Capítulo 3

Introdução à Biometria

Luciano R. Costa, Rafael R. Obelheiro e Joni S. Fraga
Departamento de Automação e Sistemas
Universidade Federal de Santa Catarina
Email: {luciano, rro, fraga}@das.ufsc.br

Abstract

Biometric authentication, based on intrinsic personal traits, has long been an object of interest to the computer security community. However, until some time ago its adoption was restricted to highly secure environments and criminal identification applications. With the recent technological improvements and reduction in device costs, biometrics has become more disseminated, being frequently touted as a promising solution for authentication problemas. This chapter provides an overview of biometric authentication, examining the most used technologies and discussing its benefits and limitations. We also address architectural aspects of biometric systems, as well as open problems that require further research.

Resumo

A autenticação biométrica, baseada em características pessoais intrínsecas, há muito tem sido objeto do interesse da comunidade de segurança computacional. Entretanto, até pouco tempo atrás a sua adoção se restringia a ambientes de alta segurança e aplicações de identificação criminal, por razões de natureza econômica e tecnológica. Com o aperfeiçoamento da tecnologia e a redução no custo dos dispositivos verificados recentemente, a biometria vem se popularizando, sendo freqüentemente apontada como uma solução promissora para problemas de autenticação. Este capítulo apresenta uma visão geral da autenticação biométrica, examinando as principais tecnologias utilizadas e discutindo seus benefícios e limitações. São considerados ainda aspectos arquiteturais de sistemas biométricos, bem como problemas em aberto que precisam ser melhor pesquisados.

3.1. Introdução

O conceito de segurança em um sistema computacional está relacionado à manutenção de três propriedades fundamentais: a *confidencialidade*, que garante que a informação somente seja revelada com autorização apropriada; a *integridade*, que garante que a informação somente seja alterada com autorização apropriada; e, a *disponibilidade*, que garante que a informação seja acessível aos legítimos usuários, quando requerida. Tem se tornado comum acrescentar duas outras propriedades, a *autenticação*, que garante que cada entidade seja aquela que alega ser, e o *não-repúdio*, que garante que uma terceira parte neutra possa ser convencida de que uma transação ou evento em particular ocorreu, ou não ocorreu [Landwehr 2001]. A autenticação possui importância fundamental, pois em geral a autorização é concedida ou negada com base na identidade associada à entidade que solicita acesso ao recurso ou em algum atributo que depende dessa identidade.

Uma credencial é uma evidência fornecida por uma entidade, ao requisitar acesso a um recurso. O protocolo de autenticação decide se as credenciais apresentadas constituem prova suficiente de identidade para autorização da entidade a acessar recursos. As credenciais apresentadas podem ser de três tipos [Miller 1994]:

- **Posse** - Qualquer detentor da posse de um objeto é capaz de utilizar o recurso. Por exemplo, o possuidor da chave do carro possui o privilégio de utilizá-lo.
- **Conhecimento** - Indivíduos possuidores de certo conhecimento são elegíveis para utilizar um recurso. Neste caso, a autenticação é baseada em um conhecimento secreto,[1] compartilhado entre o usuário e a aplicação.
- **Biometria** - Os traços das pessoas podem ser medidos e computados na forma de um identificador biométrico único, difícil de compartilhar, roubar, forjar e de ser alterado.

O objetivo deste capítulo consiste em apresentar uma visão geral sobre os sistemas biométricos e seus principais aspectos de segurança. Desta maneira, a seção 3.2 apresenta os principais conceitos envolvendo sistemas biométricos: modos de autenticação usando biometria, requisitos de características biométricas, tecnologias biométricas existentes, aplicações de biometria, modelo conceitual de sistemas biométricos, erros, critérios de seleção de tecnologias biométricas e padrões em biometria.

Dentre as diversas tecnologias biométricas enumeradas na primeira seção, existem algumas — impressões digitais, íris, faces, formato das mãos e assinaturas — que se encontram em um estágio de desenvolvimento bastante satisfatório. Essas tecnologias estão amadurecidas, estando disponíveis comercialmente em implementações de boa qualidade a um custo razoável. Em vista disso, a seção 3.3 examina mais detidamente cada uma dessas tecnologias, detalhando o seu modo de funcionamento e analisando quais os seus

[1] Entretanto, podemos distinguir conhecimento com vários graus de *segredo*. Um ID de usuário de computador ou um número de conta bancária são freqüentemente solicitados para autenticação, embora tal conhecimento não seja segredo. Mesmo assim, não são universalmente conhecidos, o que ajuda a prevenir ataques de impostação superficiais. De fato, podemos distinguir uma faixa de segredo que vai do universalmente conhecido ao segredo completo.

principais benefícios e desvantagens. São apresentados ainda os recursos existentes para pesquisa, como bancos de dados e ferramentas.

Embora essencialmente todos os sistemas biométricos se encaixem em um mesmo modelo conceitual, a implementação desse modelo pode diferir de um sistema para o outro. A seção 3.4 apresenta as arquiteturas de armazenamento e segurança de sistemas biométricos. A arquitetura de armazenamento considera as formas com que os vários processos que compõem o modelo conceitual são distribuídos no sistema, e onde são armazenados os diferentes dados biométricos usados no modelo. A arquitetura de segurança discute as vantagens dos sistemas biométricos do ponto de vista de segurança e suas vulnerabilidades específicas (notadamente a facilidade de obtenção de características biométricas sem o consentimento do usuário e a irrevogabilidade dessas características), bem como contramedidas que podem ser usadas para contornar ou minimizar essas vulnerabilidades (multibiometria, biometria cancelável e autenticação multifatores).

Finalmente, a seção 3.5 discute os principais problemas abertos na área de biometria, e a seção 3.6 apresenta as conclusões do capítulo e algumas considerações finais.

3.2. Conceitos

3.2.1. Verificação e identificação

Os sistemas biométricos são usados para a **autenticação de pessoas**. Nestes sistemas, existem dois modos de autenticação: a verificação e a identificação [Bolle et al. 2004, p. 25]. Na **verificação**, a característica biométrica é apresentada pelo usuário juntamente com uma identidade alegada, usualmente por meio da digitação de um código de identificação. Esta abordagem de autenticação é dita uma busca 1:1, ou busca fechada, em um banco de dados de perfis biométricos. O princípio da verificação está fundamentado na resposta à questão: "O usuário é quem alega ser?". Na **identificação**, o usuário fornece apenas sua característica biométrica, competindo ao sistema "identificar o usuário". Esta abordagem de autenticação é dita uma busca 1:N, ou busca aberta, em um banco de dados de perfis biométricos. O sistema busca todos os registros do banco de dados e retorna uma lista de registros com características suficientemente similares à característica biométrica apresentada. A lista retornada pode ser refinada posteriormente por comparação adicional, biometria adicional ou intervenção humana. Basicamente, a identificação corresponde a responder à questão: "Quem é o usuário?".

A identificação também é utilizada em aplicações conhecidas como aplicações de varredura (*screening*), que somente podem ser executadas com alguma forma de biometria. Estas são aplicações de busca com política negativa, pois procuram estabelecer se um indivíduo está em alguma lista de pessoas de interesse, como a lista dos mais procurados, ou um banco de dados de algum tipo de benefício. O propósito de uma varredura é prevenir o uso de múltiplas identidades. Por exemplo, se A já recebe algum benefício e agora alega ser B e gostaria de receber de novo o benefício, o sistema pode estabelecer que B já está no banco de dados.

3.2.2. Tecnologias Utilizadas

Qualquer característica fisiológica ou comportamental humana pode ser usada como característica biométrica desde que ela satisfaça alguns requisitos básicos [Clarke 1994]:

- **Universalidade**: toda a população (a ser autenticada) deve possuir a característica. Na prática, temos pessoas que não possuem impressões digitais, por exemplo.
- **Unicidade**: uma característica biométrica deve ser única para cada indivíduo, ou seja, a possibilidade de pessoas distintas possuirem características idênticas, deve ser nula ou desprezível. Assim, a altura de uma pessoa não é uma boa característica para autenticação, já que várias pessoas podem possuir a mesma altura. Na prática, as características biométricas podem apresentar maior ou menor grau de unicidade, mas nenhuma delas pode ser considerada absolutamente única para cada indivíduo.[2]
- **Permanência**: a característica deve ser imutável. Na prática, existem alterações ocasionadas pelo envelhecimento, pela mudança das condições de saúde ou mesmo emocionais das pessoas e por mudanças nas condições do ambiente de coleta.
- **Coleta**: a característica tem que ser passível de mensuração por meio de um dispositivo. Na prática, todos as características biométricas utilizadas comercialmente atendem a este requisito.
- **Aceitação**: a coleta da característica deve ser tolerada pelo indivíduo em questão. Na prática, existem preocupações com higiene, com privacidade e questões culturais que diminuem a aceitação da coleta.

Na prática, porém, nenhuma característica biométrica consegue atender com perfeição aos requisitos de uma característica biométrica ideal.

Ao longo do tempo, diversas tecnologias biométricas foram desenvolvidas. As tecnologias biométricas existentes são classificadas, por conveniência, em dois grupos (figura 3.1). O primeiro grupo está baseado em características chamadas de **fisiológicas** ou **estáticas**. Essas características são traços fisiológicos, originários da carga genética do indivíduo, e essencialmente variam pouco (ou nada) ao longo do tempo. As principais características estáticas são a aparência facial, o padrão da íris, a geometria das mãos e as impressões digitais, que serão apresentadas com maior detalhamento na seção 3.3.

Outras características estáticas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa, como a impressão palmar [Zhang and Shu 1999, Lu et al. 2003], o DNA [Bolle et al. 2004, p. 52], o formato das orelhas [Burge and Burger 2000, Victor et al. 2002], o padrão vascular da retina [Hill 1999], o odor do corpo [Korotkaya 2003], o padrão da arcada dentária [Chen and Jain 2005] e o padrão de calor do corpo ou de partes dele [Prokoski and Riedel 1999].

[2] A quantidade de variação devida à genética e ao ambiente muda de biometria para biometria. Cada pessoa é única, se analisada com suficiente detalhe. É próximo do impossível que duas pessoas diferentes tenham a mesma, idêntica, representação biométrica em qualquer sistema razoável. Contudo, ao lidar com tecnologias práticas de autenticação, encontramos limites na resolução das imagens extraídas, na capacidade de armazenamento e na habilidade de comparação entre dados extraídos. Na prática, isto extermina a noção de unicidade absoluta para todas as características biométricas.

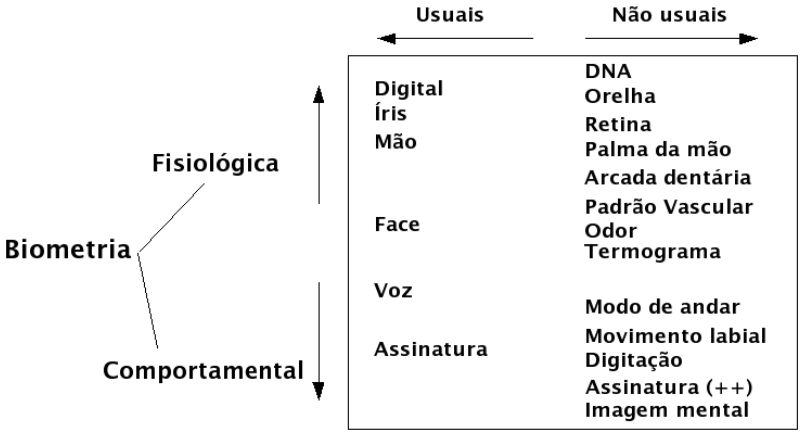

Figura 3.1. As seis características biométricas mais comuns e outras, que são usadas com menor frequência ou que estão em estágios iniciais de pesquisa. As características fisiológicas (estáticas) dependem principalmente da carga genética e as comportamentais (ou dinâmicas) dependem ainda fortemente do aprendizado e da experiência.

O segundo grupo de tecnologias biométricas está baseado em características chamadas de **comportamentais** ou **dinâmicas**. São características aprendidas ou desenvolvidas ao longo da utilização constante, e que podem variar fortemente ao longo do tempo. Além disso, podem ser facilmente alteradas pela vontade ou estado do usuário. Assim, até mesmo duas amostras consecutivas podem mudar bastante. As principais características dinâmicas utilizadas são o padrão de voz e a dinâmica da assinatura, que também serão detalhadas na seção 3.3.

Outras características dinâmicas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa, como dinâmica de digitação (*keystroke dynamics*) [Bergadano et al. 2002], modo de andar [Phillips et al. 2002], movimento labial [BioID 2005] [Valid 2005], som da assinatura[3], vídeo da assinatura [Fink et al. 2001] e imagens mentais (*pass-thoughts*) [Thorpe et al. 2005].

3.2.3. Aplicações

As tecnologias biométricas podem ser utilizadas em uma ampla variedade de aplicações, para proporcionar (1) controle de acesso físico e lógico e (2) fornecimento de unicidade. Existe uma taxonomia genérica de aplicações, segundo a qual todas aplicações podem ser particionadas em sete categorias, pelo menos [Wayman 1999b]. De uma maneira prática, as aplicações dos nichos Governamental, Comercial e Forense (classificação vertical) podem ser classificadas por finalidade (classificação horizontal). Dentre os diversos conjuntos possíveis, dependendo do refinamento, um exemplo é a classificação de alto nível de sete grupos usada no relatório BITE Market Report [BITE 2005], mostrada na tabela 3.1.

[3]Informações sobre a pesquisa fornecidas pelo prof. Lee Luan Ling (FEEC/UNICAMP) e notícia publicada em `http://www.unicamp.br/unicamp/unicamp_hoje/ju/setembro2003/ju229pg8b.html`.

Finalidade	Utilização
Identificação Criminal	28 %
Controle de acesso e atendimento	22 %
Identificação Civil	21 %
Segurança de redes e de computadores	19 %
Autenticação em pontos de vendas, ATM's e varejo	4 %
Autenticação telefônica e comércio eletrônico	3 %
Vigilância e filtragem	3 %

Tabela 3.1. Distribuição horizontal (por finalidade) das principais aplicações biométricas [BITE 2005]

3.2.4. Sistema biométrico típico

Seja qual for a característica biométrica utilizada, ela deve estar enquadrada em um **sistema biométrico**. Um sistema biométrico pode ser encarado como um sistema de reconhecimento de padrões de propósito específico [Bolle et al. 2002]. O modelo conceitual simples de sistema biométrico, apresentado na figura 3.2, leva em consideração os dados e processos básicos comuns a qualquer sistema biométrico. Num sistema biométrico, o usuário é previamente registrado e seu perfil biométrico fica armazenado. Quando da utilização posterior do sistema, o processo de aquisição obtém os dados biométricos apresentados. Características particulares dos dados são extraídas para comparação com o perfil armazenado. O processo de comparação decide se os dados apresentados são suficientemente similares ao perfil registrado.

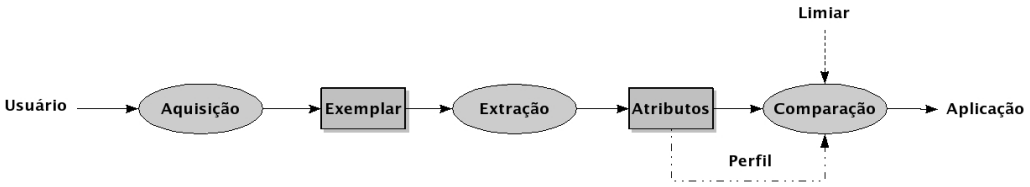

Figura 3.2. Um modelo simples de sistemas biométricos

- *Aquisição e exemplar* - O processo de aquisição ou apresentação é o processo de obtenção dos dados da característica biométrica oferecida. Normalmente a dificuldade deste processo é balancear adequadamente a qualidade da amostra sem causar excesso de inconveniência para o usuário. Neste módulo é geralmente embutido um controle da qualidade da amostra adquirida (viabilidade de processamento). O exemplar ou amostra (*sample*) é o resultado do processo de aquisição.

- *Extração e atributos* - O processo de extração produz uma representação computacional do exemplar obtido, que chamaremos de atributos, ou características extraídas (*features* ou *trial template*). A extração de características é a redução de um conjunto de medidas formado por uma grande quantidade de dados que contêm uma pequena quantidade de informação útil para um conjunto que contém menos dados mas praticamente a mesma quantidade de informação [Patrick 1972].

- *Registro e perfil* - O processo de registro, ou *enrollment*, obtém previamente os dados biométricos do usuário para cadastramento no sistema. O perfil biométrico obtido, ou *template*, é armazenado para uma comparação posterior. A linha pontilhada na figura 3.2 significa que o processo de registro, embora realizado raramente, é necessário para o estabelecimento do perfil para posterior comparação.

- *Comparação, limiar e decisão* - O processo de comparação, ou *matching*, verifica qual é o grau de similaridade entre as características extraídas da amostra do usuário e o perfil armazenado previamente. Este processo fornece um escore representativo da similaridade entre os dois conjuntos de dados. Caso a similaridade seja superior a um certo limite previamente determinado, conhecido como limiar, ou *threshold*, a decisão é aceitar o usuário, ou seja, uma autenticação válida. Caso a similaridade seja inferior ao limiar, a decisão é não aceitar o usuário, e então temos um usuário não autenticado.

3.2.5. Erros

De uma maneira geral, a comunidade biométrica diferencia vários tipos de erros, conforme a localização lógica de sua ocorrência. As diferentes aplicações biométricas podem ter diferentes definições dos erros associados. Consequentemente, há muita terminologia para expressar a precisão de uma aplicação [Bolle et al. 2004, p. 65]. O que é bastante claro e aceito por toda a comunidade biométrica é que qualquer sistema biométrico cometerá erros e que o verdadeiro valor associado às diversas taxas de erro não pode ser estabelecido teoricamente, por cálculo, mas somente por estimativas estatísticas dos erros, que são expressos em taxas e percentagens.

Há dois tipos de erros nos quais o comparador pode incorrer [Wayman 1997, Wayman 1999a].

- *False Match* (FM) - Erro do tipo I - Decidir que os exemplares são similares, enquanto na realidade eles pertencem a diferentes indivíduos. A freqüência com a qual este erro ocorre é chamada *False Match Rate* (FMR).

- *False Non-Match* (FNM) - Erro do tipo II - Decidir que dois exemplares não são do mesmo indivíduo enquanto na realidade eles pertencem ao mesmo indivíduo. A freqüência com a qual este erro ocorre é chamada *False Non-Match Rate* (FNMR).

A terminologia FM e FNM é aplicada geralmente a algoritmos de comparação ou módulos comparadores. Na prática, para os sistemas biométricos considerados como um todo, é utilizada a terminologia convencional de reconhecimento de padrões FA (*False Accept*) e FR (*False Reject*).

- *False Accept* (FA) - Erro do tipo I - Decidir que uma identidade alegada é legítima quando na realidade ela é falsa. A freqüência de ocorrências de erros deste tipo é chamada *False Accept Rate* (FAR).

- *False Reject* (FR) - Erro do tipo II - Decidir que uma identidade alegada é falsa quando na realidade ela é legítima. A freqüência de ocorrências de erros deste tipo é chamada *False Reject Rate* (FRR).

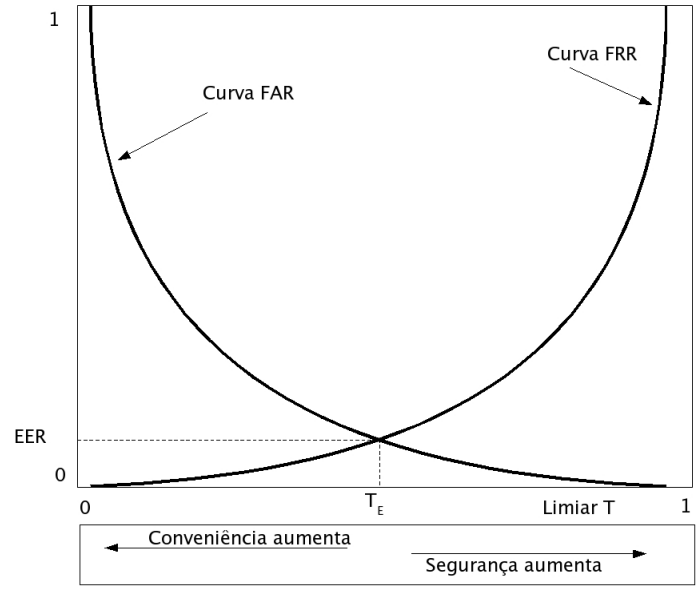

Figura 3.3. As curvas típicas das taxas de erro FAR e FRR, plotadas uma ao lado da outra, em relação ao limiar T configurado para o sistema. As curvas se cruzam num ponto notável de operação EER$(T_E) \rightarrow$ (FAR$(T_E) =$ FRR(T_E)). O sistema pode operar nas faixas de "conveniência" ou de "segurança", conforme a calibração do limiar.

Devido à possibilidade de calibrar o sistema por meio do ajuste do limiar, as taxas de erros possuem conseqüências opostas. FA resulta em brechas na segurança, com a admissão de usuários não autorizados. Por outro lado, FR resulta em problemas de conveniência, já que usuários genuínos terão acesso negado até uma verificação posterior. As taxas de erro FAR e FRR podem ser plotadas *uma ao lado da outra*, como apresentado na figura 3.3. Para avaliar de forma sumária a qualidade das curvas FAR e FRR e, por conseqüência, a precisão de operação de um dado sistema, é possível a explicitação de um ponto notável, onde as taxas são iguais, ou seja, o limiar $T = T_E$ para o qual FAR$(T) =$ FRR(T). Este ponto é conhecido como ponto de operação EE (*Equal Error*), ao qual também está associado uma taxa EER (*Equal Error Rate*).

As taxas FAR(T) e FRR(T) também podem ser comparadas *uma contra a outra* para produzir uma curva bi-dimensional característica conhecida por *Receiver Operating Characteristic* (ROC). Um exemplo hipotético pode ser apreciado na figura 3.4. Embora a curva ROC represente uma boa descrição da precisão de um sistema, sua real utilidade vem à tona quando queremos confrontar dois sistemas. É claro que não é uma tarefa trivial, pois as curvas podem não ser tão bem comportadas como a curva da figura 3.4. De fato, as curvas podem se cruzar, e podem indicar diferentes desempenhos em diferentes regiões. Assim, deve ser levado em consideração em que região de T (limiar) desejamos efetuar o confronto.

Existem outros conceitos úteis para avaliação mais delicada de comparadores, como a separação das densidades de probabilidade [Daugman and Williams 1996] e o conceito de Erro Total Esperado, com seu refinamento associado a Funções de Custo para cada tipo de erro [NIST 2003] [Bolle et al. 2004, seção 16.3]. Estas Funções de Custo levam em consideração a vocação do sistema. Por exemplo, em dado sistema, onde seja

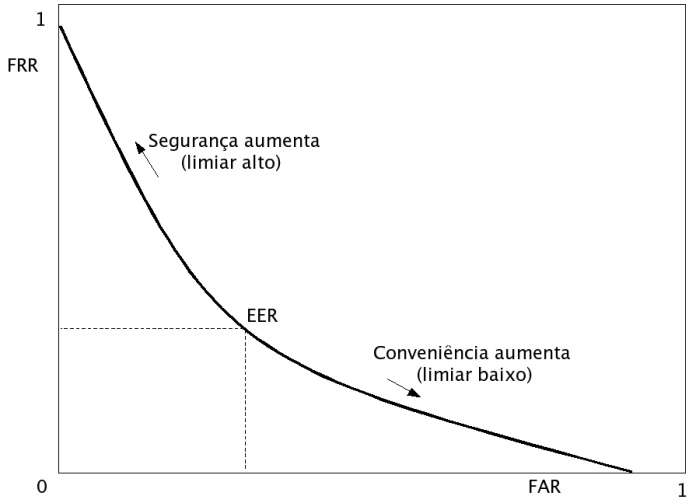

Figura 3.4. *Receiver Operating Characteristic*. As taxas de erro FAR e FRR podem ser plotadas uma contra outra numa curva bi-dimensional. Aqui tentamos mostrar a solução de compromisso entre segurança e conveniência.

necessária alta segurança, os problemas advindos de FRs são aborrecimentos rotineiros, enquanto os problemas advindos de FAs são desastrosos. Por outro lado, podem existir sistemas com maior necessidade de conveniência. Por exemplo, máquinas de autoatendimento de um banco, no qual FRs não são aceitáveis por falta de pessoal de suporte, mas FAs podem ser tolerados, já que existiria uma segunda fase de autenticação por senha.

3.2.6. Seleção

Selecionar uma tecnologia biométrica adequada para uma dada aplicação específica é um processo que envolve muitos fatores. A precisão é um fator importante, mas de maneira alguma é o fator mais importante. De uma maneira simplista, fatores de seleção são extraídos dos requisitos da aplicação. Estes fatores de seleção orientam a escolha da tecnologia biométrica mais adequada. Estes fatores, embora não sejam diretamente quantificáveis, são extremamente úteis no processo de seleção. Este processo é ilustrado na figura 3.5.

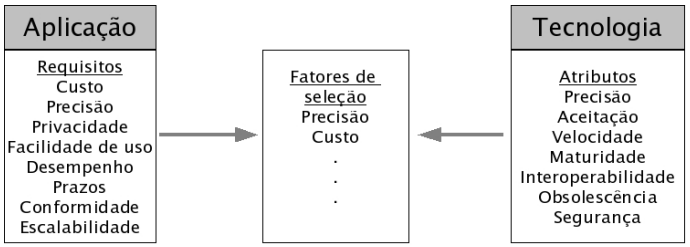

Figura 3.5. Fatores de seleção são extraídos dos requisitos da aplicação para orientar a escolha de tecnologias biométricas com atributos mais adequados.

Tendo em mente os fatores de seleção, uma primeira análise pode ser efetuada com base nos pontos fortes e pontos fracos de cada tecnologia biométrica. Como o processo de seleção pode se tornar complexo, ferramentas para orientação da escolha podem ser utilizadas. Uma **ferramenta preliminar** de análise pode ser utilizada pela construção de uma matriz de comparação baseada em pesos de atributos. A idéia básica é construir

uma matriz de avaliação. De um lado, as tecnologias biométricas disponíveis possuem atributos, aos quais podem ser vinculados valores numéricos. De outro lado, a aplicação possui requisitos. Também podem ser atribuidos valores numéricos para a importância de tais requisitos. O "casamento" entre requisitos e atributos resulta em valores de avaliação para cada tecnologia. A interpretação dos pesos simbólicos como fatores numéricos pode ser ajustada arbitrariamente. Esta matriz de avaliação é especialmente útil em estágios preliminares de análise, para apontar as sensibilidades críticas do suposto sistema [Bolle et al. 2004, p. 138].

Entretanto, um sistema biométrico pode ser suficientemente grande para incorrer em grandes investimentos. Nestes casos, uma **avaliação** mais consistente se mostra necessária. Biometria é uma tecnologia emergente com forte competição de mercado e é desejável a existência de métricas precisas e procedimentos de teste bem definidos. A tecnologia biométrica automatizada ainda é suficientemente emergente para produzir definições duvidosas de precisão e desempenho [Phillips et al. 2000]. Normalmente, as avaliações são implementadas por meio de uma competição entre os interessados (fabricantes ou grupos de pesquisa). Existem três metodologias proeminentes de avaliação: (1) avaliação de tecnologia, (2) avaliação de cenário e (3) avaliação operacional.

O objetivo da **avaliação de tecnologia** [Mansfield and Wayman 2002] é a comparação dos algoritmos competidores de uma tecnologia única. Os testes são realizados sobre um banco de dados padronizado de perfis biométricos. Os resultados dos testes são repetíveis. Neste tipo de avaliação, é concedido aos competidores um certo período de tempo para treinar seus algoritmos de verificação. Um banco de dados de perfis biométricos é disponibilizado pelos organizadores, ou seja, são usados bancos de dados de perfis biométricos previamente construídos. Os módulos de comparação competidores recebem estes dados e têm direito a um certo tempo para o treinamento de seus algoritmos. Esta é a fase de treinamento. Na outra fase, a fase de teste, são definidas as maneiras de obtenção das estatísticas de desempenho. Então, é disponibilizada aos competidores, uma partição do banco de dados de perfis biométricos. A avaliação, portanto, consiste em duas fases, uma fase de treinamento e uma fase de competição. A avaliação de tecnologia permite obter estimativas das taxas de erro dos comparadores (FMR e FNMR). O ponto fraco desta avaliação é que apenas módulos de comparação são avaliados contra bancos de dados, sem controle do ambiente de registro.

O objetivo da **avaliação de cenário** [Mansfield and Wayman 2002] é determinar o desempenho geral do sistema numa aplicação prototipada ou simulada. Os testes englobam o sistema completo num ambiente que modela a aplicação real. É fornecida uma mesma coleção de dados biométricos para os sistemas participantes da avaliação. Os resultados dos testes são repetíveis. Este tipo de avaliação ocorre em uma instalação especial, um ambiente de teste que simula um ambiente de produção. Neste ambiente, são instalados os dispositivos biométricos de verificação (1:1) usados nos testes. Um grupo de voluntários utiliza os sistemas durante um certo período de tempo (idealmente meses ou até mesmo anos), enquanto as estatísticas são coletadas. Podem ser comparados diferentes fabricantes ou até mesmo diferentes tecnologias ao mesmo tempo. Além disso, tal avaliação cria como subproduto um banco de dados de perfis biométricos que pode ser utilizado posteriormente para avaliações operacionais. São obtidas estimativas de FAR e FRR. O ponto fraco desta avaliação fim-a-fim é que os dispositivos não são realmente

atacados, o que leva a valores irreais de FAR.

O objetivo da **avaliação operacional** [Bolle et al. 2004, p. 111] é determinar o desempenho do sistema biométrico como um todo, inserido num ambiente específico de aplicação, atuando sobre uma população-alvo específica. Os resultados geralmente não são repetíveis, já que dependem de características — às vezes desconhecidas ou não documentadas — do ambiente de aplicação. Este tipo de avaliação é realizado, tanto quanto possível, sob circunstâncias reais, ou seja, no ambiente empresarial. Embora seja a avaliação mais realista, não pode medir a verdadeira FAR, já que os eventos de falsa aceitação serão de conhecimento exclusivo dos fraudadores. No entanto, ainda há a possibilidade de estimativa da verdadeira FAR por intermédio de complemento a esta avaliação, por meio da utilização de algo parecido com a contratação de testes de invasão, a exemplo do que é feito com segurança de redes de computadores. Este ainda é um campo aberto para pesquisas.

Para aliviar a dificuldade da tarefa de seleção de sistemas biométricos, existem alguns importantes **documentos de apoio** publicados por instituições dedicadas a sistemas biométricos. Por exemplo, o BWG (*Biometrics Working Group*) publicou um documento contendo um conjunto de conselhos práticos, úteis para gestores envolvidos em projetos de utilização de sistemas biométricos. O documento procura suplementar, e não substituir, metodologias e práticas de gerenciamento de projetos [Mansfield et al. 2002]. Um teste de avaliação pode ser caracterizado por cinco passos: planejamento, aquisição dos dados, análise, estimativa das incertezas e relatório final de desempenho. Regras básicas práticas para levar este trabalho a bom termo estão disponíveis no relatório publicado também pelo BWG [Mansfield and Wayman 2002] e nas especificações publicadas pelo instituto *American National Standards Institute* [ANSI 2005].

3.2.7. Padronização

A padronização é necessária para a ampla aceitação de tecnologias biométricas. Atualmente, os dispositivos não possuem **interoperabilidade**. Padrões internacionais relativos a tecnologias biométricas têm sido propostos e estão em fase de amadurecimento. Estes padrões pretendem dar suporte à troca de dados entre aplicações e sistemas e tentam evitar os problemas e custo oriundos dos sistemas proprietários. Alguns dentre os mais importantes são mostrados na figura 3.6 e descritos resumidamente nos parágrafos a seguir.

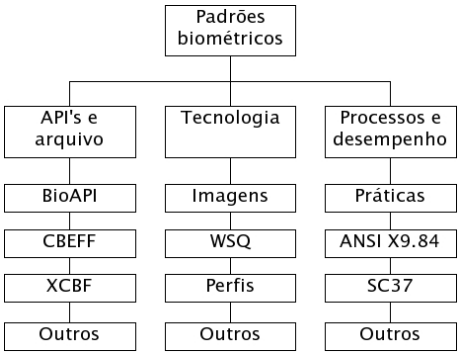

Figura 3.6. Principais esforços de padronização relacionados a sistemas biométricos

BioAPI O consórcio BioAPI[4] foi fundado para desenvolver uma API (*Application Programming Interface*) para proporcionar independência de dispositivo e de plataforma. O consórcio é formado por cerca de 120 companhias (pelo menos uma delas brasileira) interessadas em promover o crescimento do mercado biométrico. A BioAPI é a API mais popular na área biométrica. Suas primitivas se referem a tarefas de registro, identificação e verificação numa plataforma cliente/servidor e aquisição do sinal numa plataforma cliente. No nível mais alto, é definido um BSP (*Biometrics Service Provider*), que lida com todos os aspectos do processamento do sinal. Os diversos componentes se registram durante a instalação. O módulo de registro pode ser usado pelas aplicações para verificar os BSPs instalados e suas funcionalidades. Baseado na BioAPI, foi também definida uma API específica para Java Cards,[5] para dar suporte a funcionalidades biométricas em *smart cards*, principalmente quanto à segurança dos algoritmos e do perfil biométrico eventualmente armazenado no cartão.

CBEFF CBEFF (*Common Biometric Exchange File Format*) é um padrão que procura lidar com os dados biométricos, em sua forma inicial de amostra adquirida ou na forma de características extraidas [NIST 2001]. O padrão procura facilitar a troca de dados entre diferentes processos do mesmo sistema ou até mesmo entre sistemas diferentes. Os dados descritos incluem segurança (assinaturas digitais e cifragem dos dados), processamento da informação (identificação dos tipos biométricos e informação sobre a amostra) e os dados biométricos em si.

ANSI X9.84 Este padrão [ANSI 2003], desenvolvido para utilização na indústria financeira, é compatível com o padrão CBEFF. Ele define requisitos para gerenciamento e proteção da informação biométrica nas fases de coleta, distribuição e processamento dos dados. O padrão inclui especificações para a segurança do equipamento usado, o gerenciamento dos dados, a utilização da tecnologia biométrica para verificação/identificação de clientes e empregados, a aplicação da tecnologia para controle de acesso físico e lógico e técnicas para transmissão e armazenamento seguros dos dados biométricos.

XCBF Desenvolvido sob orientação de um comitê do OASIS, o *XML Common Biometric Format* (XCBF) [OASIS 2003] fornece a codificação XML para o formato padrão CBEFF. A intenção é incrementar a interoperabilidade entre aplicações biométricas baseadas em XML, como aplicações baseadas na Internet. Este padrão também procura ser compatível com as especificações ANSI X9.84.

ISO/JTC1/SC37 SC37 é um subcomitê da ISO (*International Organization for Standardization*) criado na década de 80 para padronização de aspectos ligados a sistemas biométricos. Os grupos de trabalho vinculados atuam em áreas como terminologia, interfaces, formatos de troca de dados, arquitetura funcional, teste e avaliação.

---

[4] `http://www.bioapi.org/`.

[5] A API completa é descrita no documento disponível em `http://www.javacardforum.org/Documents/JCFBIOApiVIA.pdf`.

WSQ Para arquivar o enorme banco de dados de impressões digitais do FBI, foi proposto um algoritmo de compressão eficiente, que mantém a fidelidade dos detalhes das linhas. As imagens de impressão digital, de resolução de 500 dpi (8 bits de escala de cinza) são comprimidos com o uso do algoritmo WSQ (*Wavelet Scalar Quantization*),[6] proporcionando taxas de compressão de cerca de 15:1.

3.3. Tecnologias

3.3.1. Impressão Digital

A formação das impressões digitais se inicia no sétimo mês de gestação, com a diferenciação da pele das pontas dos dedos. O fluxo de fluidos amnióticos em volta do feto e a posição do feto dentro do útero, mudam durante o processo de diferenciação. Então, as células das pontas dos dedos crescem em um micro-ambiente, que é ligeiramente diferente de mão para mão e de dedo para dedo. Os detalhes finos das impressões digitais são determinados por este micro-ambiente em constante mudança.

Em estudos dermatológicos, a máxima diferença entre impressões digitais tem sido encontrada entre indivíduos de diferentes raças. Pessoas da mesma raça, porém sem grau de parentesco, possuem similaridade muito pequena nas digitais. Pai e filho possuem alguma similaridade, por compartilharem metade dos genes. Gêmeos monozigóticos (idênticos) possuem a máxima similaridade. Estima-se que 95% das características das digitais de gêmeos idênticos sejam iguais [Maltoni et al. 2003].

O processo de **aquisição** da impressão digital obtém a imagem em preto e branco das linhas dos dedos. A impressão digital pode ser estampada em papel, pressionando o dedo previamente preparado com tinta. Esta imagem pode ser posteriormente digitalizada por meio de um *scanner*. Um tipo especial de imagens é o das impressões digitais latentes encontradas em cenas de crimes, que podem ser recuperadas por meio de um procedimento especial. Uma imagem ao vivo, por outro lado, é obtida por meio de dispositivos eletrônicos especiais. O princípio básico de todos é a detecção das rugosidades dos dedos que estão em contato com o dispositivo. A aquisição de imagens ao vivo está baseada em quatro tecnologias: ótica, capacitiva, térmica e ultrasônica.

Na tecnologia **ótica**, FTIR (*Frustrated Total Internal Reflection*) e outros métodos óticos são a maneira mais antiga de obtenção de imagens ao vivo. A superfície de aquisição de 1” $\times$ 1” é convertida em imagens de cerca de 500 dpi. A luz refletida depende das condições da pele e imagens saturadas ou difusas podem ser obtidas de peles molhadas e secas, respectivamente.

Na tecnologia **capacitiva**, as cristas e vales da pele da ponta de um dedo, criam diferentes acumulações de carga quando o dedo toca uma rede de chips CMOS. Com a eletrônica adequada, a carga é convertida num valor de intensidade de um pixel. A superfície de aquisição de $0,5$” $\times$ $0,5$” é convertida em uma imagem de cerca de 500 dpi. Tais dispositivos são sensíveis e a qualidade das imagens também é suscetível à pele molhada e seca.

A tecnologia **térmica** se baseia no fato de que a pele é um condutor de calor

[6] As especificações do codificador/decodificador WSQ podem ser encontradas em `http://www.itl.nist.gov/iad/894.03/fing/cert_gui.html`.

melhor que o ar. O contato com as cristas da pele causa uma alteração observável na temperatura da superfície do sensor. A tecnologia supera os problemas de pele seca e molhada e é bastante robusta. A imagem de 500 dpi obtida, no entanto, não é rica em tons de cinza.

Na tecnologia **ultrasônica**, um feixe ultrasônico é dirigido através da superfície do dedo, para medir diretamente a profundidade dos sulcos com base no sinal refletido. As condições de oleosidade da pele não afetam a imagem obtida, que reflete bastante bem a topologia dos sulcos. Contudo, estas unidades tendem a ser grandes e tendem a requerer um tempo de leitura bem maior que os leitores óticos.

A imagem resultante do processo de aquisição pode ser processada na ponta cliente da aplicação ou transmitida ao servidor para processamento. Esta transmissão e armazenamento da imagem envolve compressão e descompressão da mesma, geralmente usando WSQ (seção 3.2.7).

O processo de **extração** de características é o ponto central dos sistemas de autenticação baseados em impressões digitais, com implicações para o projeto do restante do sistema. As abordagens existentes são classificadas em três níveis: global, local e fina.

A abordagem **global** descreve a formação geral das linhas. Geralmente, podem ser observados um núcleo e mais de dois deltas. Estas formações singulares são usadas como pontos de controle, em volta dos quais as linhas são organizadas. A orientação geral das linhas é útil para classificação e indexação em grandes grupos, embora não seja suficiente para comparação precisa.

A abordagem **local** está relacionada com detalhes marcantes das próprias linhas, conhecidos como **minúcias** (*minutiae*). Embora exista mais de uma centena de tipos de detalhes catalogados, os mais utilizados em sistemas automatizados são a terminação de linha e a bifurcação de linha, conforme mostrado na figura 3.7. A extração destas características locais depende fortemente da qualidade da amostra adquirida. Os perfis biométricos obtidos por meio da extração de características de minúcias possuem um tamanho de 250 a 700 bytes.

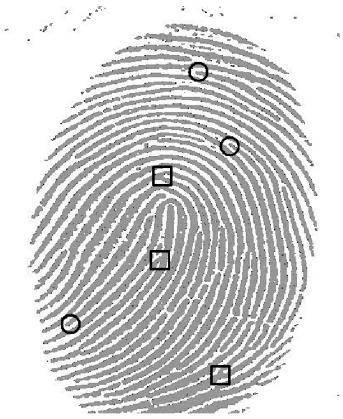

Figura 3.7. Exemplo de dois tipos de minúcias em impressões digitais: bifurcações e terminações de linha.

A abordagem **fina** está baseada nos detalhes intra-linhas, que nada mais são que a

posição e formação geral dos poros de suor, que medem cerca de 60 microns. Embora tais características sejam altamente distintivas, a sua extração somente é viável em imagens de alta resolução (cerca de 1.000 dpi) obtidas de impressões digitais de boa qualidade. A maioria dos sensores fornece imagens de resolução em trono de 500 dpi, assim este tipo de representação não é prático para a maioria das aplicações.

O processo de **comparação** é amplamente baseado nos métodos desenvolvidos por especialistas humanos. Os especialistas avaliam três fatores para declarar que duas impressões digitais pertencem ao mesmo dedo: (1) concordância na configuração global do padrão, ou seja, na distribuição do núcleo e dos deltas, o que implica em que as impressões são do mesmo tipo; (2) concordância qualitativa, ou seja, os detalhes de minúcias devem ser idênticos; e, (3) suficiência quantitativa, que especifica que ao menos um certo número de detalhes de minúcias deve ser encontrado — um mínimo de 12, segundo as orientações legais nos Estados Unidos, também aceitas no Brasil [Kazienko 2003]. A comparação por meios automatizados não segue, necessariamente, os mesmos detalhes de tais orientações, embora esteja baseada nelas de uma maneira estrutural.

Idealmente, a similaridade entre duas impressões digitais obtidas do mesmo dedo deve ser invariante quanto a (1) translação, (2) rotação, (3) pressão aplicada e (4) distorção elástica da pele. As abordagens de comparação foram estudadas por décadas, e duas classes de técnicas podem ser distinguidas:

1. Técnicas baseadas em **imagens** - Esta classe inclui técnicas de correlação de imagem tanto óticas quanto numéricas. As imagens das impressões digitais são superpostas, e a correlação no nível de intensidade entre os pixels correspondentes é computada para diferentes localizações e rotações.

2. Técnicas baseadas em **características** - A comparação baseada em minúcias é o método mais conhecido e mais largamente usado para comparação, graças à analogia com a maneira pela qual os especialistas comparam impressões digitais em aplicações forenses e graças à aceitação legal como prova de identidade na maioria dos paises. Os algoritmos de comparação mais comuns consideram cada minúcia como uma tripla $m = (x, y, \theta)$, contendo a informação de localização espacial 2D (x, y) e de orientação θ. Os detalhes extraídos são então armazenados como conjuntos de pontos, e a comparação consiste em encontrar o alinhamento para o qual os conjuntos de pontos da amostra e do perfil forneçam o máximo número de pares suficientemente coincidentes.

Os pontos fortes da tecnologia de autenticação biométrica baseada em impressão digital são:

- $\oplus$ Esta tecnologia pode proporcionar bastante precisão;[7]

[7]Na prática, a precisão obtida pelos algoritmos não deve ser avaliada pela apreciação da EER. Por exemplo, para a impressão digital, a EER obtida nas competições internacionais pode se mostrar frustrante. O resultado obtido pelo melhor algoritmo na última competição internacional (FVC2004), se aproxima de uma EER de 2,1% [Cappelli et al. 2006]. No entanto, a tecnologia de impressão digital pode trabalhar em outras faixa de operação que proporcionam excelentes resultados de precisão com um pequeno sacrifício da taxa da falsa rejeição.

⊕ Existe uma longa tradição legal no uso da impressão digital como identificador imutável;

⊕ Existem grandes bancos de dados legados de impressões digitais;

⊕ A impressão digital pode ser colhida facilmente a baixo custo.

Quanto aos pontos fracos, podemos citar:

⊖ Em algumas culturas, impressões digitais não são bem aceitas por estarem ligadas a criminosos, pessoas iletradas ou por questões de higiene;

⊖ A qualidade das impressões digitais varia enormemente dentro de uma população;

⊖ Os sensores mais baratos podem ser comprovadamente fraudados.

A tecnologia baseada em impressão digital possui vários recursos associados, como bancos de dados e aplicativos. Por exemplo, o NIST disponibiliza um banco de dados com 2.000 imagens de impressões digitais, para auxiliar pesquisas de classificação, para desenvolvimento de algoritmos e para teste e treinamento de sistemas [NIST 2005]. A Universidade de Bolonha (Itália) disponibiliza as imagens obtidas nas competições por ela organizadas em 2000, 2002 e 2004. Além disso, a mesma universidade disponibiliza um gerador automatizado de impressões digitais [BIOLAB 2005], que pode ser usado para criar imagens para uso em teste e otimização de algoritmos de reconhecimento, bem como para a execução de massa de testes para avaliações desta tecnologia.

O NIST também disponibiliza um pacote utilitário com funções de segmentação, extração e comparação de imagens de impressões digitais.[8] O algoritmo de segmentação pode ser usado para remover espaços em branco das imagens. Outro algoritmo classifica a forma geral da imagem em seis grupos diferentes. O detetor de minúcias pode localizar as terminações e bifurcações de linhas. O algoritmo de comparação pode ser executado nos modos de verificação ou identificação. Além disso, também está disponível uma grande coleção de utilitários para imagens, como codificadores e decodificadores JPEG e WSQ.

Outro exemplo bastante útil é o *FingerCode*,[9] um *software* aberto para comparação de impressões digitais implementado em MATLAB.

3.3.2. Aparência da Face

A aparência da face é uma característica biométrica particularmente convincente, pois é usada rotineiramente como primeiro método de reconhecimento entre pessoas. Por sua naturalidade, é a mais aceitável das biometrias. Devido a esta natureza amigável para o usuário, o reconhecimento de face surge como uma ferramenta poderosa, a despeito da existência de métodos mais confiáveis de identificação de pessoas, como impressão digital e íris.

O processo de **aquisição** de imagens da face possui abordagens que podem ser divididas em quatro grupos: imagem 2D, imagem 3D, seqüência de imagens e termograma.

[8] `http://fingerprint.nist.gov/NFIS/`.
[9] `http://utenti.lycos.it/matlab/speed.htm`.

1. **Imagem 2D** - A obtenção de imagens digitalizadas de fotos de documentos é importante, pois muitos dados legados estão na forma de fotografias, seja em cores, seja em preto-e-branco. Esta é a obtenção estática de imagens. Já para a obtenção de imagens ao vivo, câmeras digitais e analógicas podem ser usadas. As imagens são geralmente captadas com a cooperação do fotografado, e em condições de iluminação controladas. Qualquer câmera de baixo custo, como uma *webcam*, é utilizável para obtenção de imagens 2D. Entretanto, os melhores resultados são obtidos com câmeras que possuem foco automático e lentes apropriadas. Tanto quanto possível, câmeras com características similares devem ser utilizadas nas fases de registro e utilização. O tamanho de um arquivo contendo a imagem da face pode variar de 1 KB a 100 KB, dependendo da compressão utilizada.

2. **Imagem 3D** - Muitas técnicas modernas de reconhecimento de face estão baseadas na geometria da cabeça e exigem imagens tridimensionais. Os modelos 3D contêm mais informações da face e são invariantes à pose. Uma desvantagem ainda presente é que os modelos tratam a face como um objeto rígido, não sendo capazes de tratar expressões faciais. Embora o reconhecimento de face 2D ainda supere os métodos 3D, este cenário pode mudar num futuro próximo [Scheenstra et al. 2005]. A combinação multimodal de abordagens 2D e 3D pode incrementar a precisão total do sistema [Chang et al. 2003]. Um experiência relata uma taxa de EER de 1,9% para uma abordagem multimodal 2D+3D, contra uma taxa EER de 4,5% para as abordagens 2D e 3D separadas [Kyong I. Chang and Flynn 2005]. Para a obtenção de imagens 3D da face, podemos utilizar (1) técnicas baseadas em imagens simultâneas, onde duas câmeras 2D, cujos campos de visão são separados por um ângulo entre 8° e 15°, obtêm imagens independentes para montagem posterior; (2) técnicas baseadas em projeção de um padrão de luz conhecido, cuja distorção pode ser capturada para reconstruir a aparência 3D da face; e (3) técnicas baseadas em varredura a laser, que proporciona um mapa tridimensional pela amostragem de cada ponto da superfície da face.

3. **Seqüência de imagens** - Câmeras de vigilância gravam seqüências de vídeo, com a freqüente inclusão de imagens de faces. No entanto, devido à baixa amostragem (1 a 4 quadros por segundo), a resolução das imagens da face é de baixa qualidade, tornando difícil sua utilização em sistemas automatizados de reconhecimento. Técnicas de seguimento, em conjunção com a utilização de câmeras com *zoom* podem ser usadas para melhoria da resolução, por meio do aumento focado em faces suspeitas. É claro que o custo aumenta bastante, bem como a perda do campo de visão.

4. **Termograma da face** - Um dos problemas na aquisição de imagens da face está relacionado às condições de iluminação. Iluminação infra-vermelha de baixa potência, invisível ao olho humano, pode ser usada para suplementar o processo de detecção da face. Termogramas faciais baseados em radiação infra-vermelha oferecem atrativos, como a independência da iluminação ambiente e a habilidade de resistência a disfarces, mas o alto custo da implementação e a influência de fontes de calor pode afetar esta modalidade de biometria [Prokoski and Riedel 1999].

A figura 3.8 mostra alguns exemplos de imagens de face.

Figura 3.8. Imagem da face 2D (esquerda), 3D (centro) e infravermelho (direita).

O processo de **extração** de características da face possui como primeiro passo a detecção, ou seja, descobrir que existem uma ou mais faces em uma determinada imagem. A detecção, também conhecida como segmentação, é um processo crítico para o sucesso do reconhecimento facial. Métodos baseados em distâncias matemáticas e redes neurais alcançam cerca de 85% de taxa de detecção correta [Zhao et al. 2003]. Existem duas abordagens para a extração de características das imagens da face.

1. **Abordagem global - Aparência da Face** - A idéia básica é reduzir uma imagem de milhares de pixels para um conjunto de números. A distintividade da face pode ser capturada, independentemente do "ruído" produzido pelas variações de luminosidade, textura da pele, reflexos e outros fatores. Para isto, a imagem da face é transformada, dentro de um espaço composto por funções básicas de imagens. Falando simplesmente, as funções básicas de imagens, conhecidas como *eigenfaces*,[10] são usadas ponderadamente para compor a imagem da face em questão [Turk and Pentland 1991]. Pesquisas posteriores introduziram outras transformações similares para a representação e compressão de imagens da face. A transformação fundamental, conhecida como Transformada de Karhunen-Loéve, é agora conhecida pela comunidade biométrica como PCA (*Principal Component Analysis*).

2. **Abordagem local - Geometria da Face** - A idéia é modelar a face em termos da localização geométrica relativa de características particulares tais como olhos, boca, nariz, bochechas, etc. Assim, o reconhecimento de face se resume a comparar os sistemas geométricos obtidos.

Assim como o sistema de percepção humana usa tanto características globais como locais, um sistema de reconhecimento automatizado poderia usar ambos. Pode-se dizer que os métodos híbridos oferecem o melhor dos dois métodos.

O processo de **comparação** está baseado em três tipos de métodos: holísticos, estruturais e híbridos.

[10] *Eigenfaces* são ingredientes padronizados de face, derivados da análise estatística de muitas imagens de face. Qualquer face humana pode ser considerada como uma combinação destas faces padronizadas. A face de uma pessoa em particular poderia ser composta de 8% da face 1, 5% da face 2, e assim por diante. Isto significa que é necessário muito menos espaço para registrar uma face do que a imagem real da mesma necessita.

1. *Métodos holísticos*, que usam toda a região da face. Dentre as várias técnicas existentes, a PCA, baseada em *eigenfaces*, é a mais utilizada.

2. *Métodos estruturais*, contendo técnicas mais recentes que se utilizam de medidas geométricas (ângulos e distâncias) relativas entre diversos pontos notáveis da face, como olhos, nariz, boca e bochechas.

3. *Métodos híbridos*, que tentam oferecer o melhor dos dois métodos, na tentativa de se aproximar do sistema de percepção humano, que se utiliza tanto da aparência global da face quanto das características locais.

Estes métodos possuem em comum a dificuldade de comparação quando a aparência das características muda de forma significativa, como por exemplo, olhos fechados, olhos com óculos ou boca aberta. Em condições de laboratório, os algoritmos de reconhecimento de face podem apresentar taxas de erros bastante aceitáveis. Na prática, o desempenho dos sistemas de reconhecimento de face é muito dependente da aplicação, e bons resultados relatados em especificações de vendas ou campanhas de avaliação não significam necessariamente um bom desempenho em campo, no cenário real de uma aplicação prática [Zhao et al. 2003]. A solução encontrada tem sido restringir os problemas de captura de imagens pelo fornecimento de condições controladas. Mesmo assim, as taxas de erro ainda precisam ser bastante melhoradas.

Os pontos fortes da tecnologia de autenticação biométrica baseada na aparência da face são:

⊕ Existe larga aceitação pública para este identificador biométrico, já que fotos de faces são usadas rotineiramente em documentos.

⊕ Os sistemas de reconhecimento de face são os menos intrusivos, não exigindo qualquer contato e nem mesmo a colaboração do usuário.

⊕ Os dispositivos de aquisição de imagens 2D são de baixo custo.

Quanto aos pontos fracos, podemos citar:

⊖ Em sistemas automatizados de autenticação por meio da face, as condições de iluminação precisam ser controladas. Outros desafios técnicos ainda precisam ser vencidos.

⊖ É uma tecnologia biométrica suficientemente boa para aplicações de verificação de pequena escala. No entanto, é uma biometria pobre para aplicações de identificação de larga escala.

⊖ Uma maneira óbvia e fácil de fraudar o sistema, em aplicações de *screening*, é a utilização de disfarces.

A tecnologia baseada na aparência da face possui vários recursos associados, como bancos de dados e aplicativos. Muitos bancos de dados de imagens de face 2D estão publicamente disponíveis. Os três mais importantes são os mesmos utilizados nas competições internacionais:

- BANCA - O projeto BANCA (*Biometric Access control for Networked and e-Commerce Applications*) oferece para a comunidade de pesquisas, a oportunidade de testar seus algoritmos em um banco de dados grande e realista. Os dados de face e voz foram capturados de 208 indivíduos (metade de cada sexo), por meio de dispositivos de qualidade alta e baixa, em três diferentes cenários (controlados, degradados e adversos) [Bailly-Bailliére et al. 2003].

- FERET - O banco de dados do programa FERET (*FAcial REcognition Technology*),[11] do NIST, possui imagens neutras e naturais da face de 1.200 usuários.

- XM2VTS - Este banco de dados foi coletado durante o projeto M2VTS (*Multi Modal Verification for Teleservices and Security applications*),[12] e consiste de imagens frontais coloridas de 295 usuários em diversas posições de rosto, com fundo uniforme.

Ao contrário das imagens 2D, somente poucos bancos de dados estão disponíveis para reconhecimento facial 3D. O Max Planck Institute for Biological Cybernetics criou um banco de dados adquirido com um *laser scanner* contendo 200 indivíduos. O banco de dados XM2VTS também disponibiliza modelos 3D adquiridos de cerca de 300 indivíduos.

Competições internacionais envolvendo reconhecimento de face também são costumeiras. Existem competições documentadas desde 1995, com base nos três bancos de dados citados (BANCA, FERET e XM2VTS). A competição FVC2004 (*Face Verification Contest* 2004) foi baseada no banco de dados BANCA. A competição FRVT2006 (*Face Recognition Vendor Test* 2006)[13] foi baseada no banco de dados FERET. A competição *ICBA 2006 Face Verification*[14] teve como base o XM2VTS.

Existem vários sistemas abertos de reconhecimento de face. Por exemplo, o OSCVL (*Intel Open Source Computer Vision Library*),[15] contém algoritmos de detecção e reconhecimento de faces. A iniciação em experimentos de avaliação de sistemas de reconhecimento de face também não é difícil. Um sistema completo de avaliação é fornecido pela Colorado State University,[16] compreendendo implementações de quatro algoritmos de reconhecimento que servem como ponto de partida.

3.3.3. Padrão da Íris

A idéia do valor da íris como fonte de informação biométrica confiável, única para cada indivíduo, veio à tona em 1965. A íris contém um rico padrão composto de fibras colágenas, rugas, sulcos, estrias, veias, sardas, fendas, buracos e cores. Embora a tecnologia biométrica de reconhecimento pelo padrão da íris seja relativamente nova, ela tem se mostrado bastante precisa e estável. Dentre poucos sistemas descritos na literatura, o mais conhecido é o IrisCode [Daugman 1999].

---

[11] `http://www.nist.gov/humanid/feret/`.
[12] `http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/`.
[13] Competição de janeiro/2006, sob condução do NIST. `http://www.frvt.org/`.
[14] Conferência internacional em janeiro/2006, em Hong Kong.
[15] `http://www.intel.com/technology/computing/opencv/index.htm`.
[16] `http://www.cs.colostate.edu/evalfacerec/`.

Para o processo de **aquisição** das imagens da íris, os sistemas comerciais utilizam câmeras monocromáticas, já que os métodos de extração de características não se utilizam da cor. A maioria dos sistemas requer que o usuário posicione os olhos dentro do campo de visão de uma câmera de foco estreito. O posicionamento correto é obtido por meio de um *feedback* visual proporcionado por um espelho. Sistemas melhorados, com a utilização de mais de uma câmera, podem ser construídos para uso público e privado [Negin et al. 2000].

O processo de **extração** das características da íris para a criação de um *IrisCode* funciona simplificadamente da seguinte maneira (figura 3.9): (1) é localizada a imagem da íris na imagem adquirida, pela estimativa do centro da pupila; (2) o padrão da íris é isolado da pupila; (3) o padrão é demodulado para extração de sua informação de fase, quando são computados 256 bytes para a imagem da íris e outros 256 bytes representando a máscara para as áreas de ruído, para melhorar a precisão do comparador, perfazendo então um perfil de 512 bytes. Assim, um *IrisCode* é construído pela demodulação do padrão da íris. O processo utiliza uma transformada de Gabor (*complex-valued 2D Gabor wavelets*) para extrair, da estrutra da íris, uma seqüência de fasores (vetores no plano complexo), cujos ângulos de fase são quantizados em bits para compor o código final. A quantização leva em consideração apenas a que quadrante pertence o fasor. O processo é executado num sistema de coordenadas polares, que é invariante à alteração de tamanho da imagem e também invariante à alteração do diâmetro da pupila dentro da íris.

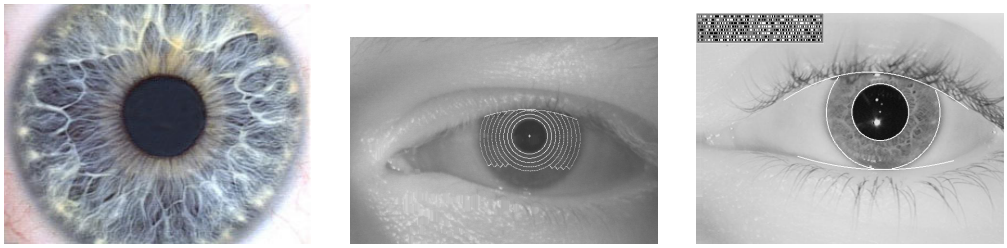

Figura 3.9. Imagem da íris adquirida sob condições ideais (esquerda). Fase de aplicação do algoritmo de extração de características (centro). Íris com seu *IrisCode* associado (direita).

O processo de **comparação** calcula uma medida da similaridade por meio da distância de Hamming normalizada, um método que simplesmente calcula a quantidade da divergência de bits entre as codificações. A chave para o reconhecimento da íris é a falha de um teste de independência estatística [Daugman 1993]. Este teste é implementado por um simples operador booleano *XOR* (OU EXCLUSIVO), aplicado aos vetores codificados dos padrões de íris. Os vetores são mascarados por meio do operador booleano *AND* (E lógico), para prevenir a influência de ruído produzido por lentes, distorções e iluminação.

A simplicidade do teste de comparação é um fator que proporciona alto desempenho. O desempenho do algoritmo é citado como sendo de 100.000 usuários por segundo numa CPU de 300MHz. A precisão dos sistemas biométricos baseados em íris também é um importante fator, que permite que a tecnologia baseada em íris seja adequada tanto para verificação como para identificação. Recente relatório de conclusão de avaliação conduzida pelo *International Biometric Group* cita o melhor ponto de ope-

ração (FMR,FNMR), de um sistema basedo em íris, como sendo $(0,00129\%, 0,583\%)$ [IBG 2005].

Os pontos fortes da tecnologia de autenticação biométrica baseada no padrão da íris são:

- $\oplus$ Dentre as seis principais tecnologias relacionadas neste trabalho, atualmente a íris é considerada como a biometria mais precisa, especialmente quanto a taxas de falsa aceitação (FAR), um importante aspecto de segurança. Portanto, poderia ser uma boa tecnologia para fins puramente de identificação.

- $\oplus$ Possui alto desempenho no processo de verificação. A codificação, comparação e tomada de decisão são computacionalmente tratáveis, com média de tempo de um segundo para a análise da imagem e codificação. Para o processo de identificação, o desempenho é muito bom, com velocidade de comparação de 100.000 registros por segundo numa CPU de 300 MHz.

Quanto aos pontos fracos, podemos citar:

- $\ominus$ A íris não é um alvo fácil. É um alvo pequeno (1 cm) para ser adquirido a uma distância de cerca de um metro. É um alvo móvel, localizado atrás de uma superfície refletora úmida e curvada, parcialmente oculta por pálpebras que piscam freqüentemente e que pode ser obscurecida por óculos, lentes e reflexos e é deformada com a dilatação da pupila. Portanto, exige a colaboração do usuário para a sua coleta.

- $\ominus$ Embora seja uma boa tecnologia para identificação, o desenvolvimento em larga escala é impedido por falta de base instalada. Ademais, criminosos não deixam traços da íris na cena do crime, o que enfraquece a possibilidade de sua utilização em aplicações de investigação criminal.

A maioria dos bancos de dados existentes foi criada para uso comercial e não está disponível publicamente. No entanto, pelo menos quatro bancos de dados estão disponibilizados para propósitos de pesquisa:

- CASIA - Um instituto de pesquisa da China (*Chinese Academy of Sciences, Institute of Automation*) disponibiliza um banco de dados contendo cerca de 3.000 imagens de íris pertencentes a cerca de 230 indivíduos diferentes.[17]

- UBIRIS - A Universidade de Beira Interior (Portugal) disponibiliza um banco de dados com cerca de 1.900 imagens da íris, contendo ruído e que simulam colaboração mínima do usuário.[18]

- CUHK - A Chinese University of Hong Kong oferece cerca de 250 imagens de íris para fins de pesquisa.[19]

[17] `http://nlpr-web.ia.ac.cn/english/irds/resources.htm`.
[18] `http://iris.di.ubi.pt`.
[19] `http://www2.acae.cuhk.edu.hk/~cvl/main_database.htm`.

- UPOL - Finalmente, 384 imagens de íris são disponibilizadas pela UPOL (Univerzita Palackého v Olomouci), da República Tcheca.[20]

Existe pelo menos um sistema de reconhecimento baseado em íris de código-fonte aberto. O sistema, implementado em MATLAB, basicamente usa como entrada uma imagem do olho e devolve como saída um perfil biométrico em código binário [Masek and Kovesi 2003].

3.3.4. Geometria da Mão

Várias tecnologias de verificação com base na geometria da mão evoluíram durante o último século, de dispositivos eletromecânicos para eletrônicos. Foi concedida, em 1960, a primeira patente para um dispositivo que media a geometria da mão, e registrava características para identificação posterior (uma máquina baseada em mecânica, projetada e construída por Robert P. Miller, sob o nome de *Identimation*). Nos anos 70 e 80, várias outras companhias lançaram esforços de desenvolvimento e implementação de dispositivos similares, pressionados pelas oportunidades de mercado. Atualmente, modernos leitores de mão executam funções de controle de acesso, registro de ponto de empregados e aplicações de pontos de venda [Zunkel 1999].

O processo de **aquisição** é baseado na geometria da mão. O comprimento, largura, espessura e curvatura dos dedos e da palma da mão, e a localização relativa destas características, distingue as pessoas entre si. O dispositivo leitor de geometria da mão usa uma câmera para capturar imagens em preto e branco da silhueta da mão (figura 3.10). Não são registrados detalhes de textura, impressões digitais, linhas e cores. Em combinação com um refletor e espelhos laterais, duas imagens distintas são produzidas, uma de cima e uma de lado. Este método é conhecido como **orto-leitura**.

Figura 3.10. Medidas típicas da geometria da mão. O modelo esquemático (esquerda) pode ser apreciado na imagem real (centro) obtida de um dispositivo (direita).

A imagem é obtida com a colaboração do usuário, que coloca a mão numa plataforma especial, contendo pinos para contenção e localização da mão. Estes pinos, que se projetam da plataforma, posicionam a mão do usuário para assegurar uma captura de imagem mais precisa, com melhor qualidade [Sanchez-Reillo et al. 2000]. Uma câmera, localizada acima da plataforma, é ativada quando sensores de pressão localizados próximos aos pinos da plataforma são ativados, indicando que o objeto de interesse está

[20] `http://phoenix.inf.upol.cz/iris/`.

corretamente posicionado. A fotografia é tomada mostrando a silhueta e imagem lateral da mão.

O processo de **extração** trabalha sobre a imagem adquirida. A imagem obtida é convertida para preto e branco, caso seja colorida, e pequenos desvios eventuais são corrigidos. Para estes ajustes, são úteis as imagens dos pinos existentes na plataforma. Um algoritmo de detecção de bordas é aplicado para extrair o contorno da mão. O processamento dos dados extraídos pode fornecer um perfil de apenas 9 bytes de dados, suficientemente pequeno para ser armazenado com facilidade em dispositivos dedicados e também é adequado para trânsito em redes de banda limitada.

No processo de **comparação**, a representação obtida é comparada com o perfil armazenado. A comparação pode envolver, por exemplo, acumulação de diferenças absolutas nas características individuais, entre a representação de entrada e o perfil armazenado. Para o cálculo da similaridade entre os dois vetores, são utilizados algoritmos baseados em distância euclidiana, distância de Hamming, modelos de mistura gaussiana (GMM—*Gaussian mixture models*) ou redes neurais. Os melhores resultados são apresentados pelos algoritmos baseados em GMMs [Sanchez-Reillo et al. 2000]. Para a acomodação dos fatores naturais e ambientais que alteram o formato da mão das pessoas, os dispositivos leitores podem possuir um processo de atualização dos perfis armazenados. Este processo é executado sob certas condições, durante o processo de comparação. Esta acomodação do perfil atualiza a descrição matemática armazenada quando a diferença entre a amostra e o perfil atinge um limite pré-determinado.

As características individuais da mão não são muito descritivas e este método de autenticação possui taxas de erro relativamente altas. Apesar disso, os sistemas de verificação com base na geometria da mão são bastante difundidos. Uma avaliação de cenário efetuada em 2001 pelo BWG relata uma taxa de erros de cruzamento de FAR$\times$FRR (ou seja, a EER) em torno de 1,5% para esta tecnologia [Mansfield et al. 2001].

Os pontos fortes da tecnologia de autenticação biométrica baseada no formato da mão são:

- $\oplus$ A coleta das características é fácil e não intrusiva.
- $\oplus$ A computação é bastante simples e os perfis são pequenos, o que torna fácil a construção de sistemas dedicados isolados. O pequeno tamanho do perfil (9 a 35 bytes) reduz as necessidades de armazenamento.
- $\oplus$ Adequado para integração com outras biometrias, em particular impressão digital e impressão palmar
- $\oplus$ Não relacionado a registros policiais e criminais.

Quanto aos pontos fracos, podemos citar:

- $\ominus$ Assim como na tecnologia de impressões digitais, a geometria da mão é medida quando o usuário pressiona uma superfície. Este contato pode despertar preocupações públicas com higiene.

⊖ Não é suficientemente distintiva para identificação, sendo adequada apenas para aplicações de verificação.

A tecnologia baseada no formato da mão é utilizada essencialmente em pequenos sistemas, uma vez que tal característica biométrica não fornece unicidade suficiente para identificação em larga escala.

3.3.5. Dinâmica da Assinatura

A assinatura pode ser ***off-line*** ou **estática**, aquela impostada em documentos de papel, escrita por meio convencional e posteriormente adquirida por meio de uma câmera ou scanner. Pode ser ainda ***on-line*** ou **dinâmica**, aquela efetuada num dispositivo eletrônico preparado para capturar, com alto grau de resolução, as característica dinâmicas temporais da assinatura, como a trajetória da caneta, a pressão, direção e elevação do traço.

O processo de **aquisição** pode ser baseado numa abordagem estática ou dinâmica. A abordagem estática data de 1975. Várias abordagens de análise automatizada são baseadas em características como número de contornos interiores e número de componentes de inclinação. Entretanto, a falta de informação dinâmica torna o processo automatizado de verificação estática bastante vulnerável a fraudes. O problema da verificação automática de assinaturas estáticas atraiu grande atenção nos últimos anos, mas os resultados não têm fornecido a precisão requerida por muitos problemas de segurança. As técnicas de abordagem criadas nos últimos 20 anos incluem transformadas 2D, histogramas de dados direcionais, curvatura, projeções verticais e horizontais do traço da assinatura, abordagens estruturais, medidas locais no traço, posição de pontos característicos. Um dos melhores resultados tem sido fornecido pela análise baseada no tamanho das distribuições granulométricas locais [Sabourin et al. 1997].

A abordagem dinâmica é bem mais interessante. A verificação da dinâmica da assinatura está baseada nas características do processo de assinatura em si. Um modo temporal de representação da assinatura contém mais informação, o que pode tornar o processo mais preciso. Contudo, este modo necessita de dispositivos especiais. Os dispositivos normalmente podem ser divididos em três tipos, de acordo com com a parte do dispositivo responsável pela aquisição: aquisição por meio da caneta, aquisição por meio da superfície e aquisição por meio de ambas.

O processo de **extração** de características se baseia principalmente na componente temporal. Na análise dinâmica, são introduzidas as noções de tempo e pressão, além do espaço bidimensional do papel. Os dispositivos utilizados podem, por exemplo, registrar um fluxo de vetores penta-dimensionais colhidos em pontos temporais equidistantes. Esses vetores poderiam, por exemplo ser compostos por $A = (x, y, p, \theta_x, \theta_y)$, onde x e y correspondem à posição, p corresponde à força axial exercida pela caneta e θ_x e θ_y registram os ângulos da caneta em relação ao plano xy. Esta informação adicional é bastante útil na prevenção de fraudes. Um arquivo de assinaturas contendo funções temporais de posição, pressão, azimute e elevação possui normalmente um tamanho entre 5 KB e 10 KB. Formatos mais eficientes e compressão na razão 3:1 permitem o armazenamento em arquivos de 1 KB a 2 KB.

Na análise de assinaturas dinâmicas, as abordagens de **comparação** incluem as

medidas de distâncias euclidianas entre as trajetórias de canetas, medidas de correlação regional e reconhecimento temporal-probabilístico como as cadeias de Markov ocultas. Afinal, o problema pode ser reduzido à classificação temporal. Durante os últimos 30 anos, numerosos algoritmos e modelos foram desenvolvidos. O conjunto de características no qual o processo de decisão está baseado, é constituido de funções temporais como pressão, posição, velocidade e aceleração, representadas por conjuntos de valores discretos periódicos e representadas por valores paramétricos obtidos com base no processamento de tais funções. Os métodos podem ser acomodados em quatro grupos:

1. *Classificadores probabilistas* - Estes métodos são baseados nas distribuições da densidade de probabilidades do conjunto de características genuíno e do conjunto de características em geral. Uma distância entre estas duas distribuições é determinada para fixar o grau de importância de dada característica. A decisão é baseada na distância Euclidiana, computada sobre um conjunto de características.

2. *Classificadores elásticos* - Esta técnica mais antiga, obscurecida desde o advento das cadeias de Markov ocultas, é baseada na utilização de DTW (*Dynamic Time Warping*) [Myers and Rabiner 1981]. Esta técnica computa as distâncias temporais mínimas entre um vetor de entrada e os vetores-modelo. Existem diferenças de tempo não-lineares entre as características das assinaturas produzidas pela mesma pessoa. O objetivo é encontrar o alinhamento temporal ótimo entre a assinatura de referência e a assinatura sob verificação.

3. *Redes neurais* - Esta ferramenta de Inteligência Artificial tem sido explorada pra a verificação dinâmica de assinaturas, mas o desempenho registrado tem sido inferior aos outros métodos.

4. *Cadeias de Markov ocultas* - Cadeias de Markov ocultas (HMM—*Hidden Markov Models*) são o meio mais popular de classificação temporal, com aplicações em áreas como reconhecimento de discurso, escrita e gesticulação. Informalmente, uma cadeia de Markov oculta é uma variante de uma máquina de estados finita e não-determinística, onde os estados e transições possuem associações probabilistas [Rabiner and Juang 1986]. Inspirada pelo sucesso da aplicação de HMMs ao reconhecimento de caracteres, este agora é o modelo com melhor desempenho na verificação de assinatura. A vantagem para esta tarefa advém da possibilidade de aceitar variabilidade, ao mesmo tempo em que se captura características individuais da assinatura.

Os pontos fortes da tecnologia de autenticação biométrica baseada na dinâmica da assinatura são:

⊕ A assinatura dinâmica é uma combinação de informação e biometria. O conteúdo e modo da escrita podem ser escolhidos e até mesmo alterados pelo usuário.

⊕ Possui grande aceitação por parte do usuário.

⊕ A assinatura dinâmica é bastante difícil de ser fraudada. A comunidade interessada em autenticação por meio da dinâmica de assinatura define o nível de sofisticação do

fraudador em categorias, como *zero-effort forgery*, *home-improved forgery*, *over-the-shoulder forgery* e *professional forgery*. Esta divisão em categorias por nível de sofisticação ainda não existe em outras tecnologias biométricas.

Quanto aos pontos fracos, podemos citar:

- ⊖ O custo dos dispositivos de aquisição é alto.

- ⊖ Esta característica biométrica possui alta variabilidade. Existem, ainda, muitas pessoas com assinaturas inconsistentes. Assim, os sistemas de verificação podem ser exigidos a apresentar a possibilidade de configuração de limiares de decisão por usuário.

Embora esta não seja uma das soluções biométricas mais seguras, ainda se justifica o uso da mesma nas práticas negociais, pois trata-se de um método *de facto* para verificação da identidade de uma pessoa. Esta tecnologia, quando utilizada para verificação (busca 1:1), ao invés da identificação (busca 1:N), possui um futuro bastante promissor. Por este motivo, várias pesquisas vêm sendo desenvolvidas, baseadas nesta tecnologia. Por exemplo, um protótipo de sistema de autenticação baseado em assinaturas dinâmicas foi construído na UNISINOS usando redes neurais do tipo *cascade-correlation* como mecanismo de comparação, relatando bons resultados de precisão, com um ponto de operação (FAR, FRR) estimado em (2,6%, 3,6%) [Heinen and Osório 2004].

Abordagens para localização da caneta e estimativa de orientação usando luz visível foram desenvolvidas, o que pode finalmente baixar o custo de aquisição de assinatura e pode até mesmo levar a assinaturas tridimensionais [Munich and Perona 1998].

O projeto BISP[21] visa desenvolver canetas multi-sensoriais para registro e análise de biometria comportamental e características neuromotoras, ambas baseadas na cinemática e na dinâmica da escrita em geral e da assinatura em particular [Hook et al. 2003].

Resultados relatados na primeira competição internacional de verificação por dinâmica da assinatura (SVC 2004)[22] relatam taxas de EER entre 2,89% e 16,34% para o melhor e pior algoritmo. Estão disponíveis no *site* da competição, arquivos de assinatura adquiridos de 40 usuários. Cada usuário contribuiu com 20 assinaturas. Por razões de privacidade, os usuários foram alertados para não contribuir com suas assinaturas reais, mas sim com assinaturas "inventadas". Para cada assinatura, existe uma assinatura forjada, perpetrada por falsários aos quais foi permitido assistir a uma exibição da impostação da assinatura. Existem assinaturas no estilo chinês (ideogramas) e no estilo latino (alfabeto latino da esquerda para a direita). Os arquivos de dados contêm vetores de dados de posição, pressão, azimute, elevação, registro de caneta em contato e registro de tempo. Este banco de dados pode ser bastante útil para a avaliação de algoritmos em desenvolvimento [Yeung et al. 2004].

[21] `http://www.bisp-regensburg.de/`.
[22] `http://www.cs.ust.hk/svc2004/`.

3.3.6. Padrão de voz

A autenticação por meio da voz tem sido uma área de pesquisa bastante ativa desde os anos 70. Atualmente, os sistemas podem ser divididos em classes, de acordo com o protocolo estabelecido:

1. *Texto fixo* - O usuário pronuncia uma palavra ou frase pré-determinada, secreta, gravada durante a fase de registro.

2. *Dependente do texto* - O usuário é solicitado, pelo sistema de autenticação, a pronunciar algo específico, dentre as diversas opções previamente registradas no sistema. Neste caso, a fase de registro é bastante longa. É similar ao protocolo de texto fixo, com um número maior de opções.

3. *Independente do texto* - O usuário pronuncia frases conforme seu desejo. O sistema processa qualquer discurso do usuário.

4. *Conversacional* - O usuário é interrogado, pelo sistema de autenticação, com perguntas cujas respostas são secretas, tornando-se um protocolo misto de conhecimento e biometria. É um protocolo similar ao dependente de texto, sendo que as frases previamente gravadas possuem um certo grau de segredo.

Para auxiliar o processo de **aquisição**, existem numerosos transdutores para transformar as ondas acústicas de voz em ondas eletromagnéticas. A quantidade de espaço de armazenamento necessária para os dados de voz sem tratamento dependem da taxa de amostragem, níveis de quantização e número de canais (mono-canal na maioria das vezes). Por exemplo, um sinal de voz amostrado a uma taxa de 16 kHz, com um nível de quantização de 16 bits, utiliza cerca de 31 KB por segundo de sinal.

Para a aplicação de ferramentas matemáticas, sem perda de generalidade, o sinal de voz deve ser representado por uma seqüência de vetores de características. O processo de **extração** pode se basear: (1) na abordagem tradicional, por meio de PCA (*Principal Component Analysis*) e FA (*Factor Analysis*); (2) na abordagem de estimativa de médias e covariâncias; e (3) na estimativa de divergências [Campbell 1997].

O processo de **comparação** das características extraídas pode ser suportado por vários métodos. Os principais métodos de abordagem para comparação dos dados de voz estão listados a seguir. Existem trabalhos que comparam algumas destas abordagens, como por exemplo [Yu et al. 1995].

- *DTW - Dynamic Time Warping* - Permite a compensação da variabilidade humana inerente ao padrão de voz. Método mais usado para verificação dependente do texto. Atualmente pouco utilizado como algoritmo *per se*, mas sim como um suplemento ao processo de decisão.

- *Métodos Estatísticos (HMM e GMM)* - Recaem na modelagem paramétrica do sinal de voz. A modelagem pode ser dependente do tempo, por meio da utilização de cadeias de Markov ocultas (HMM), ou não dependentes do tempo, por meio da utilização de modelos de mistura gaussiana (GMM). Os valores dos parâmetros

devem ser obtidos de dados de treinamento, o que é um ponto crítico nos métodos estatísticos: dados suficientes precisam ser obtidos para "treinamento". O método HMM é bastante comum para sistemas dependentes de texto. No entanto, o método GMM é agora o modelo dominante para reconhecimento de voz, freqüentemente em combinação com um provedor de informação de alto nível, como DTW.

- *VQ - Vector Quantisation* - Raramente usado, pois somente consegue superar os métodos estatísticos quando existem poucos dados disponíveis.
- *Redes Neurais* - Redes neurais têm sido usadas em pesquisas de reconhecimento de voz independente de texto, treinadas com dados de usuários genuínos e usuários impostores.
- *SVM - Support Vector Machines* - Esta abordagem tem sido proposta em pesquisas recentes (desde 1996). Os resultados relatados têm sido superiores aos resultados de GMMs.

Os pontos fortes da tecnologia de autenticação biométrica baseada no padrão de voz são:

- ⊕ A voz, assim como a face, é uma biometria usada instintivamente pelas pessoas para autenticação mútua.
- ⊕ Sistemas com infra-estrutura telefônica constituem o principal alvo do reconhecimento de voz. A fala com o objetivo único de autenticação (autenticação ativa), pode ser um tanto quanto anti-natural, mas em situações onde o usuário já tem mesmo de falar, o protocolo de autenticação se torna passivo, amigável e não-intrusivo.
- ⊕ Esta tecnologia utiliza dispositivos baratos, e além disso é facilmente desenvolvida sobre uma infra-estrutura já existente e amplamente espalhada, como o sistema telefônico.
- ⊕ Permite protocolos de autenticação de segurança incremental. Por exemplo, quando maior confiança é necessária, o sistema pode esperar por mais dados de voz. Outro exemplo, pode ser utilizado um protocolo de biometria conversacional, combinado com verificação de conhecimento. Outro exemplo, o protocolo pode verificar a identidade continuamente durante a conversação.
- ⊕ Em aplicações de texto independente e aplicações conversacionais, os usuários não necessitam de um processo separado de autenticação, o que torna o processo totalmente integrado.

Quanto aos pontos fracos, podemos citar:

- ⊖ É possível a imitação por pessoas habilidosas ou a utilização de gravações da voz do usuário legítimo para fraudar o sistema. Além disso, existem sistemas de síntese que podem ser treinados para imitar a voz de pessoas.

⊖ A tecnologia *text-to-speech* torna possível a criação de identidades não existentes, em sistemas de registro e autenticação remotos.

⊖ A qualidade do sinal de áudio é suscetível ao ruído do ambiente. Além disso, são introduzidas distorções na captação do sinal pelo microfone e na transmissão do sinal através do canal.

⊖ O padrão de voz é bastante frágil, pois pode ser alterado pelo estado do usuário (saúde, emoção, pressa, sono, preguiça, entre outros).

A tecnologia baseada no padrão de voz possui vários recursos associados, como bancos de dados e aplicativos. A utilização de bancos de dados padronizados para desenvolvimento e avaliação, mostrou seu valor no progresso das pesquisas de reconhecimento de voz e reconhecimento de discurso. Uma visão geral dos diversos bancos de dados disponíveis é proporcionada por [Campbell and Reynolds 1999], do qual foram extraídos os exemplos mais comuns:

- LDC - *Linguist Data Consortium* (EUA) - Dá suporte à pesquisa, por meio da criação e compartilhamento de recursos linguísticos, como dados, ferramentas e padrões. Mantém vários bancos de dados, inclusive o *YOHO Speaker Verification*, útil para experimentos com reconhecimento de voz dependente de texto.[23]

- ELRA - *European Language Resources Association* (Luxemburgo) - Mantém vários bancos de dados em línguas européias.[24]

O pacote LIA_RAL, da Université d'Avignon, na França, é um software de reconhecimento de voz, de código fonte aberto, implementado em C++.[25] É capaz de reconhecer vários tipos de características e tem sido usado nas avaliações do NIST. Pode servir como base de comparação com outros sistemas.

A principal competição em reconhecimento de voz é a série de avaliações conduzida pelo NIST. A série, iniciada em 1996, é focada fortemente no reconhecimento de voz por meio telefônico [Reynolds et al. 2000].

As taxas de erro para sistemas de autenticação por meio da voz são muito dependentes da aplicação. Isto quer dizer que bons resultados obtidos em competições de avaliação ou publicados em especificações de fabricantes, não significam necessariamente que os mesmos serão obtidos na prática, nas aplicações específicas. Esta tecnologia está amadurecida pelas pesquisas, mas alguns problemas permanecem ainda não resolvidos. São problemas relacionados ao usuário, ao ambiente e ao canal. O desempenho depende muito das condições de aquisição e teste. Mesmo assim, competições internacionais tentam estabelecer taxas de erros aproximadas que permitam comparações com outras tecnologias. Por exemplo, em competição aberta conduzida pelo NIST em 2003 foi obtida uma taxa EER de 5,3% [Przybocki and Martin 2004].

[23] `http://www.ldc.upenn.edu/`.
[24] `http://www.elra.info/`.
[25] `http://www.lia.univ-avignon.fr/heberges/ALIZE/LIA_RAL/index.html`.

3.3.7. Comparativo sumário

Uma comparação entre as seis tecnologias biométricas apresentadas nesta seção é mostrada na tabela 3.2 [Jain et al. 2004]. Esta comparação avalia o grau (alto, médio ou baixo) com que cada tecnologia satisfaz as propriedades desejáveis de características biométricas discutidas na seção 3.2.1; embora resumida, ela permite obter um panorama geral dessas tecnologias.

Dentre as características biométricas apresentadas, a impressão digital e a íris são as mais estáveis ao longo do tempo. A íris pode fornecer a maior precisão, embora a impressão digital seja a mais utilizada. A tecnologia baseada no formato da mão já tem seu nicho de mercado bastante consolidado. As tecnologias de face e assinatura possuem a aceitação do usuário e são de fácil coleta.

A aplicação de uma determinada tecnologia biométrica depende fortemente dos requisitos do domínio da aplicação. Nenhuma tecnologia pode superar todas as outras em todos ambientes de operação. Assim, cada uma das tecnologias é potencialmente utilizável em seu nicho apropriado, ou seja, não existe tecnologia ótima.

Biometria	Universalidade	Unicidade	Permanência	Coleta	Aceitação
Digital	Média	Alta	Alta	Média	Média
Face	Alta	Baixa	Média	Alta	Alta
Íris	Alta	Alta	Alta	Média	Baixa
Mão	Média	Média	Média	Alta	Média
Assinatura	Baixa	Baixa	Baixa	Alta	Alta
Voz	Média	Baixa	Baixa	Média	Alta

Tabela 3.2. Comparativo sumário entre as características de alguns identificadores biométricos

3.4. Arquiteturas

3.4.1. Armazenamento

Existem várias possibilidades de **distribuição dos processos** componentes de um sistema biométrico. Num caso extremo, podemos ter todos os processos localizados no dispositivo de aquisição, como é o caso de pequenos sistemas de acesso físico. Neste caso, os processos de aquisição, extração e comparação, bem como o banco de dados de perfis biométricos, estão todos localizados no mesmo equipamento ou, no máximo, limitados a uma rede local.

Noutro extremo, podemos ter um ampla distribuição dos processos. Vamos supor um sistema de larga escala, com centenas de milhares de perfis registrados e diversos locais de aquisição de biometria, como é o caso de um sistema de autenticação de clientes bancários em máquinas de auto-atendimento. O processo de aquisição pode se dar em diversos pontos do sistema. O armazenamento dos perfis pode se dar em *smart cards* em poder do usuário. Uma cópia do perfil pode ou não ser armazenado em servidor central para o caso de uma reemissão de cartões extraviados. Os processos de extração e comparação também podem estar distribuídos, dependendo da conveniência para a arqui-

tetura do sistema. Estes processos podem ser locais (junto ao dispositivo de aquisição) ou remotos (em servidor ou até mesmo no próprio *smart card*).

A forma de **armazenamento dos perfis** depende do tipo de aplicação para qual o dispositivo biométrico será utilizado e do tamanho dos perfis. Os perfis, como visto inicialmente, são os dados armazenados que representam a medida biométrica de um usuário cadastrado, utilizados pelo sistema biométrico para posterior comparação com outras amostras submetidas. De uma forma geral, os perfis podem ser armazenados de forma local, remota ou distribuída.

O armazenamento **local** corresponde ao armazenamento no próprio dispositivo de aquisição, ou em computador a ele acoplado por meio da rede local. Esta forma de armazenamento não é adequada para o caso de aplicações com um grande número de usuários ou quando o usuário precisa ser verificado em diversos locais diferentes. Quanto à segurança, os riscos de comunicação são eliminados, uma vez que não é necessária a transmissão dos perfis biométricos, e o impacto de um possível comprometimento é reduzido em extensão, pois somente atinge os dados locais. Por exemplo, os pequenos e médios sistemas de controle de acesso físico geralmente se valem de armazenamento local. O sistema armazena os perfis dos usuários candidatos a acesso a determinado local. A quantidade de usuários pode variar de unidades, no caso de acesso a uma residência, ou centenas, no caso de controle de acesso a academias, ou milhares, para controle de acesso a grandes prédios ou instalações.

O armazenamento **remoto** corresponde ao armazenamento em um servidor, o que quase sempre quer dizer uma base de dados centralizada. Esta solução é adequada para aplicações onde o número de usuários é grande ou quando é necessária verificação remota. Este processo pode ser comprometido quando a segurança dos dados é ameaçada por sistemas de comunicação ou redes vulneráveis ou por abuso de privilégios na manipulação da base de dados. Os sistemas de identificação (busca 1:N) de larga escala geralmente se utilizam da modalidade de armazenamento remota. Este sistemas geralmente comportam milhões de usuários e possuem requisitos mais refinados de precisão e desempenho. Os sistemas de verificação (busca 1:1) de larga escala podem ou não se valer desta modalidade de armazenamento.

O armazenamento **distribuído** corresponde ao armazenamento em dispositivos que ficam em poder do usuário, normalmente sob a forma de *smart cards*. O método de armazenamento de perfis utilizando cartões magnéticos permite que o usuário carregue seu próprio perfil para a utilização nos dispositivos de verificação, sendo indicado para aplicações onde o grupo de usuários seja numeroso demais para ser armazenado numa base de dados central, quando é necessário que os usuários sejam verificados remotamente ou quando há necessidade de uma transmissão rápida dos perfis.

A **entidade armazenadora** dos perfis biométricos possui sérias responsabilidades derivadas das preocupações com privacidade e possibilidade de mau uso dos dados. Os pioneiros na adoção da tecnologia de autenticação baseada em biometria normalmente estão baseados nos próprios recursos para implementação e gestão da infra-estrutura necessária para dar suporte à autenticação. Este cenário pode sofrer alterações, dependendo da entidade armazenadora e da portabilidade do dispositivo de aquisição.

Quanto à entidade armazenadora, podemos considerar dois tipos de entidades, que chamamos de agentes autorizados e agentes de confiança. Um **agente autorizado** é uma organização que adota a autenticação biométrica e assume a responsabilidade por registrar e administrar os perfis biométricos de seus usuários conforme os requisitos dessa autenticação. Um **agente de confiança**, por sua vez, é uma organização à qual é delegada a responsabilidade pelos dados biométricos: ela se encarrega do registro e administração de perfis de usuários e presta um serviço de verificação de credenciais biométricas a entidades que desejam utilizar essa forma de autenticação. Um exemplo de agente autorizado seria um banco que decide usar biometria para autenticar seus próprios clientes, e um exemplo de agente de confiança seria um órgão governamental responsável por gerenciar dados biométricos que seriam usados para fins de autenticação em vários setores do serviço público.

Já quanto ao dispositivo de aquisição, vamos considerar que ele pode ser administrado ou livre. O dispositivo de aquisição **administrado** é um equipamento que está localizado em pontos específicos de acesso ao sistema, e que pode servir a vários usuários, cada um por sua vez. Já o dispositivo de aquisição **livre** é um equipamento que está em poder do usuário, como por exemplo, um *palmtop* ou um telefone celular.

A tabela 3.3 mostra os cenários derivados das diferentes combinações possíveis entre agentes de armazenamento e dispositivos de aquisição. No cenário chamado "pioneiro" (com agente autorizado e dispositivo administrado), temos a figura de um agente autorizado que registra cada usuário e armazena o perfil para uso posterior, quando o usuário desejar fazer uma transação. Além disso, instala e gerencia a infra-estrutura necessária para os dipositivos de aquisição. Neste cenário, o início de novos projetos é facilitado, pois o agente pode decidir-se pelo uso da biometria unilateralmente, ou seja, não depende de infra-estrutura oficial. A integridade fim a fim do sistema também pode ser controlada pela entidade. É claro que este agente autorizado tem que suportar todo o custo e o risco de implementar e gerenciar o sistema. Outro ponto fraco é que o usuário deve se registrar novamente a cada novo agente ou organização, talvez usando outras características biométricas. Isto pode levar a preocupações com privacidade, uma vez que o usuário pode relutar em confiar sua característica biométrica a diversas organizações diferentes.

Entidade	Dispositivo administrado	Dispositivo livre
Agente autorizado	Cenário Pioneiro	Cenário Temerário
Agente de confiança	Cenário Organizado	Cenário Audacioso

Tabela 3.3. Cenários possíveis ao se combinar os dispositivos de aquisição (administrados ou livres) e agentes de armazenamento (autorizados ou de confiança)

No cenário dito "temerário" (com agente autorizado e dispositivo livre), temos a figura de um agente autorizado que registra cada usuário e cada dispositivo. Este é um cenário considerado ainda improvável atualmente, pois o agente autorizado fica responsável pelas condições de segurança do sistema, embora não possua o gerenciamento completo dos dispositivos de aquisição. Um exemplo atual seria um sistema de uma instituição financeira, que oferece acesso aos usuários por meio de seus telefones celulares.

No cenário considerado "organizado" (com agente de confiança e dispositivo ad-

ministrado), temos a figura de um agente de confiança que fornece um *smart card* com *status* oficial, a ser usado em múltiplas entidades integrantes do sistema. O cartão contém o perfil biométrico e permite autenticação local em dispositivos de aquisição fixos, espalhados entre várias entidades integrantes do sistema. O agente de confiança mantém cópia do perfil para nova emissão de cartão, quando necessário. Este cenário assume que um número pequeno de dispositivos de aquisição é adotado como padrão. O custo do sistema diminui bastante para os agentes autorizados, já que ele pode ser compartilhado por todos. No entanto, as entidades integrantes dependem da infra-estrutura do agente de confiança. A aceitação do sistema pelo usuário é aumentada, pois ele passa a ser o detentor de seu próprio perfil biométrico, armazenado em cartão. Todavia, o usuário pode relutar em utilizar os dispositivos de aquisição, com a suspeita de que os mesmos poderiam ter sido adulterados para capturar as características biométricas para utilização posterior.

No quarto cenário, batizado de "audacioso" (com agente de confiança e dispositivo livre), o agente de confiança distribui o perfil associado ao usuário. Além disso, o usuário se utiliza de dispositivos de aquisição que estão em seu próprio poder. Temos um cenário onde a sensação de privacidade do usuário é aumentada, pois agora o usuário carrega consigo o seu próprio dispositivo de aquisição e o seu próprio perfil biométrico. Os agentes autorizados mantêm a diminuição de seus custos pelo compartilhamento dos mesmos, mas o usuário tem o inconveniente de ter de carregar consigo o dispositivo.

3.4.2. Segurança

A segurança de sistemas biométricos pode ser diferenciada em, ao menos, três importantes aspectos: a precisão do sistema, representada pelas medidas clássicas estatísticas de taxas de falsa aceitação e falsa rejeição; a arquitetura do sistema e implementação do sistema em si, representada pela interconexão física e lógica entre suas diversas partes componentes e a aplicação; e, a robustez do sistema, representada pela sua capacidade de resistência à fraude e falsificação intencionais.

A precisão pode ser avaliada por meio de bancos de dados representativos e um conjunto básico de medidas aceitas. Com respeito à arquitetura do sistema, existem procedimentos, embora mais complexos, para avaliar a segurança de um projeto e sua implementação de uma maneira padronizada. No entanto, a robustez é a mais difícil de ser avaliada, pois é fácil mostrar que um sistema biométrico pode ser fraudado, mas é muito mais difícil mostrar que um sistema biométrico não pode ser fraudado. Assim, independentemente de quão preciso é o sistema e de quão bem projetada é a sua arquitetura, não se pode enunciar de antemão conclusões sobre a sua resistência a ataques. Esta seção se concentra em considerações sobre as vulnerabilidades de sistemas biométricos.

Vários padrões de **taxonomia de ataques** a sistemas biométricos foram apresentados. Os mais importantes são:

1. *Biometric Device Protection Profile* (BDPP) [DIN 2003].

2. *Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments* (DoDPP) [Kong et al. 2002].

3. *U.S. Government Biometric Verification Mode Protection Profile for Medium Ro-*

bustness Environments (USGovPP) [Kong et al. 2003].

Os padrões de taxonomia listados são bastante similares em várias maneiras, mas mesmo assim não é trivial comparar a nomenclatura dos ataques entre eles. De qualquer modo, a abordagem de análise de ameças e contramedidas por meio do auxílio da construção sistemática de uma árvore de possibilidades, ou árvore de ataques, permanece como ferramenta útil de projeto. Um estudo para os sistemas focados em defesa contra FRR (*False Rejection Rate*), tenta cobrir os claros existentes, acrescentando outros níveis de hierarquia à árvore de ataques [Buhan et al. 2006]. Outra abordagem, que integra conceitos de gerenciamento e de segurança, propõe uma metodologia estruturada (*BASS model*) bastante abrangente na análise de vulnerabilidades [Leniski et al. 2003]. A lista a seguir apresenta apenas alguns exemplos de vulnerabilidades:

- *Vulnerabilidades no processo de aquisição* - Um ataque pode ser implementado de várias maneiras. Num ataque de coerção, os dados biométricos verdadeiros são apresentados usando a força ou outros métodos ilegais de persuasão. Num ataque de personificação, um usuário não autorizado altera seus dados biométricos para aparecer como um indivíduo autorizado, por exemplo por meio do uso de disfarces ou imitação. Num ataque de impostação, dados verdadeiros são apresentados por um usuário não autorizado. Por exemplo, os passos necessários para criar uma impressão digital sem colaboração do seu proprietário são descritos em [Putte and Keuning 2000]. Outro exemplo seria a apresentação de partes do corpo extraídas de seus usuários. Uma análise de ataques para o caso da impressão digital pode ser apreciada em [Uludag and Jain 2004].

- *Vulnerabilidades nos processos de extração e comparação* - A utilização de um cavalo de Tróia (*Trojan horse*) pode permitir um ataque que consiste em alterar o módulo de extração. Por exemplo, a corrupção do processo de extração pode ser programada para produzir um conjunto de caractarísticas favoráveis à aceitação do impostor. A corrupção do processo de comparação pode permitir a produção de escores superiores ao escore real e pode, ainda, permitir a modificação da decisão final produzida no módulo de comparação. Outros ataques interessantes podem ser executados [Schneier 1999]. O ataque *hill-climbing* envolve a submissão repetida de dados biométricos, com pequenas modificações entre cada repetição, com a preservação das modificações que resultem num escore melhorado. O ataque *swamping* é similar ao ataque de força bruta, e consiste na submissão de dados em abundância, na esperança de que seja alcançado pelo menos o escore necessário para autenticação.

- *Vulnerabilidades no processo de registro* - A segurança do processo de registro é de extrema importância, pois uma vez que um fraudador consiga colocar seu perfil biométrico no sistema, passará a ser tratado como usuário válido. Até mesmo possíveis ataques em conivência com o administrador do sistema devem ser analisados neste processo. Outro ataque poderoso é aquele dirigido ao banco de dados dos perfis biométricos armazenados (centralizado ou distribuído), para leitura ou modificação não autorizada dos perfis.

- *Vulnerabilidade nos canais entre os processos* - Em muitos sistemas reais, alguns módulos do sistema podem estar fisicamente distantes entre si. Em tais sistemas, os canais entre os processos podem constituir vulnerabilidades importantes. Ataques de repetição (*replay*) são os mais comuns.

Assim como outros mecanismos de segurança, qualquer sistema biométrico pode ser fraudado com um adequado investimento em tempo e dinheiro. Do ponto de vista do gerenciamento de riscos, a tarefa do projetista de segurança é fazer com que o custo para se violar a segurança do sistema seja superior ao benefício obtido com a violação. A única coisa que pode ser feita a favor da segurança é o incremento dos custos envolvidos para a consecução da fraude. A vantagem do projetista é que ele pode investir tempo e dinheiro previamente para tentar proteger o sistema contra todo ataque possível e imaginável. A vantagem do impostor é que ele apenas necessita usar a criatividade para encontrar um ataque ainda não pensado. Esta luta entre ataques e contramedidas pode ser bem exemplificado por meio de uma coletânea de ataques e contramedidas referente a um sistema hipotético baseado no padrão da íris [Ernst 2002]. Além dos mecanismos tradicionais de cifragem e estampilha de tempo, a lista a seguir apresenta algumas das principais contramedidas de caráter geral e outras que ainda estão em fase de pesquisa.

- Suporte na área de aquisição - Em aplicações biométricas nas quais a supervisão está presente quando os sujeitos estão submetendo seus dados biométricos, a probabilidade de um indivíduo ludibriar o sistema é substancialmente reduzida. Algumas aplicações simplesmente não permitem tal supervisão, como é o caso de autenticação de usuários via Web. Em outras aplicações pode existir uma solução de compromisso entre custo e segurança, como seria o caso de uma aplicação de autenticação de usuários em terminais de auto-atendimento de bancos.

- Detecção de repetição - O sistema pode se valer de uma propriedade das características biométricas como ferramenta de segurança. Afinal, é desprezível a possibilidade de dois exemplares biométricos serem exatamente iguais. O sistema poderia então descartar qualquer exemplar idêntico a um dos exemplares anteriores. O preço a pagar por tal ferramenta é custo do espaço de armazenamento e capacidade de processamento extra. Mesmo assim, uma solução econômica pode manter em histórico os códigos *hash* dos últimos exemplares colhidos de cada usuário. Uma coincidência exata em nova amostra indica um ataque de repetição. Outro método poderia ser a solicitação de reapresentação da biometria. Por exemplo, em sistemas baseados em dinâmica da assinatura, o usuário pode ser solicitado a assinar mais de uma vez, devendo o sistema certificar-se de que os exemplares de assinatura não sejam idênticos.

- Detecção de perfeição - A mesma propriedade do item anterior serve para a criação de outra contramedida aplicável a sistemas biométricos. Caso o exemplar apresentado seja idêntico ao perfil armazenado, é certo que houve vazamento do perfil biométrico.

- Resposta sumária - As respostas sumários ou ocultação dos dados (*hiding data*), servem para evitar ataques *hill-climbing*. Assim, o sistema deve fornecer apenas uma

resposta ao usuário não autenticado (NÃO), abstendo-se de explicar qual o motivo da recusa e abstendo-se, é claro, de informar qualquer valor de escore obtido.

- Desafio e resposta - Medida bastante apropriada contra ataques de repetição, o desafio e reposta envolve o envio de um desafio ao usuário, que deve responder apropriadamente para obter autorização. Em sistemas de voz, pode ser usada a verificação independente de texto ou a verificação conversacional.

- Detecção de vitalidade (*liveness detection*) - A detecção de vitalidade (ou detecção de vivacidade) num sistema biométrico de autenticação deveria assegurar que somente características reais, pertencentes a pessoas vivas, fossem aceitas como válidas. Isto tornaria o sistema mais seguro e aumentaria também o poder de não-repudiação. No entanto, até mesmo pequenos esforços podem levar à fraude em sensores biométricos atuais. Trabalhos descrevendo fraudes em impressões digitais [Sandstrom 2004], íris e imagens da face demonstram isto claramente. A detecção de vitalidade pode se dar no processo de aquisição ou no processo de extração de características.

Além das citadas, outras três contramedidas podem vir a se tornar importantes ferramentas de segurança: a utilização conjunta de várias biometrias, a aplicação de transformações irreversíveis sobre os dados biométricos (para aumentar a privacidade) e a combinação de biometria e *smart cards*. Vejamos mais detalhes quanto a estas contramedidas.

Multibiometria

Algumas limitações dos sistemas biométricos podem ser superadas com a utilização sistemas biométricos multimodais. A proposta de tais sistemas é aumentar a confiabilidade e atender os requisitos impostos por várias aplicações [Ross et al. 2006]. A obtenção de multiplicidade pode se dar em diversos pontos do sistema, conforme ilustrado na figura 3.11:

1. Múltiplas biometrias podem ser utilizadas (voz e face, por exemplo) ou múltiplas unidades da mesma biometria (dedos diferentes ou olhos diferentes, por exemplo).

2. Múltiplos sensores, como sensores óticos e capacitivos para impressão digital.

3. Múltiplas amostras da mesma biometria; por exemplo, múltiplas impressões do mesmo dedo.

4. Múltiplos comparadores, ou seja, diferentes abordagens para a representação de características e diferentes algoritmos de comparação.

O processo de fusão também pode se dar em diversos pontos do sistema (figura 3.11):

1. Fusão na amostra, ou seja, os diversos dados obtidos são concatenados em um único vetor de características com maior poder de diferenciação.

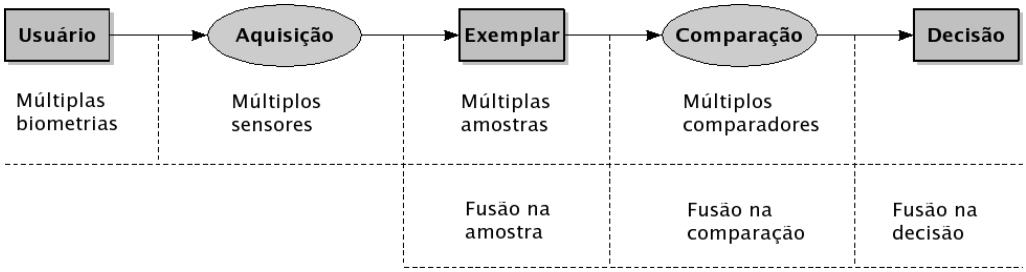

Figura 3.11. Dentro do processo genérico de um sistema biométrico, há diversos pontos para obter multiplicidade e há diversos pontos para efetuar a fusão.

2. Fusão na comparação, ou seja, os diversos escores de similaridade obtidos são combinados por meio de médias ponderadas.

3. Fusão na decisão, ou seja, as diversas decisões obtidas são combinadas para produzir uma única decisão.

O aumento de custo e a maior inconveniência para o usuário são as maiores barreiras para a utilização de sistemas biométricos multimodais em aplicações comerciais. No entanto, em aplicações de alta segurança, em aplicações de identificação de larga escala e em aplicações de varredura a utilização de tais sistemas é bastante adequada [Jain et al. 2004].

Biometria cancelável

Uma técnica conhecida como **biometria cancelável** pode aliviar as preocupações com privacidade e segurança. Trata-se de uma distorção intencional efetuada sobre os dados biométricos, por meio de uma transformação escolhida. Geralmente, as transformações não são reversíveis, de modo a proteger a característica biométrica original. Em caso de comprometimento, o perfil transformado pode ser cancelado, e outra variante pode ser criada por meio de outra transformação. As transformações podem ser aplicadas no domínio do sinal adquirido ou no domínio das características extraídas. As **distorções no domínio do sinal** se referem às transformações aplicadas aos dados biométricos adquiridos por meio do sensor. Exemplos de transformações neste domínio são a grade de deformação e a permutação de blocos. Na grade de deformação, a imagem original é estruturada dentro de uma grade alinhada com as características marcantes da mesma. Um algoritmo de deformação qualquer é então aplicado, com diferentes parâmetros para cada porção da grade. Já na permutação de blocos, uma estrutura de blocos é superposta à imagem, alinhada com pontos característicos da mesma. Os blocos da imagem original são então misturados de uma forma aleatória, mas repetível. Estas transformações são mais comumente aplicáveis a imagens 2D de face, impressão digital, íris e mão.

As **distorções no domínio das características** extraídas atuam sobre o perfil biométrico, geralmente por meio de um mapeamento irreversível. Assim, o sinal adquirido é processado da forma usual, e os atributos extraídos é que sofrem uma transformação. Por exemplo, seja um perfil biométrico representativo de uma impressão digital, representado por um conjunto de pontos de minúcias $M = (x_i, y_y, \theta_i); i = 1, \ldots, n$. As coordenadas

dos pontos podem ser transformadas através de um mapeamento baseado em polinômios. Como mostra a figura 3.12, cada coordenada x_i é transformada para uma nova coordenada X_i por meio de uma função polinomial de, digamos, terceira ordem $X = F(x)$. As coordenadas y e θ podem ser transformadas de modo similar por meio de $Y = G(y)$ e $\Theta = H(\theta)$.

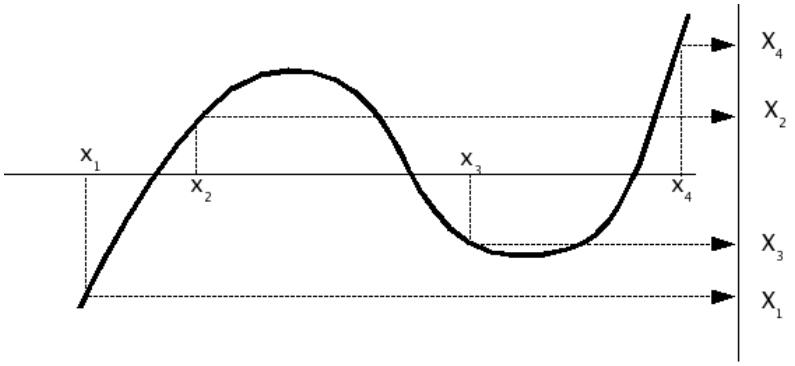

Figura 3.12. Um exemplo de mapeamento de uma das coordenadas de um conjunto de pontos de minúcias em um novo conjunto de coordenadas, por meio de uma transformação irreversível.

Outro exemplo seria o sistema proposto para tornar revogáveis os perfis biométricos de impressões palmares, por meio do armazenamento de vários códigos, compostos pelo *hash* da impressão palmar em conjunto com uma chave pseudo-aleatória [Connie et al. 2005].

Utilização de *smart cards*

Em muitas soluções de segurança, é usada uma infra-estrutura de chaves públicas, cuja confiabilidade repousa na existência de chaves privadas de conhecimento exclusivo dos seus proprietários. A criptografia assimétrica permite a criação de uma par de chaves, a chave pública D_k e a chave privada E_k. Ora, a chave privada proporciona alta resistência à fraude dificulta o ataque de força bruta, devido ao tamanho da chave. A chave privada (E_k) deve ser de conhecimento exclusivo do usuário e deve permanecer sempre em poder deste. Na prática, este requisito de segurança causa ao usuário um certo grau de inconveniência, pois a chave privada é muito grande para ser memorizada. Geralmente ela é armazenada em algum dispositivo, como um disco magnético, um *pen drive* ou um *smart card*.

No caso de armazenamento em cartão inteligente, é necessário que o usuário forneça um código para acessar o *smart card*, o que geralmente é feito pelo fornecimento de um número PIN ou uma senha. Isto leva a um ponto desvantajoso no armazenamento da chave privada. Para a proteção da mesma, é utilizado um código fornecido pelo usuário. Se o usuário se vale de um código forte (longo e complicado) não é prático memorizá-lo e se o usuário se vale de um código apenas guardado na memória, provavelmente será um código fraco. Isto reduz a segurança proporcionada pela chave privada para o nível de segurança proporcionado pelo código usado para acessá-la. Idealmente, a chave privada deveria ser protegida por um método tão seguro quanto a segurança que ela proporciona. Assim, estamos de volta ao impasse código forte (difícil de memorizar) $\times$ código fraco

(fácil de memorizar). Esta situação leva naturalmente ao desejo de utilização de biometria como código de acesso ao dispositivo que armazena uma chave privada. Esta combinação valiosa poderia proporcionar excelente nível de segurança.

As questões a serem consideradas nesta união de *smart card* e biometria envolvem a capacidade computacional dos cartões e o projeto de algoritmos eficientes de processamento de sinais, adequados ao ambiente proporcionado pela estrutura dos cartões. Além disso, para tratar as ameças de segurança proporcionadas pela comparação *off-card* de amostras e perfis biométricos, é necessário que o algoritmo de comparação seja implementado dentro do *smart card*. Atualmente, para algumas tecnologias biométricas, é possível também embutir o dispositivo de aquisição no próprio cartão, como é o caso da impressão digital e da voz. Alguns algoritmos específicos para reconhecimento de impressões digitais *on-card* foram desenvolvidos. Por exemplo, uma parceria entre companhias francesa e sueca desenvolveu um cartão com acesso por meio de impressão digital [Carlson 2003]. [26]

Embora existam *smart cards* com sensores de impressão digital ou microfones embutidos, a inserção de sensores de outras tecnologias biométricas no corpo de um *smart card* é assunto para o futuro próximo. O problema maior para a larga utilização desta facilidade é a diversidade de sistemas operacionais e ambientes de desenvolvimento. Uma alternativa promissora é a utilização de *Java Cards*, mesmo com a penalidade ao desempenho imposta por uma linguagem interpretada [Osborne and Ratha 2003]. Por meio do armazenamento, aquisição e comparação no *smart card*, o perfil biométrico fica circunscrito ao cartão. Este método é normalmente visto como o meio mais seguro de proteção biométrica em segurança da informação. Na prática, o *smart card* é tornado pessoal, posto que não pode ser acessado sem a autenticação biométrica apropriada. Os perfis biométricos nunca são expostos a ambientes não confiáveis e o usuário carrega consigo seus próprios perfis biométricos, o que soluciona várias questões relativas à privacidade das características biométricas.

A introdução de biometria para o acesso ao cartão que armazena uma chave privada também introduz um problema. O que acontece se a característica biométrica muda? Por exemplo, suponhamos que apenas o polegar direito seja usado para acesso e o usuário sofre um acidente que altera a sua impressão digital? Este problema da irrevogabilidade é o mesmo do usuário que esquece a senha de acesso a um certo recurso. É necessário alterar a senha. No caso descrito, é necessário que o usuário utilize os serviços da mesma entidade que registrou o seu perfil biométrico atualizar o cartão.

É razoável supor, então, que uma determinada aplicação possa contar com a existência de chaves privadas de usuários armazenada em *smart cards* e somente acessíveis por meio de dispositivos de aquisição embutidos no cartão. Mesmo assim, será necessário um dispositivo de leitura para interagir com o cartão. Outra camada necessária é uma camada de *software* localizada no computador que hospeda a aplicação principal, que geralmente toma a forma de um *driver* de dispositivo. Desta maneira, considerando a necessidade de segurança em sistemas, remanesce a pergunta: quanta segurança foi

[26] Segundo alegação de um fabricante específico de *smart card* acessível por meio de impressão digital, o sistema embutido no cartão suporta níveis de precisão desde 1% FAR até 0.0001% FAR, e testes independentes mostraram que a precisão de EER fica em torno de 0.1% [Nordin 2004].

adicionada à aplicação, ou, em outras palavras, quão poderosa é a ferramenta descrita?

3.5. Problemas Abertos

Além da larga utilização em investigação criminal, as tecnologias biométricas estão sendo rapidamente sendo adotadas numa grande variedade de aplicações de segurança, como controle de acesso físico e lógico, comércio eletrônico, gestão digital de direitos autorais, segurança de prédios e residências e bloqueio de equipamentos. Em geral, essas aplicações requerem, dos subsistemas biométricos, alta precisão, alto desempenho e baixo custo.

Entretanto, embora tenha havido grandes avanços recentes, ainda é necessário um vigoroso esforço de pesquisa para resolver muitos problemas desafiadores. Um trabalho recente organiza os principais obstáculos à ampla disseminação de sistemas biométricos [Chandra and Calderon 2005]. Seis grandes classes abrangem cerca de 30 problemas atuais ainda não resolvidos concernentes a tecnologias biométricas. Companhias fabricantes e usuárias que planejam implementar a tecnologia de sistemas biométricos automatizados devem refletir sobre as principais questões que desfiam tais sistemas. Tais desafios necessitam de uma solução abrangente que satisfaça às legítimas preocupações dos usuários. Existe um campo aberto para pesquisas sobre o assunto, do qual elaboramos uma lista não exaustiva:

- Unicidade - Métodos e métricas para estimar a quantidade de informação contida nos diversos identificadores biométricos, o que está relacionado diretamente com a unicidade dos mesmos.
- Avaliação - Padrões, métodos e métricas para avaliação estatística da precisão e do desempenho dos diversos tipos de sistemas biométricos.
- Escala - Análise de diversas características específicas de sistemas de verificação e de identificação de larga escala.
- Cifragem - Técnicas eficientes de proteção dos perfis biométricos, dos dados que transitam entre os processos e técnicas de proteção de privacidade.
- Multibiometria - Fusão da informação em diversos níveis.
- Certificação - Proposta de entidade(s) certificadora(s) de sistemas biométricos. Natureza da entidade e escopo da certificação.
- Desenvolvimento de sensores, considerando aspectos desejáveis como baixo custo, detecção de vitalidade, portabilidade, entre outros.
- Processos - Melhoria ou criação de métodos ou algoritmos de aquisição, extração e comparação de características.
- Protocolos e arquiteturas - Análise dos protocolos e arquiteturas existentes e efetivação de novas propostas com foco no reforço de segurança e privacidade dos dados.

- Detecção de vitalidade - Equipamentos e métodos de detecção de vitalidade ou, até mesmo, de detecção de não-vitalidade.

- Revogação ou cancelamento - Criação ou melhoria de métodos e técnicas para prover a revogação das características biométricas.

- Novas tecnologias - Criação de novos identificadores biométricos.

- *Smart cards* - Conjugação de biometria e *smart cards*.

3.6. Conclusão

Este capítulo buscou apresentar uma visão geral sobre sistemas de autenticação biométrica. Os tipos de autenticação biométrica levam à diferenciação dos sistemas em sistemas de identificação (busca 1:N) e de verificação (busca 1:1), sendo que cada um destes tipos possui características específicas e aplicações mais adequadas. Existem numerosas características físicas e comportamentais do ser humano que podem ser usadas como identificadores biométricos. Dentre elas, os mais utilizados atualmente foram apresentados com um pouco mais de detalhe. Cenários de armazenamento de perfis foram levantados e, finalmente, questões de segurança foram abordadas.

Mostramos que não existe uma tecnologia "melhor", mas sim a tecnologia mais adequada perante cada aplicação. Mostramos ainda que a biometria possui grande utilidade. Para sistemas de identificação, a utilização de biometria já está bastante consolidada, sendo a impressão digital a tecnologia biométrica mais utilizada, embora haja espaço para outras tecnologias. Para sistemas de verificação, consideramos que, no estágio atual de desenvolvimento tecnológico, a utilização de biometria deve ser cuidadosamente analisada. No caso de haver risco para o usuário, a biometria deve ser utilizada como acessório.

Não é demais relembrar à exaustão que a biometria não é cem por cento precisa. Esta é uma característica que permite configurar um sistema para ser mais rigoroso ou mais permissivo, dependendo do limiar de comparação. Os pontos fortes das tecnologias biométricas em geral são: (1) a biometria é fortemente vinculada a uma identidade e (2) a biometria não precisa ser memorizada, nem pode ser esquecida ou emprestada. No entanto, estes pontos fortes levam também a fraquezas correspondentes, que são: (1) a biometria não é revogável e (2) a biometria não é segredo. Pesquisas têm sido levadas a cabo no sentido de eliminar ou amenizar os pontos fracos.

Uma mensagem final sobre a utilização de sistemas biométricos não pode deixar de lado a questão principal deste trabalho, que é o reforço de segurança. A segurança de sistemas biométricos se traduz na proteção da aplicação e é alcançada pela eliminação de vulnerabilidades nos pontos de ataque aos ativos da aplicação. A introdução de biometria em um sistema não deve criar novas vulnerabilidades e aberturas. Em outras palavras, a introdução de biometria para incrementar segurança deve ser convenientemente analisada e justificada. A autenticação biométrica deve ser um aspecto integrado da segurança da aplicação como um todo, o que inclui a identificação e prevenção de brechas de segurança do próprio sistema biométrico.

Até mesmo o reforço de segurança proporcionado por sistemas biométricos necessita ser cuidadosamente avaliado, devido ao efeito da *mudança do elo fraco*. Um sistema qualquer possui pontos de vulnerabilidades quanto à segurança. Os pontos mais vulneráveis são os "elos fracos". Ao reforçarmos a segurança em um elo mais fraco, outro ponto do sistema vai se tornar o elo mais fraco. Um exemplo particularmente alarmante é o do homem que teve a extremidade de um dedo amputada por ladrões para que estes pudessem roubar seu carro, protegido por um sistema biométrico [BBC 2005]. Neste caso, a contramedida causou uma mudança de tática do atacante, mudando o elo fraco para o próprio usuário.

Referências

[ANSI 2003] ANSI (2003). Biometric information management and security for the financial services industry. ANSI X9.84-2003, American National Standards Institute.

[ANSI 2005] ANSI (2005). *ANSI INCITS 409 - Information Technology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework - Part 2: Technology Testing and Reporting - Part 3: Scenario Testing and Reporting*. American National Standards Institute.

[Bailly-Bailliére et al. 2003] Bailly-Bailliére, E., Bengio, S., Bimbot, F., Hamouz, M., Kittler, J., Mariéthoz, J., Matas, J., Messer, K., Popovici, V., Porée, F., Ruiz, B., and Thiran, J.-P. (2003). The BANCA database and evaluation protocol. In *4th International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, volume 2688 of *Lecture Notes in Computer Science*, pages 625–638, Guildford, UK. Springer-Verlag.

[BBC 2005] BBC (2005). Malaysia car thieves steal finger. `http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm`. Acessado em julho/2006.

[Bergadano et al. 2002] Bergadano, F., Gunetti, D., and Picardi, C. (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, 5(4):367–397.

[BioID 2005] BioID (2005). Humanscan. `http://www.bioid.com`. Acessado em julho/2006.

[BIOLAB 2005] BIOLAB (2005). Synthetic FINgerprint GEnerator. Biometric Systems Lab - `http://bias.csr.unibo.it/research/biolab`. Acessado em julho/2006.

[BITE 2005] BITE (2005). Global biometric market and industry report. Technical report, Biometric Identification Technology Ethics. `http://www.biteproject.org/`.

[Bolle et al. 2004] Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., and Senior, A. W. (2004). *Guide to Biometrics*. Springer Professional Computing, 1st edition.

[Bolle et al. 2002] Bolle, R. M., Connell, J. H., and Ratha, N. K. (2002). Biometric perils and patches. In *Pattern Recognition*, volume 35, pages 2727–2738. Elsevier Science.

[Buhan et al. 2006] Buhan, I., Bazen, A., Hartel, P., and Veldhuis, R. (2006). A false rejection oriented threat model for the design of biometric authentication systems. *Proceedings of the International Conference on Biometrics 2006 (Hong Kong, China)*, 3832:728–736.

[Burge and Burger 2000] Burge, M. and Burger, W. (2000). Ear biometrics in computer vision. In *International Conference on Pattern Recognition*, volume 2, pages 2822–2826, Los Alamitos, CA, USA. IEEE Computer Society.

[Campbell 1997] Campbell, J. P. (1997). Speaker recognition: A tutorial. *Proceedings of the IEEE*, 85(9):1437–1462.

[Campbell and Reynolds 1999] Campbell, J. P. and Reynolds, D. A. (1999). Corpora for the evaluation of speaker recognition systems. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing*, 2:829–832.

[Cappelli et al. 2006] Cappelli, R., Maio, D., Maltoni, D., Wayman, J. L., and Jain, A. K. (2006). Performance evaluation of fingerprint verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(1):3–18.

[Carlson 2003] Carlson, L. (2003). Match on card system for IT security. In *Biometric Technology Today*, volume 11, pages 3–4. Elsevier Science.

[Chandra and Calderon 2005] Chandra, A. and Calderon, T. (2005). Challenges and constraints to the diffusion of biometrics in information systems. *Communications of the ACM*, 48(12):101–106.

[Chang et al. 2003] Chang, K., Bowyer, K., and Flynn, P. (2003). Multimodal 2D and 3D biometrics for face recognition. *IEEE International Workshop on Analysis and Modeling of Faces and Gestures*, pages 187–194.

[Chen and Jain 2005] Chen, H. and Jain, A. K. (2005). Dental biometrics: Alignment and matching of dental radiographs. *IEEE Tansactions on Pattern Analysis and Machine Intelligence*, 27(8):1319–1326.

[Clarke 1994] Clarke, R. (1994). Human identification in information systems: management challenges and public policy issues. *Information Technology & People*, 7(4):6–37.

[Connie et al. 2005] Connie, T., Teoh, A., Goh, M., and Ngo, D. (2005). Palmhashing: a novel approach for cancelable biometrics. *Information Processing Letters*, 93(1):1–5.

[Daugman 1999] Daugman, J. (1999). Recognizing persons by their iris patterns. In Jain, A. K., Bolle, R. M., and Pankanti, S., editors, *Biometrics: Personal Identification in Networked Society*, chapter 5. Kluwer Academic Publishers, Boston, MA, USA.

[Daugman 1993] Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161.

[Daugman and Williams 1996] Daugman, J. G. and Williams, G. O. (1996). A proposed standard for biometric decidability. In *Proceedings of CardTech/SecureTech*, pages 223–234, Atlanta, GA, USA.

[DIN 2003] DIN (2003). Information Technology - security techniques - a framework for security evaluation and testing of biometric technology. ISO/IEC JTC 1/SC 27 N 3806, Deutsches Institut fur Normung, Berlin, Germany.

[Ernst 2002] Ernst, J. (2002). Iris recognition: Counterfeit and countermeasures. `http://www.iris-recognition.org/counterfeit.htm`. Acessado em julho/2006.

[Fink et al. 2001] Fink, G. A., Wienecke, M., and Sagerer, G. (2001). Video-based online handwriting recognition. In *International Conference on Document Analysis and Recognition*, pages 226–230, Los Alamitos, CA, USA. IEEE Computer Society.

[Heinen and Osório 2004] Heinen, M. R. and Osório, F. S. (2004). Biometria comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas. *Infocomp Revista de Ciência da Computação*. ISSN 1807-4545 volume 3 fasciculo 2 pgs 31 a 37 Lavras MG Brasil.

[Hill 1999] Hill, R. B. (1999). Retina identification. In Jain, A. K., Bolle, R. M., and Pankanti, S., editors, *Biometrics: Personal Identification in Networked Society*, chapter 6. Kluwer Academic Publishers, Boston, MA, USA.

[Hook et al. 2003] Hook, C., Kempf, J., and Scharfenberg, G. (2003). New pen device for biometrical 3d pressure analysis of handwritten characters, words and signatures. In *WBMA '03: Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, pages 38–44, New York, NY, USA. ACM Press.

[IBG 2005] IBG (2005). Independent testing of iris recognition technology. Technical Report NBCHC030114/0002, International Biometric Group.

[Jain et al. 2004] Jain, A. K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Tecnhology*, 14(1):4–20.

[Kazienko 2003] Kazienko, J. F. (2003). Assinatura digital de documentos eletrônicos através da impressão digital. Dissertação de mestrado, Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina.

[Kong et al. 2002] Kong, A., Griffith, A., Rhude, D., Bacon, G., and Shahs, G. (2002). Department of Defense federal biometric system protection profile for medium robustness environments. Technical report, U.S. Department of Defense.

[Kong et al. 2003] Kong, A., Griffith, A., Rhude, D., Bacon, G., and Shahs, G. (2003). US Government biometric verification mode protection profile for medium robustness environments. Technical report, The Biometrics Management Office and National Security Agency.

[Korotkaya 2003] Korotkaya, Z. (2003). Biometric person authentication: Odor. Inner report in Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology. in “Advanced Topics in Information Processing: Biometric Person Authentication”.

[Kyong I. Chang and Flynn 2005] Kyong I. Chang, K. W. B. and Flynn, P. J. (2005). An evaluation of multimodal 2D+3D face biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(4).

[Landwehr 2001] Landwehr, C. E. (2001). Computer security. *International Journal of Information Security*, 1(1):3–13.

[Leniski et al. 2003] Leniski, A. C., Skinner, R. C., McGann, S. F., and Elliott, S. J. (2003). Securing the biometric model. In *IEEE* 37^{th} *Annual 2003 International Carnahan Conference on Security Technology*, pages 444–449.

[Lu et al. 2003] Lu, G., Zhang, D., and Wang, K. (2003). Palmprint recognition using eigenpalms features. *Pattern Recognition Letters*, 24(9-10):1463–1467.

[Maltoni et al. 2003] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. Springer Verlag, New York, USA.

[Mansfield and Wayman 2002] Mansfield, A. and Wayman, J. (2002). Best practices in testing and reporting performance of biometric devices, version 2.0.1. Technical report, Biometrics Working Group, `http://www.afb.org.uk/bwg/bestprac.html`.

[Mansfield et al. 2001] Mansfield, T., Kelly, G., Chandler, D., and Kane, J. (2001). Biometric product testing final report. Technical Report CESG contract X92A/4009309, UK Biometrics Working Group.

[Mansfield et al. 2002] Mansfield, T., Kelly, G., Chandler, D., and Kane, J. (2002). Biometrics for identification and authentication - advice on product selection. Technical report, UK Biometrics Working Group.

[Masek and Kovesi 2003] Masek, L. and Kovesi, P. (2003). MATLAB source code for a biometric identification system based on iris patterns. Master’s thesis, The School of Computer Science and Software Engineering, The University of Western Australia. Código-fonte disponível em `http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html`. Acessado em julho/2006.

[Miller 1994] Miller, B. (1994). Vital signs of identity. *IEEE Spectrum*, 31(2):22–30.

[Munich and Perona 1998] Munich, M. E. and Perona, P. (1998). Camera-based ID verification by signatures tracking. *Lecture Notes in Computer Science*, 1406:782.

[Myers and Rabiner 1981] Myers, C. S. and Rabiner, L. R. (1981). A comparative study of several dynamic time-warping algorithms for connected word recognition. *The Bell System Technical Journal*, 60(7):1389–1409.

[Negin et al. 2000] Negin, M., Chmielewski(Jr.), T. A., Salganicoff, M., Camus, T. A., von Seelen, U. M. C., Venetianer, P. L., and Zhang, G. G. (2000). An iris biometric system for public and personal use. *IEEE Computer Society*, 33(2):70–75.

[NIST 2001] NIST (2001). CBEFF - Common Biometric Exchange File Format. Technical Report NISTIR 6529, National Institute of Standards and Technology, USA.

[NIST 2003] NIST (2003). NIST year 2003 speaker recognition evaluation plan. Technical report, NIST Speech Group. `http://www.nist.gov/speech/tests/spk/2003/doc/2003-spkrec-evalplan-v2.2%.pdf`.

[NIST 2005] NIST (2005). NIST special database 4 - NIST 8-bit gray scale images of fingerprint image groups (FIGS). `http://www.nist.gov/srd/nistsd4.htm`. Acessado em julho/2006.

[Nordin 2004] Nordin, B. (2004). *Match-on-Card Technology*. Precise Biometrics Inc., /urlhttp://www.precisebiometrics.com. Acessado em julho/2006.

[OASIS 2003] OASIS (2003). XCBF - XML Common Biometric Format. Technical report, Organization for the Advancement of Structured Information Standards. `http://www.oasis-open.org/committees/xcbf/`.

[Osborne and Ratha 2003] Osborne, M. and Ratha, N. K. (2003). A JC-BioAPI compliant smart card with biometrics for secure access control. *Lecture Notes in Computer Science*, 2688:903–910.

[Patrick 1972] Patrick, E. A. (1972). *Fundamentals of Pattern Recognition*. Prentice-Hall Inc.

[Phillips et al. 2000] Phillips, P., Martin, A., Wilson, C., and Przybocki, M. (2000). An introduction to evaluating biometric systems. *IEEE Computer*, 33(2):56–63.

[Phillips et al. 2002] Phillips, P. J., Sarkar, S., Robledo, I., Grother, P., and Bowyer, K. (2002). The gait identification challenge problem: Data sets and baseline algorithm. In *International Conference on Pattern Recognition*, volume 01, pages 385–388, Los Alamitos, CA, USA. IEEE Computer Society.

[Prokoski and Riedel 1999] Prokoski, F. J. and Riedel, R. (1999). Infrared identification of faces and body parts. In Jain, A. K., Bolle, R. M., and Pankanti, S., editors, *Biometrics: Personal Identification in Networked Society*, chapter 9. Kluwer Academic Publishers, Boston, MA, USA.

[Przybocki and Martin 2004] Przybocki, M. and Martin, A. (2004). NIST speaker recognition evaluation chronicles. Technical report, Speech Group, Information Access Division, Information Technology Laboratory National Institute of Standards and Technology, USA. Published in the Odissey 2004 Conference.

[Putte and Keuning 2000] Putte, T. and Keuning, J. (2000). Biometrical fingerprint recognition: don't get your fingers burned. In *Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289–303.

[Rabiner and Juang 1986] Rabiner, L. R. and Juang, B. H. (1986). An introduction to Hidden Markov Models. *IEEE Magazine on Accoustics, Speech and Signal Processing*, 3(1):4–16.

[Reynolds et al. 2000] Reynolds, D. A., Doddington, G. R., Przybocki, M. A., and Martin, A. F. (2000). The NIST speaker recognition evaluation - overview methodology, systems, results, perspective. *Speech Communications*, 31(2-3):225–254.

[Ross et al. 2006] Ross, A. A., Nandakumar, K., and Jain, A. K. (2006). *Handbook of Multibiometrics*. International Series on Biometrics. Springer.

[Sabourin et al. 1997] Sabourin, R., Genest, G., and Preteux, F. J. (1997). Off-line signature verification by local granulometric size distributions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(9):976–988.

[Sanchez-Reillo et al. 2000] Sanchez-Reillo, R., Sanchez-Avila, C., and Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10):1168–1171.

[Sandstrom 2004] Sandstrom, M. (2004). Liveness detection in fingerprint recognition systems. Linkoping University, Department of Electrical Engineering, Eletronic Press, Student Thesis.

[Scheenstra et al. 2005] Scheenstra, A., Ruifrok, A., and Veltkamp, R. C. (2005). A survey of 3D face recognition methods. In *5^{th} International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*, volume 3546 of *Lecture Notes in Computer Science*, pages 891–899, Rye Brook, NY, USA. Springer-Verlag.

[Schneier 1999] Schneier, B. (1999). Inside risks: the uses and abuses of biometrics. *Communications of the ACM*, 42(8):136.

[Thorpe et al. 2005] Thorpe, J., van Oorschot, P., and Somayaji, A. (2005). Passthoughts: Authenticating with our minds. *Proceedings of the New Security Paradigms Workshop*.

[Turk and Pentland 1991] Turk, M. and Pentland, A. (1991). Face recognition using eigenfaces. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pages 586–591, Maui, HI, USA.

[Uludag and Jain 2004] Uludag, U. and Jain, A. K. (2004). Attacks on biometric systems: A case study in fingerprints. *Proc. SPIE-EI*.

[Valid 2005] Valid (2005). Visual audio lip-motion identification. `http://www.validbiometrics.com`. Acessado em julho/2006.

[Victor et al. 2002] Victor, B., Bowyer, K., and Sarkar, S. (2002). An evaluation of face and ear biometrics. In *International Conference on Pattern Recognition*, volume 1, pages 429–432, Quebec City, Canada. IEEE Computer Society.

[Wayman 1997] Wayman, J. L. (1997). A scientific approach to evaluation biometric systems using mathematical methodology. In *Proceedings of CardTech/SecureTech*, Orlando, FL, EUA.

[Wayman 1999a] Wayman, J. L. (1999a). Error rate equations for the general biometric system. *IEEE Robotics & Automation Magazine*, 6(1):35–48.

[Wayman 1999b] Wayman, J. L. (1999b). National biometric test center collected works. Technical report, National Biometric Test Center, San Jose, California, USA.

[Yeung et al. 2004] Yeung, D.-Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., and Rigoll, G. (2004). SVC2004: First international signature verification competition. In *1st International Conference on Biometric Authentication (ICBA)*, volume 3072 of *Lecture Notes in Computer Science*, pages 16–22, Hong Kong, China. Springer-Verlag.

[Yu et al. 1995] Yu, K., Mason, J., and Oglesby, J. (1995). Speaker recognition using Hidden Markov Models, Dynamic Time Warping and Vector Quantisation. *IEE Proceedings – Vision, Image and Signal Processing*, 142:313–318.

[Zhang and Shu 1999] Zhang, D. and Shu, W. (1999). Two novel characteristic in palmprint verification: Datum point invariance and line feature matching. *Pattern Recognition*, 32(4):691–702.

[Zhao et al. 2003] Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys*, 35(4):399–458.

[Zunkel 1999] Zunkel, R. L. (1999). Hand geometry based verification. In Jain, A. K., Bolle, R. M., and Pankanti, S., editors, *Biometrics: Personal Identification in Networked Society*, chapter 4, pages 87–101. Kluwer Academic Publishers, Boston, MA, USA.