conhecido como pré-processamento. O exemplar (ou amostra) é o resultado do processo de aquisição.

1.2. Atributos e Extração de Características

O processo de extração produz uma representação digital do exemplar obtido, chamado de atributo, característica ou *template*. Um *template* é associado com um identificador do usuário. Eles podem ser armazenados em cartões de memória, cartões magnéticos ou em uma base de dados central. O tipo de armazenamento dar-se-á pela aplicabilidade prática a que se destina o sistema e pelo tamanho dos *templates* gerados.

A extração de características é a redução do conjunto de medidas biométricas tomadas do indivíduo e formado por um grande volume de dados que contém uma pequena quantidade de informação útil, para um volume menor de dados, mas praticamente com a mesma quantidade de informação.

1.3. Registro e Perfil

O processo de registro, cadastramento ou *enrollment*, obtém previamente os dados biométricos do indivíduo para cadastramento no sistema. O perfil biométrico obtido (*template*) é armazenado para uma comparação posterior. O processo de registro, embora realizado uma única vez para cada indivíduo, é necessário para o estabelecimento do perfil e para comparações posteriores.

1.4. Comparação, Limiar e Decisão

O processo de comparação ou *matching* é responsável por verificar qual é o grau de similaridade entre as características extraídas da amostra do indivíduo com o perfil armazenado previamente. Este processo fornece uma pontuação (score) representativa da similaridade entre os dois conjuntos de dados. Caso a similaridade seja superior a certo limite previamente determinado, conhecido como limiar, ou *threshold*, a decisão é aceitar o indivíduo, ou seja, uma autenticação válida. Caso a similaridade seja inferior ao limiar, a decisão é não aceitar o indivíduo, ou seja, ele não é autenticado no sistema e o seu acesso, negado.

2. Requisitos do Sistema Biométrico

Como os sistemas biométricos se baseiam em características intrínsecas do ser humano, podem ser empregados como métodos de autenticação rápida e com alto nível de precisão. Têm como uma de suas principais vantagens o fato de serem intransferíveis, não podendo ser perdidos e nem roubados.

Para que um sistema de identificação biométrico seja considerado seguro, é necessário que atenda a três requisitos básicos:

- A característica biométrica deve conter diferenças significativas entre indivíduos distintos;
- As características devem ser estáveis durante o período de vida do indivíduo;
- O sistema deve ser robusto e oferecer segurança contra tentativas de fraudes.

Em teoria, qualquer característica humana, seja ela física ou comportamental pode ser usada na identificação biométrica, desde que satisfaça os seguintes requerimentos:

- **Universalidade** – todos os indivíduos devem possuir a característica a ser utilizada como medida;
- **Singularidade** – indica que a medida da característica utilizada não deve ser igual em pessoas diferentes, ou no mínimo, que a probabilidade de haver duas pessoas com a mesma medida dessa característica seja muito pequena;
- **Permanência** – cada característica não deve variar com o tempo, por exemplo, alterar-se devido ao envelhecimento;
- **Mensurabilidade** – pode ser medida quantitativamente, tendo por base um modelo da característica selecionada;

Além destas, há outras três características importantes no que se refere ao funcionamento de um sistema de reconhecimento biométrico, que são:

- **Precisão e Desempenho:** refere-se à precisão com que se realiza a identificação, aos recursos necessários para atingir uma medição de precisão aceitável e ao trabalho ou fatores ambientais que afetam a precisão na identificação. Normalmente, maior precisão dos resultados implica em um menor desempenho do sistema;
- **Aceitabilidade:** esta característica indica o nível de aceitação do sistema de reconhecimento biométrico por parte de seus usuários;
- **Proteção:** consiste na facilidade ou dificuldade de usuários conseguirem burlar o sistema, através da utilização de técnicas fraudulentas.

Deve-se observar que, antes que um sistema biométrico possa ser utilizado, todos os usuários devem ser registrados. O registro envolve o indivíduo, que fornece uma amostra de sua característica biométrica que será usada pelo sistema para gerar um modelo biométrico e o próprio sistema biométrico.

O processo inicial compreende o reconhecimento do ambiente e das características biométricas selecionadas. Para isto, a característica selecionada é obtida por sensores especiais, usando um software de processamento de imagens ou outra tecnologia para gerar um modelo biométrico. Geralmente os sistemas biométricos obtêm as informações através de equipamentos dotados de sensores ópticos, térmicos, indutivos, ultra-sônicos ou acústicos, como é o caso dos equipamentos orientados para o reconhecimento de voz.

O modelo é então armazenado no sistema biométrico (um banco de dados, por exemplo), para ser utilizado em um ciclo de comparação posterior. Quando o acesso da aplicação é requerido, a característica biométrica é novamente capturada e outro modelo é gerado e comparado com o modelo biométrico armazenado. A aplicação será desbloqueada se o resultado da comparação for positivo.

2.1. Modelo Biométrico Básico

Como mencionado, em um sistema biométrico, uma característica individual precisa ser registrada e a sua gravação é chamada de registro (*enrollment*). Este registro está baseado na criação de um modelo (*template*), que é a representação digital de uma característica física. O modelo normalmente é um extenso conjunto de caracteres alfanuméricos baseado em algum tipo de algoritmo biométrico que descreve as características físicas de um indivíduo.

Um algoritmo é uma seqüência limitada de instruções ou passos que um sistema computacional utiliza para resolver um problema específico. Na biometria são utilizados diferentes tipos de algoritmos, para processamento de imagens, geração de

modelo, para comparação, entre outros, com o objetivo de atender aos diferentes tipos de sistemas. Assim, o algoritmo biométrico pode ser visto como o tradutor da característica física em uma representação digital na forma de um modelo.

O algoritmo também permite comparar o modelo registrado em um Banco de Dados Biométrico com o modelo de um indivíduo que deseja se autenticar no sistema, chamado de "modelo vivo". Quando os modelos são comparados, o sistema calcula a semelhança entre eles. Se a comparação for positiva (dentro de certa tolerância ou limiar), o indivíduo será autenticado, caso contrário, seu registro será negado.

Podem-se distinguir três macro-processos no sistema biométrico básico: obtenção do modelo biométrico, processamento e comparação. A captura do tipo biométrico envolve a camada que interage com os dispositivos físicos de leitura (sensores), garantindo a qualidade da captura da característica biométrica e convertendo essa característica em dados digitais. O processamento é responsável pela geração do modelo biométrico, a partir dos dados digitais gerados na etapa de captura. No processo de comparação temos os algoritmos que comparam os *templates* obtidos nas etapas anteriores com outros, armazenados na base de dados do sistema, para determinar o grau de semelhança entre eles.

Esses macro-processos são formados por um subconjunto de rotinas, estruturas de dados, objetos, etc., que são combinados e interagem com os sistemas operacionais e rotinas de baixo nível para realizar funções específicas, como a análise qualitativa das imagens, classificação datiloscópica, geração de modelos biométricos com auxílio de algoritmos, criptografia de dados, entre outras (Fig 2). Trata-se de uma API (*Application Programming Interface*) de múltiplos níveis, que encapsula os processos inerentes ao uso do sistema biométrico, englobando dois métodos principais: um método que ocorre de modo automático e atua na camada de relação com o *hardware* de leitura e funções básicas do sistema operacional. O outro método consiste em eventos que, acionados pelo aplicativo, irão atender os requisitos para o uso adequado do sistema biométrico correspondente.

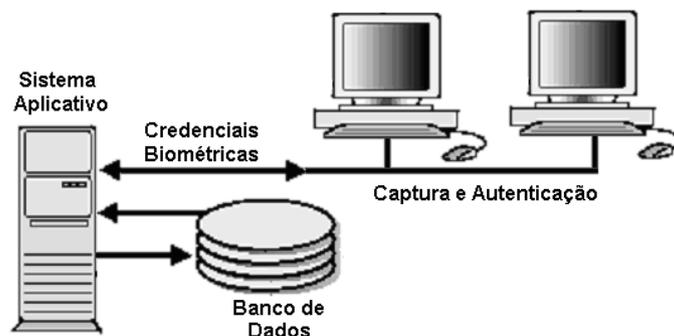


Figura 2 – Uma API encapsula as credenciais biométricas no sistema aplicativo