LUCIANO COSTA

UM MODELO DE AUTENTICAÇÃO BIOMÉTRICA PARA *WEB BANKING*

FLORIANÓPOLIS
2007

UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROGRAMA DE PÓS-GRADUAÇÃO
EM ENGENHARIA ELÉTRICA

UM MODELO DE AUTENTICAÇÃO BIOMÉTRICA PARA *WEB BANKING*

Dissertação submetida à
Universidade Federal de Santa Catarina
como parte dos requisitos para a
obtenção do grau de Mestre em Engenharia Elétrica.

LUCIANO COSTA

Florianópolis, março de 2007.

UM MODELO DE AUTENTICAÇÃO BIOMÉTRICA PARA *WEB BANKING*.

Luciano Costa

‘Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica, Área de Concentração em *Automação e Sistemas*, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina.’

_____

Joni da Silva Fraga, Dr
Orientador

_____

Nelson Sadowski, Dr.
Coordenador do Programa de Pós-Graduação em Engenharia Elétrica

Banca Examinadora:

_____

Joni da Silva Fraga, Dr.
Presidente

_____

Rafael Rodrigues Obelheiro, Dr.

_____

Jean-Marie Farines, Dr.

_____

Carlos Barros Montez, Dr.

_____

Frank Augusto Siqueira, PhD.

À Dona Tita

AGRADECIMENTOS

Agradeço a quem me orientou, me apoiou e me defendeu.

Resumo da Dissertação apresentada à UFSC como parte dos requisitos necessários para obtenção do grau de Mestre em Engenharia Elétrica.

UM MODELO DE AUTENTICAÇÃO BIOMÉTRICA PARA *WEB BANKING*

Luciano Costa

Março/2007

Orientador: Joni da Silva Fraga, Dr.
Área de Concentração: Automação e Sistemas
Palavras-chave: Biometria, Sistemas Biométricos, Serviços Web

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. O canal de atendimento *web banking* tem sido alvo de freqüentes ataques que levam a fraudes, o que exige reforço na autenticação de clientes. As credenciais tradicionais de conhecimento e posse apresentam algumas deficiências que podem ser supridas pela autenticação biométrica. Apresentamos um modelo de implementação para autenticação biométrica em sistemas de *web banking*. O modelo se utiliza da tecnologia de Serviços Web, que se caracteriza pela interoperabilidade e facilidade de integração para os sistemas legados. A aplicabilidade do modelo é verificada através de um protótipo.

Abstract of Dissertation presented to UFSC as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering.

A BIOMETRIC AUTHENTICATION MODEL FOR WEB BANKING

Luciano Costa

March/2007

Advisor: Joni da Silva Fraga, Dr.
Area of Concentration: Automation and Systems
Keywords: Biometrics, Biometric Systems, Web Services

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 problems. The web banking channel has frequently been the target of attacks leading to banking fraud, making it necessary to reinforce user authentication mechanisms. The traditional credentials of knowledge and possession show some deficiences that can be solved by biometric authentication. We present an implementation model for biometric authentication in web banking systems. The model uses the Web Services technology, which is characterized by its interoperability and easy integration to legacy systems. The applicability of the model is verified by means of a prototype.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 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 *autenticidade*, que garante a validade de dados ou de entidades, 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, que é o procedimento que garante a autenticidade, pode ser subdividida em autenticação de dados e autenticação de entidades. A autenticação de entidades 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 relativamente secreto, 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.

As credenciais de conhecimento e posse possuem limitações, pois podem ser observadas, esquecidas ou perdidas. Além disso, elas não permitem vincular com suficiente grau de certeza uma transação

ao indivíduo que a realiza. A autenticação biométrica é capaz de contornar essas deficiências: ela caracteriza unicamente um indivíduo e não pode ser esquecida ou perdida. O uso adequado de credenciais biométricas, possivelmente em conjunto com credenciais de conhecimento ou posse, pode aumentar significativamente a segurança da autenticação de usuários. A autenticação baseada em características biométricas se mostra uma alternativa promissora e que vem despertando grande interesse de fabricantes, desenvolvedores, empresas e usuários finais. No entanto, ainda não é uma tecnologia consolidada, e sua utilização ainda precisa ser melhor estudada, principalmente a sua inclusão em sistemas que exigem alto grau de confiança mesmo em plataformas heterogêneas e distribuídas, como é o caso de sistemas de *web banking*.

O *web banking*, que alia conveniência para os clientes e baixo custo para o banco, destaca-se dentre os canais de atendimento oferecidos pelos bancos de varejo. O número de transações bancárias pela *web* já supera o de transações realizadas nos caixas tradicionais. Apesar da grande utilização, o uso do canal *web* está sujeito a uma série de riscos, o que leva a grandes investimentos no sentido de melhorar a sua segurança. Um dos aspectos de segurança que tem recebido maior atenção é a autenticação dos usuários, um dos mais freqüentes alvos de fraudes bancárias. Como os mecanismos tradicionalmente adotados para autenticação em sistemas de *web banking* são credenciais de conhecimento e de posse, estão suscetíveis aos problemas citados no parágrafo anterior. A utilização de um processo de autenticação de usuários por meio de tecnologia biométrica em sistemas de *web banking* mostra-se como alternativa bastante interessante, contudo sua inclusão em tais sistemas ainda não foi suficientemente discutida.

1.1 Motivação

A tecnologia de autenticação com base em credenciais biométricas tem sofrido relativo crescimento devido às pesquisas efetuadas para desenvolvimento de novas características biométricas e para desenvolvimento de algoritmos de extração e comparação eficientes e que proporcionem desempenho aceitável. O canal de atendimento *web banking* tem se tornado bastante popular, no entanto, está sujeito a fraudes e necessita de reforço de segurança. A biometria pode proporcionar reforço de segurança na autenticação de usuários de *web banking*, vencidos os empecilhos das vulnerabilidades dos sistemas biométricos e da diversidade da plataforma de TI das instituições bancárias. A introdução de novas funcionalidades em um ambiente de plataforma heterogênea pode ser facilitada com a utilização de Serviços Web.

1.2 Objetivos

O objetivo geral desta dissertação é analisar a utilização de autenticação biométrica em instituições financeiras de grande porte, particularmente em sistemas de *web banking*. Esse objetivo geral pode ser desdobrado nos seguintes objetivos específicos:

1. Fazer um amplo estudo bibliográfico de sistemas de autenticação biométrica e das principais tecnologias utilizadas;

2. Propor um método de avaliação e seleção de tecnologias biométricas;

3. Propor uma arquitetura para autenticação biométrica em sistemas de *web banking*.

1.3 Organização do Texto

O capítulo 2 apresenta os principais conceitos envolvendo sistemas biométricos: quais são os modos de autenticação usando biometria, requisitos de características biométricas, algumas 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 que se encontram em um estágio de desenvolvimento bastante satisfatório. Essas tecnologias são examinadas mais detidamente. São apresentadas 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. Na discussão sobre a arquitetura de segurança, são mostradas suas vulnerabilidades específicas, bem como contramedidas que podem ser usadas para contornar ou minimizar essas vulnerabilidades.

O capítulo 3 demonstra que a tecnologia biométrica mais adequada depende dos requisitos da aplicação. Este capítulo apresenta uma metodologia simples para seleção da tecnologia biométrica mais adequada para uma dada aplicação. Num primeiro passo, são apresentados os padrões de avaliação de desempenho de um sistema biométrico quanto ao seu item mais característico, que é a precisão, ou seja, a estimativa das taxas de falsa aceitação e falsa rejeição. Num segundo passo, é apresentada uma matriz de avaliação de conformidade das características biométricas aos requisitos da aplicação.

O capítulo 4 discute um estudo de caso. Neste capítulo, descrevemos o ambiente computacional bancário com ênfase nos sistemas de *web banking*, apresentamos a tecnologia de Serviços Web e os padrões usados para garantir segurança nessa tecnologia, apresentamos o nosso modelo para autenticação biométrica em sistemas de *web banking* e discutimos a sua implementação por meio de um protótipo.

Finalmente, o capítulo 5 discute os principais problemas que permanecem abertos na área de biometria, apresenta as conclusões do trabalho e algumas considerações finais.

Capítulo 2

Biometria

As características biométricas da voz e da face são utilizadas há muito tempo na autenticação entre pessoas. Com o advento da civilização, escrita e relações comerciais, a assinatura manuscrita proporcionou reforço para a autenticação. Impressões palmares já eram usados no séc. XIV, na China, conforme relatos do explorador João de Barros. Ele observou que, para distinguir suas crianças de outras, mercadores chineses estampavam impressões palmares das mesmas em papel com tinta. Na década de 1890, Alphonse Bertillon, um antropologista e policial francês propôs um método de autenticação de condenados por meio de várias medidas das proporções do corpo [Tarbell 2005] [Rhodes 1956]. Este método (Bertillonage) foi usado por autoridades policiais pelo mundo afora, até que o mesmo falhou.

Depois disso, a polícia passou a usar impressões digitais, um método então estruturado pela Scotland Yard. Em 1893, o Ministério do Interior da Inglaterra aceitou o fato de que dois indivíduos não teriam as mesmas impressões digitais, iniciando uma cadeia de eventos que levou ao primeiro sistema automático de identificação por meio de impressão digitais (AFIS) em 1960. Nas últimas três décadas, a biometria automatizada cresceu de um único método (impressão digital) para mais de dez métodos diferentes. Existem fabricantes de sensores às centenas e os preços para os dispositivos vêm caindo, tornando os sistemas viáveis para orçamentos baixos e médios. Há dezenas de companhias envolvidas com novos métodos e, assim como cresce a indústria e o interesse acerca de tais sistemas, cresce também a preocupação pública com questões de privacidade. Leis e regulamentos continuam a ser escritos e padrões são desenvolvidos e propostos. Embora nenhuma outra tecnologia biométrica tenha ainda alcançado a abrangência da impressão digital, algumas delas estão começando a ser usadas em áreas legais e de negócios.

A identificação de seres humanos tem sido crucial para as relações sociais. Conseqüentemente, a identificação de pessoas é parte integral da infra-estrutura necessária para diversos setores de negócios, como finanças, saúde, transporte, entretenimento, segurança publica, entre outros [Jain et al. 2004]. À medida que nossa sociedade se torna eletronicamente conectada para formar uma grande comunidade global, tem se tornado cada vez mais frequente a necessidade de realizar a identificação remota de pessoas, através de meios automatizados. Representações substitutas de identidade como senhas (prevalecentes em controle de acesso eletrônico) e cartões (prevalecentes em aplicações bancárias e

governamentais) não são totalmente suficientes. Afinal, senhas e cartões podem ser compartilhadas e então, em última análise, não podem prover a não-repudiação. Biometria, que se refere à identificação automática de pessoas, baseada na sua fisiologia (p.ex. face, digital, íris, mão) e comportamento (p.ex. voz, assinatura, modo de andar), deveria ser um componente essencial de qualquer solução efetiva de identificação de pessoas, porque os identificadores biométricos não podem ser compartilhados (emprestados), e então eles representam intrinsecamente a identidade do indivíduo. Conseqüentemente, biometria não é somente um importante problema de pesquisa de reconhecimento de padrões, mas é também uma tecnologia capaz de tornar nossa sociedade mais segura, reduzir fraudes e proporcionar conveniência para o usuário.

A biometria envolve o uso de partes do corpo do indivíduo (como impressões digitais ou face) ou comportamentos do indivíduo (como o modo de andar ou a assinatura) como uma forma de autenticação do mesmo. Praticamente todos os sistemas funcionam registrando previamente a característica escolhida em um repositório. Posteriormente, quando a autenticação se torna necessária, o sistema obtém novamente a característica biométrica e compara com o registro armazenado. Este capítulo expõe os conceitos básicos relacionados aos sistemas biométricos em geral e apresenta algumas das tecnologias mais utilizadas.

2.1 Conceitos

Esta seção apresenta os dois principais modos de autenticação em que podem ser usados os sistemas biométricos, faz um apanhado das diferentes tecnologias biométricas existentes, traça um panorama das aplicações que se valem de biometria, apresenta um modelo genérico de um sistema biométrico de autenticação, apresenta os principais tipos de erros nos quais os sistemas podem incorrer, discute alguns padrões utilizados, considera as formas de distribuição dos dados e processos e discute as vulnerabilidades de segurança dos sistemas biométricos em geral.

2.1.1 Autenticação

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 consiste em 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. Os diagramas de blocos destes dois modos podem ser apreciados na Figura 2.1.

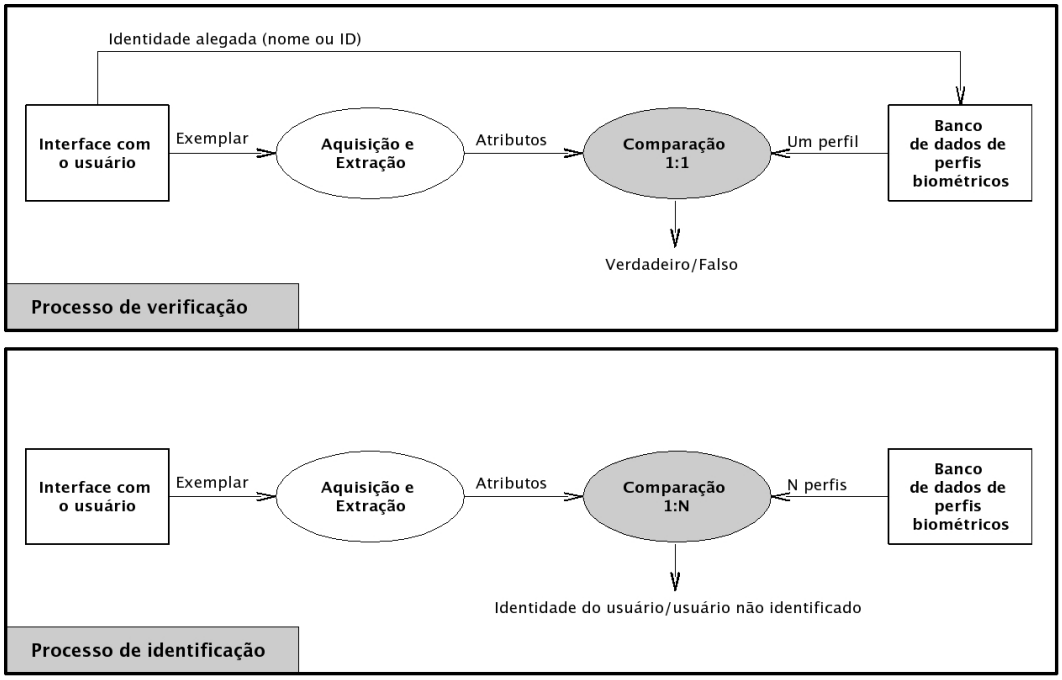


Figura 2.1: Diagrama de blocos ilustrativo dos processos de verificação e identificação. A verificação é uma busca fechada (1:1) e a identificação é uma busca aberta (1:N).

2.1.2 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, a característica pode não estar disponível para toda a população, como é o caso de deficientes físicos.

- **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 apresen-

tar maior ou menor grau de unicidade, mas nenhuma delas pode ser considerada absolutamente única para cada indivíduo.[1]

- **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 e as mais utilizadas atualmente estão listadas na tabela 2.1.

Tecnologia	Utilização
Impressão Digital	52%
Face	16%
Íris	12%
Voz	10%
Mão	6%
Assinatura	3%

Tabela 2.1: Utilização proporcional das principais tecnologias biométricas[BITE 2005].

As diversas tecnologias biométricas existentes são geralmente classificadas, por conveniência, em dois grupos (figura 2.2). 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 2.2.

Outras características estáticas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa. Entre várias outras, podemos citar 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 odor do corpo [Korotkaya 2003], o padrão da arcada dentária [Chen and Jain 2005], o padrão de calor do corpo ou de partes dele

[1] 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.

[Prokoski and Riedel 1999], o formato 3D dos dedos da mão [Woodard and Flynn 2005], o padrão da linha de contorno da silhueta da mão [Yörük et al. 2006], o padrão de reverberação sonora na cavidade do ouvido [Akkermans et al. 2005] e o padrão vascular de várias partes do corpo, como o padrão vascular da retina [Hill 1999] e o padrão vascular das costas da mão [Lin and Fan 2004].

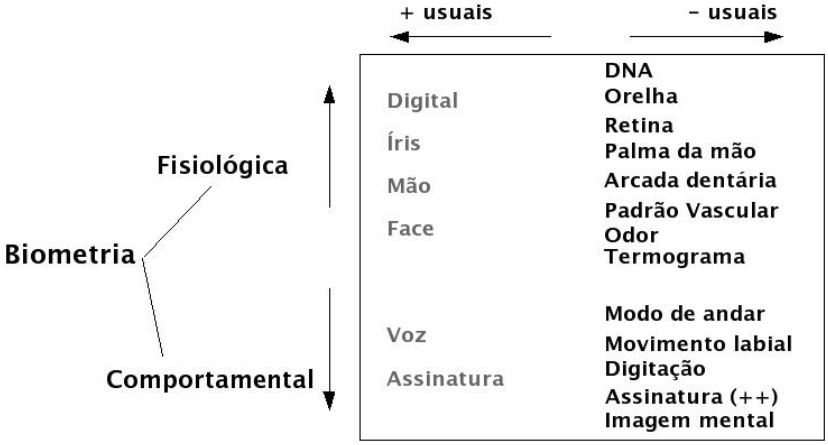


Figura 2.2: As seis características biométricas mais comuns e outras, que são usadas com menor frequência ou que estão em estágios iniciais de pesquisa. As características fisiológicas (estáticas) dependem principalmente da carga genética e as comportamentais (ou dinâmicas) dependem ainda fortemente 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 2.2.

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], vídeo da assinatura [Fink et al. 2001] e imagens mentais (*pass-thoughts*) [Thorpe et al. 2005].

É desejável que as características biométricas apresentem uma boa relação de ponderação de contexto (*contextual weighting*). Esta relação é a razão entre a variação inter-classe e a variação intra-classe [Turney 1993]. Assim, uma relação de ponderação de contexto é grande quando uma característica varia bastante através das fronteiras de classe, mas varia pouco dentro da própria classe, sugerindo então que esta característica pode ser boa para o processo de classificação. Este conceito é ilustrado na figura 2.3. Sejam $I_1, I_2, ..., I_n$ os diversos indivíduos pertencentes a uma população. Sejam $A_1, A_2, ..., A_m$ as diversas amostras colhidas de uma determinada característica dos indivíduos e sejam $S_{11}, S_{12}, ..., S_{nm}$ os diversos valores das características obtidos. Então, no nossso exemplo, a variação intra-classe representaria a variação entre diversas amostras do mesmo indivíduo. Já a variação inter-classe representaria a variação entre diversas amostras de indivíduos diferentes. O grau de universalidade indica que proporção de indivíduos possui a característica escolhida para ser amostrada. O grau de unicidade representa quão grande é a variação inter-classe. O grau de permanência

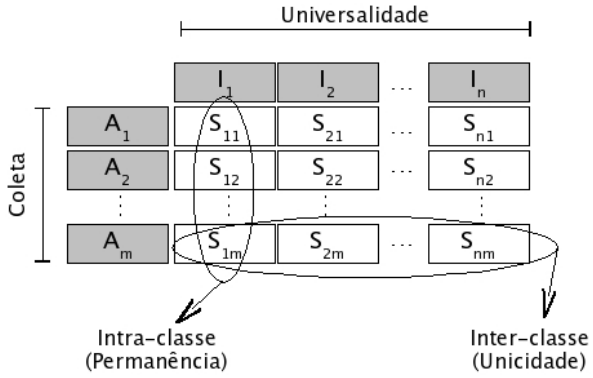


Figura 2.3: É desejável que as características biométricas apresentem uma boa relação de ponderação de contexto, que é a razão entre a variação inter-classe e a variação intra-classe .

representa quão pequena é a variação intra-classe. O grau de coleta indica a viabilidade técnica de coleta de amostras e o grau de aceitação indica quão baixa é a rejeição do indivíduo ao processo de amostragem.

2.1.3 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].

Dentre os diversos conjuntos possíveis, dependendo do refinamento, apresentamos a classificação de alto nível de sete grupos presente no relatório BITE Market Report [BITE 2005]. A projeção do montante de negócios envolvendo tecnologias biométricas para o ano de 2005 era da ordem de 1,9 bilhões de dólares [BITE 2005].

1. **Controle de acesso e atendimento** - Uso da biometria para identificar ou verificar a identidade de um indivíduo que acessa uma área, tipicamente um edifício, um andar ou uma sala. A biometria complementa ou substitui mecanismos de autenticação como chaves, fichas, cartões e crachás. Controle de acesso e atendimento restringem ou registram a presença de um indivíduo.

2. **Identificação Civil** - Uso da biometria para identificar ou verificar a identidade de um indivíduo que interage com uma agência governamental como um cidadão legalmente capaz. A biometria complementa ou substitui processos como fornecimento de documentos, assinaturas, provas e certidões. Este grupo engloba emissão de documentos de identidade, verificação de antecedentes, imigração, aplicações de controle alfandegário e serviços sociais

3. **Identificação Criminal** - Uso da biometria para identificar ou verificar a identidade de um suspeito, detido, ou indivíduo em uma aplicação legal ou de combate ao crime. O papel principal da biometria é identificar um indivíduo de modo a iniciar ou interromper um processo de

aplicação da lei. A utilização de tecnologias biométricos tem se mostrado bastante efetiva neste grupo de aplicações.

4. **Autenticação telefônica e comércio eletrônico** - O uso da biometria para identificar ou verificar a identidade de um indivíduo que conduz transações remotas com vistas a mercadorias ou serviços. A biometria complementa ou substitui processos como fornecimento de senhas, impostação de PIN's, interação desafio-resposta. O comércio eletrônico e telefonia estão agrupados pela similaridade de elementos transacionais e interação não supervisionada.

5. **Segurança de redes e de computadores** - O uso da biometria para identificar ou verificar a identidade de um indivíduo que acessa computadores, redes, *intranets*, recursos de rede e aplicações. A biometria complementa ou substitui processos como apresentação de senhas e *tokens*. A segurança de redes e de computadores assemelha-se ao controle de acesso lógico tradicional, mas este grupo em separado significa que o faturamento é baseado principalmente em licenciamento e vendas, em oposição à interação transacional.

6. **Autenticação em pontos de atendimento e de vendas** - O uso da biometria para identificar ou verificar a identidade de um indivíduo consumidor conduzindo transações em pessoa. A biometria complementa ou substitui processos como identificação baseada em fotografias, entrada de PIN's ou impostação de assinaturas em papel. O que caracteriza este grupo é a existência de elementos transacionais e o requisito do indivíduo estar presente num local específico de atendimento (como um terminal bancário de auto-atendimento) ou venda (como um POS, ou *point of sale*) .

7. **Vigilância e filtragem** - O uso da biometria para identificar um indivíduo presente em ou se movendo através de uma dada área. A biometria complementa ou substitui processos como vigilância através de câmera. A vigilância assume um usuário não-cooperativo e a filtragem assume um usuário cooperativo, mas ambas buscam em um banco de dados de indivíduos de interesse na intenção de localizar potenciais coincidências.

De uma maneira prática, as aplicações dos nichos Governamental, Comercial e Forense (conhecida como classificação vertical - tabela 2.2) podem ser classificadas por finalidade (classificação horizontal - tabela 2.3).

Nicho	Utilização
Governamental	36%
Comercial	36%
Policial	28%

Tabela 2.2: Distribuição vertical das principais aplicações biométricas[BITE 2005].

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 atendimento e de vendas	4 %
Autenticação telefônica e comércio eletrônico	3 %
Vigilância e filtragem	3 %

Tabela 2.3: Distribuição horizontal (por finalidade) das principais aplicações biométricas [BITE 2005]

2.1.4 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 um sistema deste tipo, apresentado na figura 2.4, 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.

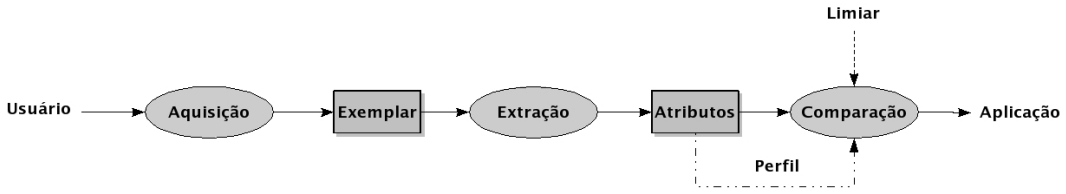


Figura 2.4: Um modelo simples de sistemas biométrico.

- *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 as características biométricas do usuário para cadastramento no sistema. O *perfil biométrico* obtido, ou *template*, é armazenado para uma comparação posterior. A linha pontilhada na figura 2.4 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.

2.1.5 Erros

Ao longo do tempo, diferentes definições dos erros associados aos sistemas biométricos foram criados. Consequentemente, há muita terminologia para expressar a precisão de uma aplicação [Bolle et al. 2004, p. 65]. O que é bastante claro e aceito pela comunidade biométrica em geral 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. Esta seção apresenta a terminologia mais comumente aceita.

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).

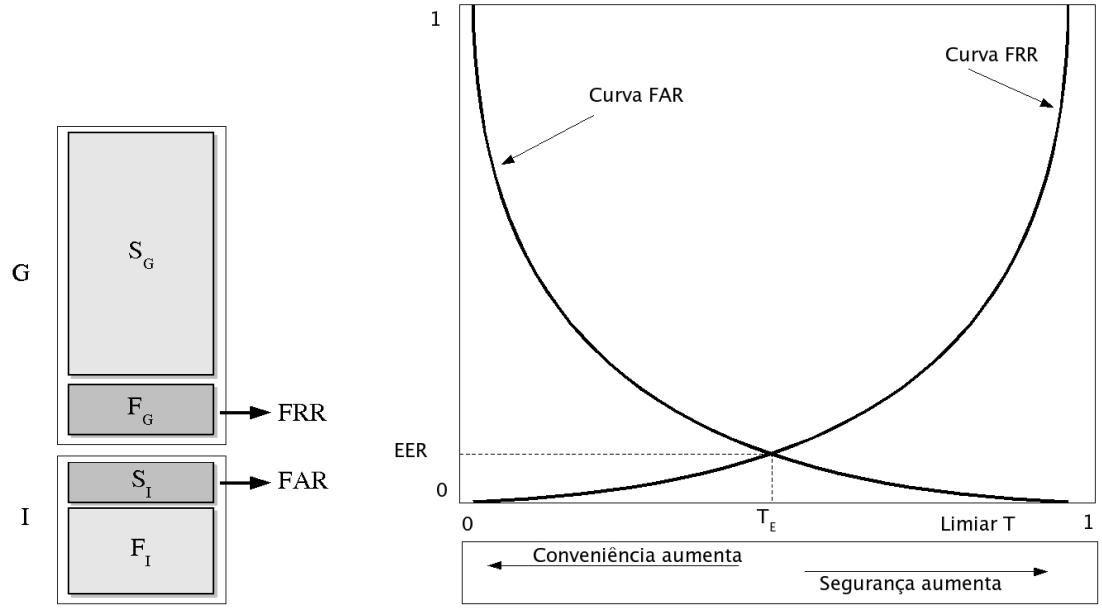
- *False Non-Match* (FNM) - Erro do tipo II - Decidir que dois exemplares não são do mesmo indivíduo enquanto na realidade eles pertencem ao mesmo indivíduo. A freqüência com a qual este erro ocorre é chamada *False Non-Match Rate* (FNMR).

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).

A figura 2.5(a) ajuda a esclarecer como são calculadas as taxas FAR e FRR. Em um sistema biométrico hipotético, ocorrem G tentativas de acesso de usuários genuínos com S_G sucessos e F_G falhas. Além disso, acontecem I tentativas de acesso de usuários impostores, com S_I sucessos e F_I falhas. Cada tentativa produz sucesso ou fracasso. Assim, $G = S_G + F_G$ e $I = S_I + F_I$ e as taxas são calculadas por $FAR = \frac{S_I}{I}$ e $FRR = \frac{F_G}{G}$.



(a) Como calcular as taxas FAR e FRR.

(b) As curvas típicas das taxas de erro FAR e FRR.

Figura 2.5: Modo de cálculo das taxas FAR e FRR (figura 2.5(a)). As taxas de erro FAR e FRR mostram que o sistema pode operar nas faixas de "conveniência" ou de "segurança", conforme a calibração do limiar (figura 2.5(b)).

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*, em relação ao limiar T configurado para o sistema, como apresentado na figura 2.5(b). 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 $\mathrm{FAR}(T) = \mathrm{FRR}(T)$. Este ponto é conhecido como ponto de operação EE (*Equal Error*), ao qual também está associado uma taxa EER (*Equal Error Rate*).

As taxas $\mathrm{FAR}(T)$ e $\mathrm{FRR}(T)$ também podem ser comparadas *uma contra a outra* para produzir uma curva bidimensional característica conhecida por *Receiver Operating Characteristic* (ROC).

Um exemplo hipotético pode ser apreciado na figura 2.6. 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 2.6. 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.

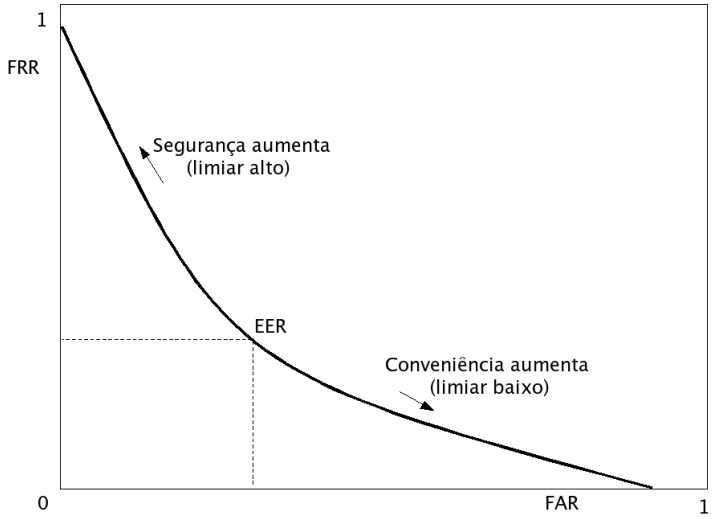


Figura 2.6: *Receiver Operating Characteristic*. As taxas de erro FAR e FRR podem ser plotadas uma contra outra numa curva bi-dimensional. Aqui tentamos mostrar a solução de compromisso entre segurança e conveniência.

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 2003b] [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 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 auto-atendimento de um banco, no qual *FR*'s não são aceitáveis por falta de pessoal de suporte, mas *FA*'s podem ser toleradas, já que existiria uma segunda fase de autenticação por senha.

2.1.6 Padrões

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 2.7 e descritos resumidamente nos parágrafos a seguir.

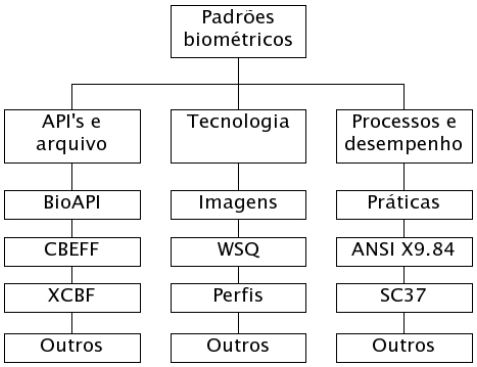


Figura 2.7: Principais esforços de padronização relacionados a sistemas biométricos

BioAPI O consórcio BioAPI [BioAPI 2001] 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 [NIST 2002], 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.

ISO 19092 Este é um padrão ainda em construção que estende e internacionaliza o padrão ANSI X9.84. Acrescenta características solicitadas pela comunidade internacional de serviços financeiros,

como auditoria, gerenciamento de perfis, instruções práticas, entre outras. A primeira parte (*security framework*) descreve controles e procedimentos para o uso de biometria como mecanismo de autenticação, descreve os requisitos de segurança físicos de dispositivos biométricos, o conteúdo mínimo de uma política biométrica (BP) e instruções práticas (BPS). O padrão pretende ainda acrescentar a segunda parte, que trata de sintaxe de mensagens e requisitos criptográficos [ISO 2006].

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.

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*), proporcionando taxas de compressão de cerca de 15:1 [NIST 1999].

PIDS CORBA *Object Services* são serviços de propósito geral que proporcionam interoperabilidade entre aplicações. São peças fundamentais para o desenvolvimento de aplicações baseadas em CORBA, pois podem ser usados para construir funcionalidades de nível mais alto, que ainda mantenham interoperabilidade através de múltiplos ambientes. Existe pelo menos um serviço CORBA padronizado cujo objetivo é gerenciar credenciais de identificação de pessoas. Embora um tal serviço seja necessário em outros domínios que simplesmente a saúde, ele foi padronizado na partição CORBA *Healthcare* como PIDS, ou *Person Identification Service Specification* [PIDS 2001]. Esta especificação define as interfaces de um serviço CORBA que organiza a funcionalidade de gerenciamento de ID's de pessoas. O serviço foi projetado para:

- Suportar o registro de ID's (chamados ID Values) dentro de um domínio e entre domínios (chamados ID Domain).
- Suportar busca e comparação de pessoas.
- Suportar federações de serviços PIDS independentes de topologia.
- Permitir a proteção da confidencialidade das pessoas sob uma larga variedade de políticas de confidencialidade e mecanismos de segurança.

- Permitir interoperabilidade de serviços PIDS *plug-and-play*.
- Definir os níveis de conformidade apropriados para vários graus de sofisticação, variando do nivel pequeno (*query-only single ID Domains*) ao grande (*large federated correlating ID Domains*).

Outros A *International Association for Biometrics* (iAfB) procura promover um glossário de termos relacionados à biometria [iAfB 2007]. Outra associação comercial, a IBIA [IBIA 2006] procura representar a indústria biométrica, no debate sobre a utilização de tais tecnologias. Aberta a companhias fabricantes, integradoras e usuários finais, procura educar os formadores de opinião e legisladores sobre as possibilidades de utilização da biometria e suas aplicações de segurança. Quanto ao *Biometric Consortium* [BC 2006], aglomera departamentos governamentais, fabricantes e instituições de pesquisa. Serve como ponto focal para o governo americano, em assuntos de pesquisa, desenvolvimento, avaliação e aplicação de sistemas baseados em biometria. Trabalha em parceria com o laboratório de tecnologia da informação e o laboratório de biometria e *smart cards* do NIST, e com o *National Biometric Test Center* da *San Jose University*.

2.1.7 Armazenamento dos Perfis Biométricos

2.1.7.1 Abordagens de Armazenamento

Existem várias possibilidades de distribuição dos processos e dados 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. No outro extremo, podemos ter uma 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 armazenada em um 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 arquitetura do sistema. Estes processos podem ser locais (junto ao dispositivo de aquisição) ou remotos (em servidor ou até mesmo no próprio *smart card*).

Mesmo existindo diversas possibilidades de distribuição, é útil examinar a organização destes sistemas em seus extremos, correspondentes à decisão de armazenamento dos perfis biométricos, quais sejam: abordagem centralizada e abordagem distribuída.

Na **abordagem centralizada**, os perfis biométricos são colecionados em um banco de dados e ficam em poder da empresa proprietária do sistema. O caso típico da abordagem centralizada é o

armazenamento remoto, que corresponde ao armazenamento em um servidor com uma base de dados centralizada. Esta solução é adequada para aplicações nas quais 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.

Um caso especial da abordagem centralizada é o armazenamento local, que 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.

Na **abordagem distribuída**, o armazenamento dos perfis se dá 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.

Independentemente da abordagem utilizada, o tamanho do perfil, o número de perfis armazenados por usuário e a disponibilidade de mecanismos de compressão determinam a capacidade de armazenamento necessária. Quando o tamanho dos perfis é grande e os perfis são armazenados em uma base de dados central, a capacidade de banda da rede pode se tornar um gargalo para o sistema. O tempo necessário para um sistema biométrico tomar uma decisão também pode se tornar essencial em sistemas de controle de acesso, como uma aplicação bancária remota, por exemplo.

2.1.7.2 Cenários de Utilização

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 diretos e agentes delegados. Um **agente direto** 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 delegado**, 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 direto seria um banco que decide usar biometria para autenticar seus próprios clientes, e um exemplo de agente delegado 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 2.4 mostra os cenários derivados das diferentes combinações possíveis entre agentes de armazenamento e dispositivos de aquisição. No cenário chamado “pioneiro” (com agente direto e dispositivo administrado), temos a figura de um agente direto que registra cada usuário e armazena o perfil para uso posterior, quando o usuário desejar fazer uma transação. Além disso, o agente instala e gerencia a infra-estrutura necessária para os dispositivos 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 direto 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 direto	Cenário Pioneiro	Cenário Temerário
Agente delegado	Cenário Organizado	Cenário Audacioso

Tabela 2.4: Cenários possíveis ao se combinar os dispositivos de aquisição (administrados ou livres) e agentes de armazenamento (diretos ou delegados)

No cenário dito “temerário” (com agente direto e dispositivo livre), temos a figura de um agente direto que registra cada usuário e cada dispositivo. Este é um cenário considerado ainda improvável atualmente, pois o agente direto 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 ofereça acesso aos usuários por meio de seus telefones celulares.

No cenário considerado “organizado” (com agente delegado e dispositivo administrado), temos a figura de um agente delegado 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 delegado 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, pois pode ser compartilhado por todas as entidades beneficiárias que o utilizam. No entanto, as entidades integrantes dependem da infra-estrutura do agente delegado. 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 possam ter sido adulterados para capturar as características biométricas para utilização posterior.

No quarto cenário, batizado de "audacioso" (com agente delegado e dispositivo livre), o agente delegado 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. As entidades beneficiadas mantêm a diminuição de seus custos pelo compartilhamento dos mesmos, mas o usuário tem o inconveniente de ter de carregar consigo o dispositivo.

2.1.8 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.

Os sistemas biométricos em geral ainda não foram suficientemente atacados, no sentido de não terem sido submetidos a sérias tentativas efetuadas por criminosos sofisticados fortemente financiados. Ainda assim, vários padrões de **taxonomia de ataques** a sistemas biométricos foram apresentados. Os mais importantes são:

1. *UK Government Biometric Device Protection Profile* (BDPP) [BWG 2001].

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 Robustness Environments* (USGovPP) [Kong et al. 2003].

4. *Germany DIN framework for security evaluation and testing of biometric technology* (ISO 3806) [DIN 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.

- *Vulnerabilidades nos canais entre os processos* - Em muitos sistemas reais, alguns módulos do sistema podem estar fisicamente distantes entre si. Em tais sistemas, os canais de comunicação entre os processos podem constituir vulnerabilidades importantes. Após a obtenção de dados sensíveis, 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. 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 usuários 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 dos dados biométricos como ferramenta de segurança. Afinal, a possibilidade de dois exemplares biométricos serem exatamente iguais é desprezível. 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 sumárias ou ocultação dos dados (*hiding data*) servem para evitar ataques *hill-climbing*. Assim, o sistema deve fornecer apenas uma resposta negativa ao usuário não autenticado, abstendo-se de explicar qual o motivo da recusa e abstendo-se principalmente 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. Por exemplo, em sistemas de autenticação baseados no padrão da voz, o usuário pode ter de ler um texto apresentado ou responder a uma pergunta colocada pelo sistema.

- 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.

2.1.8.1 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 2.8:

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 2.8):

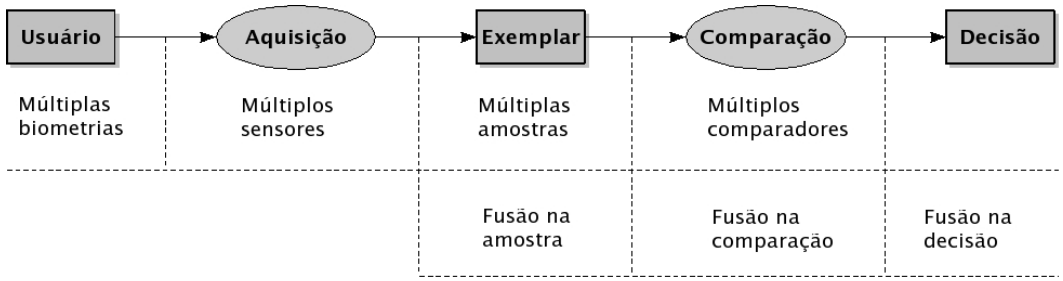


Figura 2.8: Dentro do processo genérico de um sistema biométrico, há diversos pontos para obter multiplicidade e há diversos pontos para efetuar a fusão.

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

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

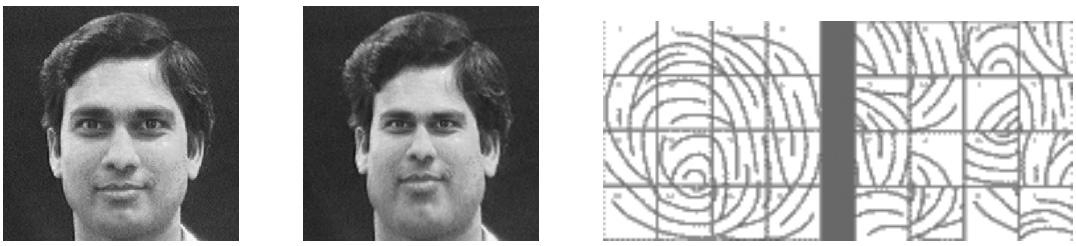
3. Fusão na decisão, ou seja, as diversas decisões obtidas são combinadas para produzir uma única decisão.

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].

2.1.8.2 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 (figura 2.9). 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, como nas figuras 2.9(a) e 2.9(b). 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, como na figura 2.9(c).



(a) Face normal

(b) Face modificada

(c) Permutação de blocos

Figura 2.9: Um exemplo de transformação da imagem 2D da face por meio de uma distorção e um exemplo de transformação da imagem de impressão digital por meio da permutação de blocos.

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 representado por um conjunto de pontos representados por coordenada espaciais $P = (x_i, y_y)$. As coordenadas dos pontos podem ser transformadas através de um mapeamento baseado em polinômios. Como mostra a figura 2.10, 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 podem ser transformadas de modo similar por meio de $Y = G(y)$. 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].

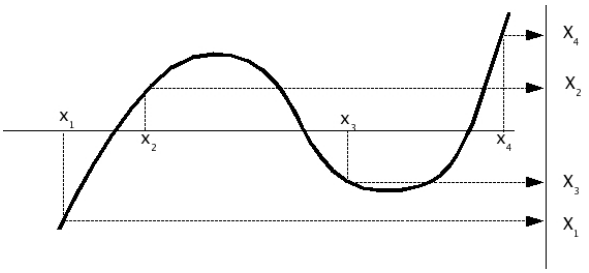


Figura 2.10: Um exemplo de mapeamento de uma das coordenadas de um conjunto de pontos de minúcias em um novo conjunto de coordenadas, por meio de uma transformação irreversível.

2.1.8.3 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 E e a chave privada D. Ora, a chave privada proporciona alta resistência à fraude porque dificulta o ataque de força bruta, devido ao tamanho da chave. A chave privada D 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 fácil de memorizar, 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]. [2]

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. 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

[2] 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].

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 para atualizar o cartão.

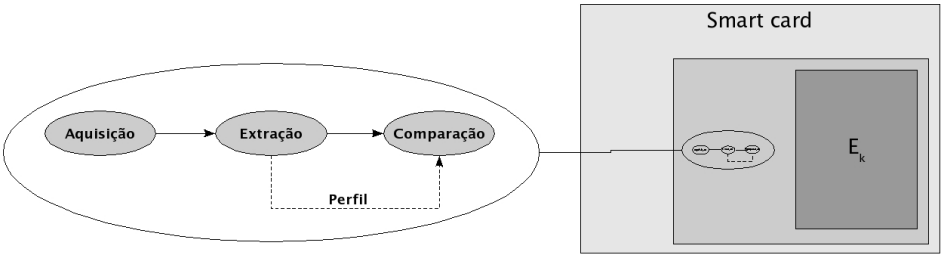


Figura 2.11: Acesso à chave privada por meio de dispositivo de aquisição biométrico embutido no cartão. Quão poderosa é esta ferramenta?

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

2.2 Tecnologias Biométricas

Diversas características biométricas podem ser utilizadas em sistemas de autenticação. Esta seção descreve as seis tecnologias biométricas mais usadas segundo [BITE 2005]. Os identificadores biométricos mais comumente utilizados são (1) impressão digital, (2) aparência da face, (3) padrão da íris, (4) geometria da mão, (5) dinâmica da assinatura e (6) padrão da voz.

2.2.1 Impressão Digital

A tecnologia biométrica de impressão digital possui um longo e interessante histórico. A descoberta de impressões digitais em artefatos arqueológicos evidencia que os povos antigos, notadamente os chineses, estavam cientes da individualidade das mesmas desde há 5.000 anos atrás. Desde o primeiro artigo científico (1684) até sua adoção oficial na Inglaterra (1893), vários avanços na pesquisa levaram à consolidação da idéia da unicidade das impressões digitais. No início do séc. XX, o reconhecimento por impressões digitais era formalmente aceito e tornou-se rotina forense. Os bancos de dados de impressões digitais de criminosos foram estabelecidos e técnicas foram consolidadas. Em 1924, foi criada a divisão de identificação do FBI com um banco de dados de 810.000 cartões de digitais. A rápida expansão da quantidade e tamanho dos bancos de dados exigiram a criação de

sistemas automatizados de análise de impressões digitais, conhecidos como AFIS - *Automatic Fingerprint Identification System*. Estes sistemas melhoram a produtividade operacional das forças policiais e reduzem os custos de contratação e treinamento de especialistas. A tecnologia de reconhecimento automático de digitais se estendeu rapidamente das aplicações forenses para aplicações comerciais. De fato, os sistemas baseados nessa tecnologia são bastante populares, e se tornaram quase sinônimos de biometria.

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 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 o aloritmo WSQ (seção 2.1.6).

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) Arch 5% (b) Loop 65% (c) Whirl 30%

Figura 2.12: Uma classificação básica do formato geral das linhas de impressões digitais em três grupos. Existem outras classificações mais minuciosas.

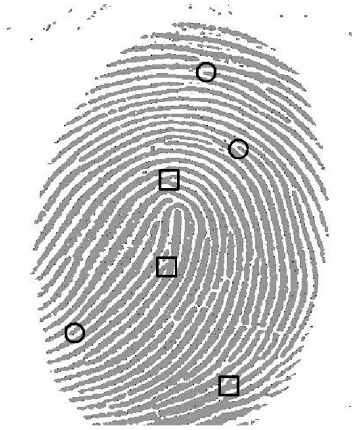


Figura 2.13: Abordagem local baseada em minúcias. Algumas terminações de linha (círculos) e bifurcações de linha (quadrados) estão marcadas.

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 (figura 2.12).

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. 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 2.13).

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 mícrons. 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 países. 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;[3]
- $\oplus$ Existe uma longa tradição legal no uso da impressão digital como identificador imutável;
- $\oplus$ Existem grandes bancos de dados legados de impressões digitais;
- $\oplus$ A impressão digital pode ser colhida facilmente a baixo custo.

Quanto aos pontos fracos, podemos citar:

[3]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.

- ⊖ 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 [NIST 2007]. 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* [Jain et al. 1999], um *software* aberto para comparação de impressões digitais implementado em MATLAB.

2.2.2 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.

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 [Chang et al. 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 2.14 mostra alguns exemplos de imagens de face.

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.

(a) Imagem 2D (b) Imagem 3D (c) Imagem IR

Figura 2.14: Imagem da face 2D, 3D e infravermelho.

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*.*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. 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.

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.

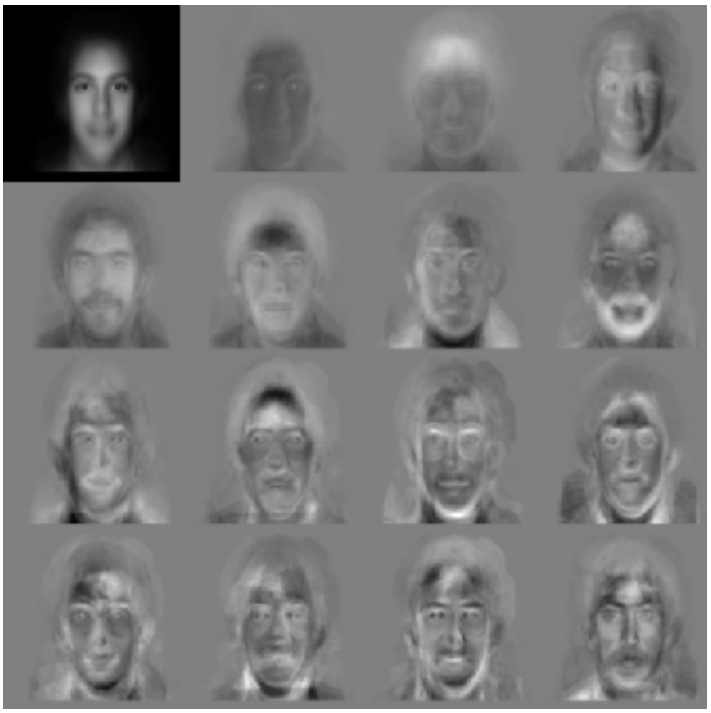


Figura 2.15: *Eigenfaces* são componentes estruturais que podem ser utilizados em um conjunto ponderado para representar uma determinada imagem de face.

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 [Gross 2005]. 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*), do NIST, possui imagens neutras e naturais da face de 1.200 usuários [NIST 2003a].
- XM2VTS - Este banco de dados foi coletado durante o projeto M2VTS (*Multi Modal Verification for Teleservices and Security applications*), [UCL 2005] e consiste de imagens frontais coloridas de 295 usuários em diversas posições de rosto, com fundo uniforme [XM2VTS 2006].

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), sob condução do NIST, foi baseada no banco de dados FERET. A competição *ICBA 2006 Face Verification* teve como base o XM2VTS.

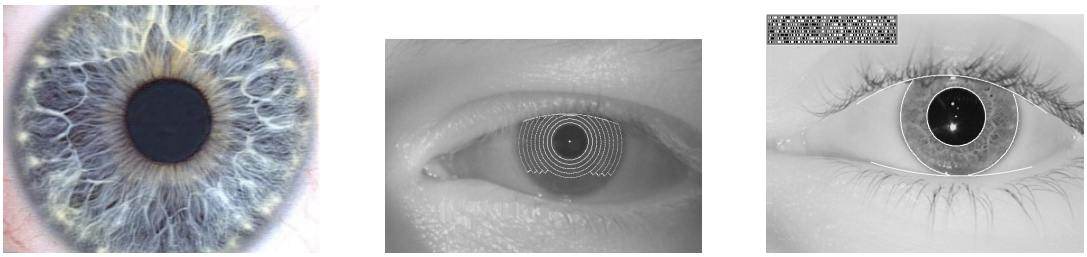
Existem vários sistemas abertos de reconhecimento de face [Grgic and Delac 2007]. Por exemplo, o OSCVL (*Intel Open Source Computer Vision Library*) [INTEL 2000] contém algoritmos de detecção e reconhecimento de face. A iniciação em experimentos de avaliação de sistemas de reconhecimento de face também não é difícil. Um sistema completo de avaliação é fornecido pela *Colorado State University*, compreendendo implementações de quatro algoritmos de reconhecimento que servem como ponto de partida [CSU 2003].

2.2.3 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].

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 2.16): (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.



(a) Aquisição (b) Extração (c) IrisCode

Figura 2.16: 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. Sejam C_A e C_B são os códigos extraídos de duas íris A e B, e M_A e M_B são máscaras para eliminar ruído. A distância de Hamming HD é calculada por

$$HD = \frac{\| (C_A \otimes C_B) \wedge M_A \wedge M_B \|}{\| M_A \wedge M_B \|}$$

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 operação (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 [CASIA 2006].
- 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 [Proença and Alexandre 2005].
- CUHK - A *Chinese University of Hong Kong* oferece cerca de 250 imagens de íris para fins de pesquisa [CUHK 2006].

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]. Uma boa coletânea da luta entre ataques e contramedidas referente a um sistema hipotético baseado no padrão da íris pode ser encontrado em [Ernst 2002].

2.2.4 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 2.17). 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**.

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

(a) Modelo esquemático (b) Imagem real (c) Dispositivo de aquisição

Figura 2.17: Medidas típicas da geometria da mão. O modelo esquemático (esquerda) pode ser apreciado na imagem real (centro) obtida de um dispositivo (direita).

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 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.

⊕ Adequado para integração com outras biometrias, em particular impressão digital e impressão palmar

⊕ Não relacionado a registros policiais e criminais.

Quanto aos pontos fracos, podemos citar:

⊖ 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.

2.2.5 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 suporte onde é traçada a assinatura. Os dispositivos podem registrar, por exemplo, conjuntos de dados 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** tratam o problema como um problema de classificação temporal de dados. Métodos utilizados incluem as medidas de distâncias euclidianas entre as trajetórias de canetas, medidas de correlação regional e medidas de reconhecimento temporal-probabilístico como as cadeias de Markov ocultas. 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, baseada na utilização de DTW (*Dynamic Time Warping*) [Myers and Rabiner 1981], está obscurecida desde o advento das cadeias de Markov ocultas. 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 determinista, 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 neste tipo de autenticação 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 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] [Gruber et al. 2006].

Resultados relatados na primeira competição internacional de verificação por dinâmica da assinatura [Yeung et al. 2004] 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.

2.2.6 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. [Campbell and Reynolds 1999] proporciona uma visão geral dos diversos bancos de dados disponíveis, dos quais citamos 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.
- ELRA - *European Language Resources Association* (Luxemburgo) - Mantém vários bancos de dados de trechos de voz em línguas européias.

O pacote LIA_RAL, da Université d'Avignon, na França, é um software de reconhecimento de voz, de código fonte aberto, implementado em C++ . 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 [Bonastre 2005].

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

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 manuais 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].

2.2.7 Considerações

2.2.7.1 Sumário comparativo

Uma comparação entre as seis tecnologias biométricas apresentadas nesta seção é mostrada na tabela 2.5 [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 2.1.1; 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	Precisão	Robustez
Digital	Média	Alta	Alta	Média	Média	Alta	Alta
Face	Alta	Baixa	Média	Alta	Alta	Baixa	Baixa
Íris	Alta	Alta	Alta	Média	Baixa	Alta	Alta
Mão	Média	Média	Média	Alta	Média	Média	Média
Assinatura	Baixa	Baixa	Baixa	Alta	Alta	Baixa	Baixa
Voz	Média	Baixa	Baixa	Média	Alta	Baixa	Baixa

Tabela 2.5: Comparativo entre as características de alguns identificadores biométricos [Jain et al. 2004].

2.2.7.2 Gêmeos e clones

O genótipo corresponde ao conjunto de genes específico do indivíduo. O fenótipo corresponde ao conjunto de características observáveis dos organismos biológicos, como a aparência, e demonstram a interação entre os genes e o ambiente. Assim, a aparência física em geral é uma parte do fenótipo do indivíduo. É de conhecimento geral que gêmeos idênticos e clones não possuem a mesma impressão digital. Ou seja, apesar de compartilharem o mesmo DNA, a impressão digital pode ser diferente. A razão é que esta característica não é apenas geneticamente determinada [Matsumoto et al. 2002]. 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.

Portanto, uma pequena mudança no micro-ambiente é amplificada pelo processo de diferenciação celular. Há tantas mudanças durante este processo de formação que seria virtualmente impossível que duas impressões digitais fossem iguais. No entanto, como as impressões digitais são diferenciadas dos mesmos genes, elas não são padrões totalmente aleatórios. 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]. Contudo, também tem sido anunciado que, apesar de as impressões digitais de gêmeos idênticos e clones serem diferentes, elas são apenas ligeiramente diferentes. Os sensores atuais são capazes de distinguir entre impressões digitais de gêmeos idênticos e resultados experimentais demonstram que as impressões palmares também possibilitam tal distinção [Kong et al. 2006].

As outras tecnologias aqui apresentadas também apresentam suas próprias peculiaridades no que tange aos gêmeos idênticos e clones. O padrão da íris também se mostra diferente para gêmeos idênticos e clones. Embora a cor dos olhos e a aparência geral da íris seja determinada geneticamente, os detalhes do padrão não são similares, proporcionando tanta distinção quanto os padrões de íris de pessoas não relacionadas [Daugman 2004]. O padrão de voz é bastante parecido, mas mesmo assim existem qualidades invariantes da voz que são únicas para cada indivíduo. Embora especialistas humanos consigam distinguir o padrão de voz de gêmeos idênticos, provavelmente as diferenças existentes não seriam perceptíveis para os dispositivos atuais [Decoster et al. 2001]. O padrão da assinatura manuscrita também é diferente.

No entanto, algumas características fisiológicas são iguais, como o padrão da face e o formato da mão, salvo diferenças ocasionadas pelo ambiente, como acidentes, doenças ou cirurgia plástica. a tabela 2.6 resume como as características biométricas se comportam quanto a gêmeos idênticos e clones.

Biometria	Gêmeos e clones	Referência
Digital	Diferentes	[Matsumoto et al. 2002]
Face	Iguais	Trivial
Íris	Diferentes	[Daugman 2004]
Mão	Iguais	Trivial
Assinatura	Diferentes	Trivial
Voz	Diferentes	[Decoster et al. 2001]

Tabela 2.6: Para gêmeos idênticos e clones, algumas características biométricas são iguais e outras são diferentes.

2.3 Conclusões do capítulo

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.

Capítulo 3

Seleção de tecnologias biométricas

Uma das características mais importantes de sistemas biométricos é o seu desempenho, representado por meio da estimativas das taxas de falsa aceitação e falsa rejeição. A seção 3.1 apresenta os padrões de avaliação do desempenho de um sistema biométrico. No entanto, o desempenho não é o único fator considerado na escolha de uma tecnologia biométrica. A tecnologia biométrica mais adequada depende fortemente dos requisitos da aplicação. A seção 3.2 apresenta uma matriz de avaliação de conformidade das características das tecnologias biométricas em relação aos requisitos da aplicação.

3.1 Avaliação de desempenho

Um sistema biométrico pode ser suficientemente grande para incorrer em investimentos cujo volume justifique uma avaliação consistente de seu desempenho. 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 de desempenho são implementadas por meio de uma competição entre os interessados (fabricantes ou grupos de pesquisa). Baseados em [Mansfield and Wayman 2002], vamos apresentar as três metodologias proeminentes de avaliação de desempenho: (1) avaliação de tecnologia; (2) avaliação de cenário; e (3) avaliação operacional.

O objetivo da **avaliação de tecnologia** 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** 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** 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 organizacional. 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, complementando esta avaliação por meio da utilização de algo parecido com a utilização de testes de invasão, a exemplo do que é feito com segurança de redes de computadores. Este ainda é um campo aberto para pesquisas.

Um ponto importante a ser considerado é a definição das taxas de erros máximas que podem ser tolerados pela aplicação. Uma estimativa inicial é fornecida por [Jain et al. 2004], que aponta requisitos de precisão típicos para um algoritmo de comparação, conforme resumido na tabela 3.1. Os números são baseados no que o autor acredita que deva ser a ordem de magnitude da precisão necessária do algoritmo de comparação, para viabilizar uma aplicação típica. O autor assume um sistema de larga escala contendo cerca de um milhão de identidades e assume um sistema de *screening* envolvendo cerca de 500 identidades. Os valores são bastante plausíveis. Por exemplo, na competição entre algoritmos de comparação de impressões digitais FVC2002, o melhor algoritmo alcançou o ponto de operação $\{FMR, FNMR\} = \{0.2\%, 0.2\%\}$.

E quanto às taxas de FAR e FRR, que valores são toleráveis por aplicações típicas? Os melhores valores até agora documentados em competições internacionais estão resumidos na tabela 3.2. Ora, vamos considerar um ataque de força bruta em um sistema biométrico operando no modo de verificação. A chance de sucesso do ataque de força bruta depende da precisão do sistema como um

Funcionalidade	FMR%	FNMR%
Verificação	0,1	0,1
Identificação	0,0001	10
Screening	0,0001	1

Tabela 3.1: Requisitos de precisão típicos de um comparador.

todo (FAR e FRR). Suponhamos que o sistema esteja operando com $\{FAR, FRR\} = \{0.001\%, 1\%\}$, o que é razoável para as tecnologias de impressão digital e íris. Esta taxa FAR de 0.001% indica que um fraudador tentando um ataque de força bruta necessita em média efetuar 100 mil tentativas para ter a esperança de conseguir um sucesso. Esta robustez possui ordem de grandeza equivalente à oferecida por uma boa senha de 5 dígitos, o que não é grande coisa. Por outro lado, para os usuários genuínos, haverá falsas rejeições na proporção de uma para cada 100 tentativas. Assim, se a utilização do sistema estiver na ordem de mil usuários por dia, haverá em média 10 casos de falsa rejeição para serem tratados. Isto demonstra que as taxas de erro FAR e FRR toleráveis para sistemas biométricos, dependem dos requisitos da aplicação. Em outras palavras, uma companhia deve saber quantos casos de falsa rejeição está disposta a tratar e quantos casos de falsa aceitação está disposta a tolerar, para então definir os requisitos de precisão do sistema. A seção 3.2 mostra como extrair fatores de seleção dentre os requisitos da aplicação e os atributos das tecnologias.

Tecnologia	EER%	Fonte
Impressão Digital	2,1%	[Cappeli,2006]
Face	4,5%	[Chang,2005]
Mão	1,5%	[BWG,2001]
Íris	$(0,00129\%, 0,583\%)$	[IBG,2005]
Voz	5,3%	[Przybocki,2004]
Assinatura	2,9%	SVC2004

Tabela 3.2: Os valores de EER obtidos para as principais tecnologias biométricas documentados em competições internacionais.

3.2 Conformidade aos requisitos

O desempenho de um sistema biométrico (representado por meio de suas taxas de falsa aceitação e falsa rejeição) não é a única característica a ser levada em conta quando da escolha de uma tecnologia biométrica para uma dada aplicação. De fato, várias outras questões surgem:

- A aplicação necessita de verificação (1:1) ou identificação (1:N)? Por exemplo, se uma aplicação requer a identificação (busca 1:N) de indivíduos em um grande banco de dados, então ela necessita de uma característica biométrica escalável e relativamente mais distintiva, como íris ou digital. Se a aplicação é de verificação, outras tecnologias biométricas podem ser usadas.
- Quais são os modos operacionais da aplicação? Por exemplo, se é atendida (supervisionada) ou não-atendida (totalmente automática), se os usuários são habituados ou não, se a aplicação é declarada ou não, se os usuários são cooperativos ou não-cooperativos, entre outros.

- Quais são os requisitos de armazenamento da aplicação? Por exemplo, uma aplicação que executa autenticação num servidor remoto pode exigir um perfil de tamanho pequeno, dependendo da banda disponível para a aplicação.

- Quão restritivos são os requisitos de desempenho? Por exemplo, uma aplicação que exija precisão excepcionalmente alta pode necessitar de uma tecnologia mais precisa que íris, como a retina. Este pode ser o caso de aplicações de alta segurança.

- Que tipos de tecnologias são aceitáveis para os usuários? Diferentes tecnologias biométricas são aceitáveis em aplicações desenvolvidas em diferentes grupos sociais, dependendo dos padrões culturais, éticos, sociais, religiosos e higiênicos. A aceitação é uma troca entre a sensibilidade da comunidade a vários tabus e a conveniência oferecida pelo reconhecimento biométrico.

Então, 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. Os fatores de seleção devem ser extraídos dos requisitos da aplicação, de modo a orientar 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 3.1.

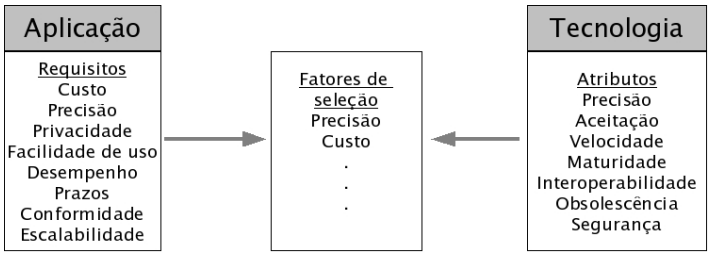


Figura 3.1: Fatores de seleção são extraídos dos requisitos da aplicação para orientar a escolha de tecnologias biométricas com atributos mais adequados.

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.

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 *American National Standards Institute* [ANSI 2005].

Uma **ferramenta de análise preliminar** pode ser utilizada pela construção de uma matriz de comparação baseada em pesos de atributos, conforme proposto por [Bolle et al. 2004, p. 138]. 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 (pesos dos atributos). De outro lado, a aplicação possui requisitos, a cuja importância também podem ser atribuidos valores numéricos (pesos dos requisitos). A interpretação dos pesos simbólicos como fatores numéricos pode ser ajustada arbitrariamente. O "casamento" entre requisitos e atributos resulta em valores de avaliação para cada tecnologia. Esta matriz de avaliação é especialmente útil em estágios preliminares de análise, para apontar as sensibilidades críticas do suposto sistema.

Resumidamente, o processo consiste dos seguintes passos:

1. Requisitos da aplicação - Elencar, normalizar e pontuar.
2. Atributos das tecnologias - Elencar, normalizar e pontuar.
3. Efetuar a comparação entre requisitos e atributos.

Para exemplificar estes passos, vamos considerar uma aplicação hipotética simples de controle de acesso físico, que possui os seguintes requisitos.

R_1 - A aplicação pretende se valer somente de biometria para autenticação, dispensando o uso de outras credenciais. Assim, é necessária uma tecnologia biométrica que seja possuida pela maioria da população alvo. Chamamos este requisito de disseminação e atribuímos ao mesmo alta importância.

R_2 - A aplicação vai trabalhar no modo verificação, fazendo buscas $1:1$ em um banco de dados de tamanho considerável, o que não exige uma tecnologia biométrica extremamente precisa. Chamamos este requisito de diferenciação e atribuímos ao mesmo importância baixa.

R_3 - A aplicação não está pronta para fazer atualizações no perfil biométrico do usuário, quando necessário. Chamamos este requisito de permanência e atribuímos ao mesmo importância baixa.

R_4 - A aplicação foi construída com a suposição de uma coleta rápida do exemplar biométrico, ou seja, a janela de tempo para coleta do exemplar é bastante pequena. Chamamos este requisito de tempo de coleta e atribuímos ao mesmo importância alta.

R_5 - O sucesso da aplicação depende da tolerância do usuário em fornecer a característica biométrica solicitada. Chamamos este requisito de tolerância e atribuímos ao mesmo importância alta.

R_6 - O sistema controla o acesso a uma instalação de segurança, então os eventos de falsa aceitação são indesejáveis. Chamamos este requisito de precisão e atribuímos importância alta.

R_7 - O sistema deve resistir a tentativas de invasão fraudulenta. Chamamos a este requisito de robustez e atribuímos importância alta.

No primeiro passo, é útil se construir uma tabela indicativa da importância dos requisitos da aplicação. Neste ponto, é necessário fazer uma escolha. A avaliação pode ser efetuada sobre pontos fortes (vantagens) ou sobre pontos fracos (desvantagens). Isto quer dizer que os requisitos da aplicação devem ser normalizados para proporcionar uma comparação adequada. Esta normalização consiste em transformar os requisitos em pontos fortes, ou então em pontos fracos.

Na análise baseada em pontos fortes, cada tecnologia recebe uma pontuação de acordo com o grau de satisfação do requisito considerado. Por exemplo, para o requisito *tolerância* (R_5), uma tecnologia que seja facilmente aceita pelos usuários recebe uma pontuação maior do que outra que tenha menor aceitação. Ao final, a observação das maiores pontuações globais nos fornece as tecnologias **mais** adequadas. Esta análise é indicada para escolha por eleição.

Por outro lado, na análise baseada em pontos fracos, as tecnologias são pontuadas de acordo com a sua dificuldade em satisfazer o requisito considerado. Por exemplo, para o requisito *diferenciação* (R_2), as tecnologias com menor precisão (que, portanto, constituem um ponto fraco em relação a este requisito) recebem uma pontuação mais alta do que aquelas que possuem maior precisão. Ao final, a observação das maiores pontuações globais nos fornece as tecnologias **menos** adequadas. Esta análise é indicada para escolha por eliminação.

Para o nosso exemplo, vamos utilizar a segunda modalidade para eliminar as tecnologias biométricas menos indicadas para a aplicação considerada. Cada requisito da aplicação torna-se, portanto, um ponto fraco a ser analisado.

Agora vamos atribuir a respectiva importância a cada item de requisito, ou seja, explicitar o que é mais sensível para a aplicação. Por exemplo, imaginemos que um requisito da aplicação seja a cor do sensor utilizado, que deve ser verde. É necessário especificar quão importante é este requisito. A cor verde pode ser um simples capricho ou pode ser uma exigência indispensável do país importador ao qual o sensor se destina. Assim, um item com importância *alta* indica que o respectivo ponto fraco deve ser considerado com extremo cuidado para a aplicação, em comparação com um ponto fraco cujo atributo esteja marcado como de *baixa* importância. O conjunto de atributos escolhido é completamente arbitrário. Podem ser escolhidos atributos com várias gradações, com cores, com valores numéricos ou qualquer outro conjunto. Afinal, o método exige que, em fase posterior, todos atributos sejam convertidos para valores numéricos adequados. Em nosso caso, escolhemos o conjunto $\{\text{Alta}, \text{Média}, \text{Baixa}\}$, com base em atributos apresentados na literatura [Jain et al. 2004].

A figura 3.2 nos fornece os requisitos da aplicação normalizados, ou transformados em desvantagens (tabela R). Para o conjunto $\{\text{Alta}, \text{Média}, \text{Baixa}\}$, referente aos valores das importâncias relativas dos requisitos, arbitrariamente escolhemos os pesos $\{16, 4, 2\}$. Esta escolha de pesos privilegia os itens de importância alta, pois, uma vez que estamos trabalhando com desvantagens, queremos ressaltar quais são os pontos críticos de nossas alternativas.

O próximo passo é relacionar os mesmos itens de desvantagens às diversas tecnologias biométricas sob análise, ou seja, normalizar os atributos das tecnologias. Como exemplo, vamos considerar como candidatas as seis tecnologias biométricas estudadas na seção 2.2 e os seus respectivos atributos listados na tabela 2.5. Para o conjunto de valores dos atributos $\{\text{Alta}, \text{Média}, \text{Baixa}\}$, arbitrariamente es-

Requisito	Desvantagem	Importância
Disseminação	Restrito	16
Diferenciação	Compartilhado	2
Permanência	Variação	2
Coleta	Dificuldade de coleta	16
Tolerância	Rejeição	16
Precisão	Permissivo	16
Robustez	Vulnerável	16

Tabela R – requisitos normalizados

Tabela A – atributos normalizados

Atributo	Desvantagem	Digital	Íris	Face	Mão	Voz	Assinatura
Universalidade	Restrito	3	1	1	3	3	10
Unicidade	Compartilhado	1	1	10	3	10	10
Permanência	Variação	1	1	3	3	10	10
Coleta	Dificuldade de coleta	3	3	1	1	3	1
Aceitação	Rejeição	3	10	1	3	1	1
Precisão	Permissivo	3	1	10	3	10	10
Robustez	Vulnerável	3	3	10	3	10	10

Tabela D – escore das desvantagens

Desvantagem	Digital	Íris	Face	Mão	Voz	Assinatura
Restrito	48	16	16	48	48	160
Compartilhado	2	2	20	6	20	20
Variação	2	2	6	6	20	20
Dificuldade de coleta	48	48	16	16	48	16
Rejeição	48	160	16	48	16	16
Permissivo	48	16	160	48	160	160
Vulnerável	48	48	160	48	160	160
$D = R^T \times A$	**244**	**292**	**394**	**220**	**472**	**552**

Figura 3.2: Exemplo do processo de avaliação preliminar das tecnologias biométricas candidatas a uma dada aplicação.

colhemos os pesos $\{10, 3, 1\}$ para representar sua importância relativa. Esta escolha de pesos também privilegia os itens de importância alta. No nosso exemplo, os pesos adotados (16, 4, 2 para os requisitos e 10, 3, 1 para os atributos) privilegiam os itens de importância alta, que correspondem aos pontos críticos de nossas alternativas. Em particular, esses valores garantem que, quando um requisito tem importância alta e o atributo associado possui valor baixo (ou vice-versa), isso terá uma pontuação maior — ou seja, é mais penalizado — do que quando tanto o requisito como o atributo possuem valor médio.

As pontuações consideradas para as tecnologias biométricas seguem um certo consenso dentro da comunidade biométrica, conforme documentado por [Jain et al. 2004]. A transformação dos itens em valores numéricos é conveniente para que as tabelas sejam úteis em um processo de cálculo. O escore final, que representa o valor relativo de cada desvantagem de cada tecnologia biométrica, agora avaliado *em face de nossa aplicação particular*, é fornecido da seguinte maneira:

1. Toma-se a coluna da matriz *R* de requisitos.
2. Toma-se cada coluna da matriz *A* de atributos, uma por vez.
3. Efetua-se o produto de cada elemento de *R* pelo respectivo elemento da coluna de *A*. A coluna resultante *D* é formada pelo produto simples dos elementos de *R* e *A*. Uma linha adicional de soma é útil para a análise posterior.
4. Repete-se o processo para todas as tecnologias biométricas, obtendo então o quadro de penalidades representado pela matriz *D*.

Ao final, temos a matriz *D*, cuja linha de soma nos fornece os valores de desvantagens acumuladas para cada tecnologia em face de nossa aplicação. Devemos considerar, no caso exemplificado de análise por desvantagens, que os maiores escores (penalidades) servem para apontar as tecnologias menos apropriadas para esta aplicação e explicitar claramente quais são os pontos mais sensíveis.

É importante alertar que alguns requisitos podem ser numéricos desde o início, como custo, taxas de erros, tamanho dos perfis, velocidade de processamento, tamanho da população, entre outros. Não é difícil converter atributos numéricos em valores ponderáveis. Por exemplo, vamos considerar o custo do sensor como uma desvantagem. Vamos supor que temos o custo do sensor para todas as tecnologias, e este custo v varia entre o mais barato (US$ 20) e o mais caro (US$ 5.000). Então, uma transformação candidata do valor v para a penalidade p poderia ser uma transformação linear do tipo $p = 1 + (v - 20)/554$ ou uma transformação logarítmica do tipo $p = 1 + \log(v/2) \times 3,753$ ou uma outra transformação prática qualquer que relaciona faixas de custo a valores numéricos entre 1 e 10, ou quaisquer extremos escolhidos para as penalidades. Para mapear um conjunto de valores y que varia entre os extremos y_1 e y_2, para um conjunto de valores x que varia entre os extremos x_1 e x_2, podemos usar uma transformação do tipo $x = x_1 + (y - y_1) \times (x_2 - x_1)/(y_2 - y_1)$. Podemos ainda usar uma transformação do tipo $x = x_1 + (\log(y/y_1) \times (x_2 - x_1)/\log(y_2/y_1))$. Uma transformação prática poderia ser o mapeamento de faixas de valores de y a valores de x, como por exemplo, se $20 \leq y \leq 100$, então $x = 1$, se $101 \leq y \leq 175$, então $x = 2$, e assim por diante ...

3.2.1 Considerações sobre a metodologia

Esta metodologia de avaliação preliminar possui pelo menos duas grandes vantagens que a capacitam para utilização por grandes empresas interessadas na seleção de sistemas biométricos, como é o caso de instituições financeiras de grande porte. Em primeiro lugar, permite sistematizar o debate sobre os pontos importantes a serem considerados na seleção de um sistema biométrico para uma dada aplicação, o que é bastante útil para uma empresa de grande porte, onde normalmente vários departamentos com interesses diferentes e às vezes conflitantes se envolvem num trabalho de seleção deste tipo. Em segundo lugar, permite que o esforço de seleção seja documentado plenamente em seus diferentes aspectos, utilidade valiosa quando se trata de justificar posteriormente as escolhas feitas perante qualquer entidade de auditoria.

Uma limitação desta metodologia consiste na grande liberdade concedida para a escolha dos pesos de importância de atributos e de importância de requisitos e das maneiras de mapeamento destes pesos em valores numéricos. A premissa subjacente é que essas escolhas sejam realizadas por especialistas com conhecimento das tecnologias consideradas e da aplicação a ser desenvolvida. Todavia, existe o risco de que escolhas indevidas apontem uma solução que não seja efetivamente a mais indicada; estes equívocos podem ocorrer de forma acidental, devido ao desconhecimento de um ou mais aspectos das tecnologias ou da aplicação, ou de forma intencional, para desvirtuar a análise de forma a apontar uma tecnologia previamente escolhida como a mais apropriada. A viabilidade de utilização desta metodologia de seleção será demonstrada na seção 4, onde é aplicada para a escolha da tecnologia biométrica mais adequada para uma aplicação hipotética de *web banking*.

3.3 Conclusões do capítulo

Existem alguns padrões de avaliação da precisão das tecnologias biométricas. Para a seleção de uma tecnologia biométrica para uma dada aplicação, no entanto, outras características devem ser observadas. Este capítulo mostrou que tecnologia biométrica mais adequada depende fortemente dos requisitos da aplicação e apresentou uma metodologia de avaliação preliminar. Numa aplicação real, a quantidade de requisitos de aplicação a serem considerados alcançaria o montante das dezenas. O escore final de penalidades se mostra como uma ferramenta bastante útil pra explicitar e proporcionar o debate sobre os pontos críticos das tecnologias candidatas a uma determinada aplicação em particular.

Capítulo 4

Estudo de caso - autenticação biométrica em um *web banking*

Os serviços bancários oferecidos por um banco de varejo típico são acessíveis através de uma variedade de canais de atendimento, como agências, máquinas de auto-atendimento e Internet. Dentre esses canais, destaca-se o *web banking*, que alia conveniência para os clientes e baixo custo para o banco. De fato, no caso dos bancos brasileiros, o número de transações bancárias pela *web* já supera o de transações realizadas nos caixas tradicionais [Febraban 2006]. A despeito dessa popularidade, o uso do canal *web* está sujeito a uma série de riscos, o que leva a grandes investimentos no sentido de melhorar a sua segurança. Um dos aspectos de segurança que tem recebido maior atenção é a autenticação dos usuários, um dos mais freqüentes alvos de fraudes bancárias. Os mecanismos tradicionalmente adotados para autenticação são credenciais de conhecimento (códigos e senhas) e de posse (cartões) [Sklira et al. 2003].

Estas credenciais possuem limitações, pois podem ser observadas, esquecidas ou perdidas. Além disso, elas não permitem vincular com suficiente grau de certeza uma transação ao indivíduo que a realiza. A autenticação biométrica é capaz de contornar essas deficiências: ela caracteriza unicamente um indivíduo e não pode ser esquecida ou perdida. O uso adequado de credenciais biométricas, possivelmente em conjunto com credenciais de conhecimento ou posse, pode aumentar significativamente a segurança da autenticação de usuários de *web banking*. Este trabalho propõe um modelo de implementação para autenticação biométrica em sistemas de *web banking*. Este modelo possibilita que as vantagens das credenciais biométricas sejam aproveitadas sem negligenciar as suas limitações. Para integrar novos mecanismos de autenticação ao complexo ambiente computacional bancário, o modelo se utiliza da tecnologia de Serviços Web, que se caracteriza pela interoperabilidade e suporte a sistemas legados. A aplicabilidade do modelo é demonstrada usando um protótipo.

Neste capítulo, descrevemos o ambiente computacional bancário com ênfase nos sistemas de *web banking*; apresentamos a tecnologia de Serviços Web e os padrões usados para garantir segurança nessa tecnologia; e, discutimos o nosso modelo para autenticação biométrica em sistemas de *web banking* e a sua implementação.

4.1 Descrição do *web banking*

A figura 4.1 apresenta um modelo de alto nível da arquitetura de TI de um banco de varejo típico. Nela também se evidencia entre que camadas se mostra mais adequada a introdução de funcionalidades focadas na interoperabilidade, como é o caso das funcionalidades fornecidas por Serviços Web [Shan 2004]. Os elementos principais são:

1. Arquitetura técnica da empresa: lida com a arquitetura e a infra-estrutura no mais alto nível através da organização; exerce a governança, define políticas, estratégias e padrões corporativos; é responsável por todos os serviços estruturais, como *data centers*, rede corporativa, armazenamento, monitoração, gerenciamento do sistema e segurança.

2. Arquitetura intercanal: preocupa-se com as funcionalidades básicas e comuns, compartilháveis entre os diferentes canais de atendimento; lida com padrões de serviços, métodos de distribuição e gerencia uma infra-estrutura independente de canal, composta de recursos e aplicações relacionados a dados corporativos utilizáveis por todos os canais, como os dados de clientes, dados de agências, dados de produtos, entre outros.

3. Arquitetura do canal: lida com os requisitos de sistema, de segurança, de carga, de armazenamento, de capacidade, entre outros, específicos de um canal particular.

4. Aplicação (App): envolve os requisitos de negócios e características tecnológicas relacionados a cada aplicação específica.

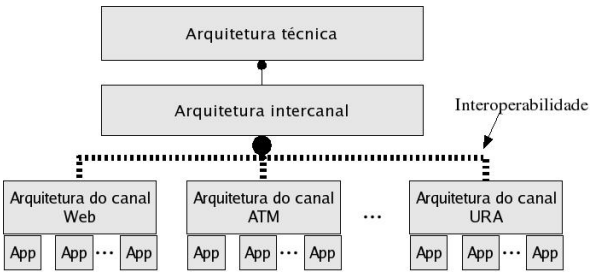


Figura 4.1: Modelo de alto nível da arquitetura da empresa

A dependência de sistemas legados é uma característica comum em ambientes computacionais bancários. Em geral, estes sistemas se constituem de bases de dados e aplicações construídas ao longo de décadas, utilizando diversas tecnologias e arquiteturas, para atender a requisitos funcionais e de negócios. Estas aplicações legadas dificilmente poderiam ser portadas para outra plataforma, devido ao custo e ao risco inerentes, uma vez que são aplicações de missão crítica. Em termos do modelo da figura 4.1, podemos dizer que sistemas legados podem ser encontrados em todas as camadas, em especial na arquitetura intercanal.

Dentre os vários canais de atendimento disponíveis no ambiente bancário, o canal *web* merece destaque devido ao crescimento de sua utilização [Febraban 2006]. A figura 4.2 mostra um exemplo típico de aplicação do canal *web banking*. O usuário efetua o acesso a partir de um computador ligado à Internet usando um navegador *Web*. A rede do banco, embora complexa, pode ser modelada

por meio um servidor *Web* que atende às requisições específicas para este canal e realiza o interfaceamento com os sistemas legados que implementam os serviços bancários. A comunicação entre o cliente e o servidor *Web* é protegida por um canal SSL (*Secure Sockets Layer*), que garante a confidencialidade, integridade e autenticidade do tráfego. É muito comum a utilização de *applets* Java no lado cliente, o que permite a implementação de funcionalidades mais sofisticadas e seguras (por exemplo, estabelecimento de cifragem fim a fim entre o cliente e o serviço legado de transações bancárias), além de facilitar a manutenção e distribuição do código da aplicação pelo banco. Apesar disso, a vulnerabilidade do ambiente computacional do cliente e o desconhecimento de noções de segurança por parte dos usuários dificultam a tarefa de garantir a segurança nesta ponta da transação.

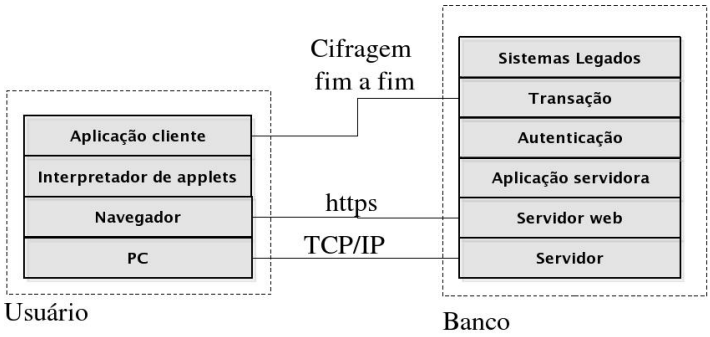


Figura 4.2: Um exemplo de aplicação de *web banking*.

4.1.1 Problemas e soluções de segurança do *web banking*

Dentre os aspectos de segurança relacionados a sistemas de *web banking*, um dos mais importantes é a **autenticação de usuários** [Gupta et al. 2004]. Tipicamente, essa autenticação usa uma combinação agência/conta/senha. Em muitos casos, a senha do canal *web* é diferente da senha do cartão magnético, podendo substituir esta última ou complementá-la. Esta autenticação baseada em conhecimento está sujeita a ataques fraudulentos baseados na obtenção do segredo. Este segredo pode vazar devido a ações inadequadas do próprio usuário ou a ações fraudulentas de uma atacante. Alguns exemplos de obtenção da senha ilustram a fraqueza da autenticação baseada apenas em conhecimento:

- Observação da senha - O usuário é observado por um terceiro ao informar a senha no canal virtual ou o usuário anota a senha em algum local ao alcance do fraudador, como a parte inferior do teclado.
- Roubo da senha - A senha do usuário pode ser obtida por meio de programas residentes instalados na máquina do usuário à revelia do mesmo (cavalos de tróia).
- Senha compartilhada - O usuário pode compartilhar a senha com pessoas de sua confiança.
- Sessão aberta - O usuário pode esquecer a sessão aberta e esta, então, pode ser utilizada por terceiros.
- *Link* falso - O usuário que navega na Internet pode ser falsamente induzido a clicar em um *link* que supostamente indica o *site* do Banco. No entanto, o usuário é enganado, pois o *link* indica,

de fato, a página de um terceiro (fraudador), construída para imitar o *site* do Banco. O usuário desavisado acaba informando seus dados (inclusive senha) no formulário que ele pensa ser do Banco.

- *Phishing* - O usuário é convencido a informar seus dados pessoais, inclusive senha, na falsa esperança de obter um privilégio. Exemplos comuns são mensagens falsamente atribuídas a órgãos oficiais, mensagens que falsamente anunciam provas de adultério e mensagens que falsamente anunciam um prêmio tentador, entre outros.

- Senha fraca - Composição da senha com parte dos dados pessoais dos usuários, como datas de nascimento, placas de automóveis, entre outros.

Para aumentar a confiança na autenticação baseada em conhecimento, os bancos bancos tomam várias medidas de reforço da segurança, como rejeição de cadastramento de senhas óbvias ou relacionadas ao usuário, medidas restritivas para alteração da senha, bloqueio da senha por excesso de tentativas erradas, bloqueio da senha por inatividade, limite diário de movimentação, política anti-*spam*, teclado virtual obrigatório e ações de educação do usuário quanto ao quesito segurança. Cumulativamente, alguns bancos estão adotando soluções baseadas em credenciais de posse, tais como:

- cadastramento prévio dos endereços IP dos computadores usados pelo cliente;

- distribuição de cartões contendo um conjunto de códigos, os quais serão usados a cada acesso, um de cada vez, uma única vez, em ordem pré-estabelecida (esquema de *one-time password*);

- distribuição de certificados digitais que precisam ser apresentados a cada acesso.

Embora estas soluções de autenticação de dois fatores aumentem sobremaneira a segurança da autenticação, elas são insuficientes para vincular o acesso ao sistema a uma pessoa específica, pois as credenciais utilizadas podem ser repassadas ou emprestadas. Sistemas biométricos de autenticação procuram vincular unicamente um indivíduo com suas credenciais biométricas. Adequadamente implementados, podem aumentar significativamente a confiança na autenticação de usuários.

4.2 Seleção da tecnologia biométrica

Segundo [Bolle et al. 2004] [Ashborn 2004], é necessário o levantamento prévio dos **requisitos da aplicação**, para que se possa escolher posteriormente as tecnologias biométricas mais adequadas para a aplicação específica. Alguns requisitos típicos de uma aplicação de *web banking* estão resumidos na tabela 4.1.

Vamos utilizar o método descrito na seção 3.2 como ferramenta preliminar de análise para seleção da tecnologia biométrica mais apropriada para a nossa aplicação de *web banking*. A nossa escolha novamente recai sobre uma análise baseada em desvantagens, o que nos proporciona uma escolha

R_n	Requisito	Descrição
R_1	Mobilidade	Os usuários efetuam a maioria dos acessos sempre por meio do mesmo computador. Alguns usuários até mesmo se valem da facilidade de cadastramento de computadores para acesso. No entanto, um requisito essencial da aplicação é a mobilidade, ou seja, o usuário pode acessar o canal por meio de qualquer computador conectado à Internet. Este requisito é de alta importância.
R_2	Resistência à fraude	A aplicação já enfrenta seus próprios problemas com relação à segurança. A introdução de qualquer característica nova no sistema não deve enfraquecê-lo ainda mais, razão pela qual a resistência à fraude é um fator importante pra o sistema. Este requisito é de alta importância.
R_3	Variação	É desejável que a característica biométrica varie pouco ao longo do tempo, economizando assim os custos de atualização dos perfis biométricos. Este requisito é de alta importância.
R_4	Aceitação	A coleta da característica deve ser tolerada pelo usuário. Este requisito é de média importância.
R_5	Desempenho	O processo de autenticação não pode ser muito lento, sob pena de comprometer o sistema. Este requisito é de média importância.
R_6	Custo	O sensor de aquisição deve possuir um cutos razoável. Este requisito é de média importância.
R_7	Facilidade de uso	O sistema deve ser de fácil utilização pelo usuário. Este requisito é de baixa importância.
R_8	FA @ FR=1%	A precisão do sistema deve ser adequada ao processo de autenticação. Estando fixado um índice de falsa rejeição de 1%, o sistem será tanto pior quanto maior for a falsa aceitação. Este requisito é de alta importância.
R_9	População coberta	É desejável que a característica biométrica seja possuída pela maior parte da população alvo. Este requisito é de baixa importância.
R_{10}	Tamanho do perfil	O tamanho do perfil influencia diretamente nos custos de armazenamento, processamento e transmissão, motivo pelo qual um perfil de menor tamanho é mais desejável. Este requisito é de média importância.

Tabela 4.1: Requisitos da solução.

por eliminação. Baseados nos requisitos da aplicação listados na tabela 4.1 , vamos construir a tabela *R* (figura 4.3) indicativa da importância dos requisitos aplicáveis às tecnologias biométricas sob avaliação. Cada requisito aplicável é transformado em uma *desvantagem* a ser analisada, em um *ponto fraco* a ser examinado (segunda coluna da tabela *R*). O nível de importância de cada requisito também é mapeado do conjunto $\{\text{Alta}, \text{Média}, \text{Baixa}\}$ para o conjunto $\{10, 3, 1\}$ (terceira coluna da tabela *R*). Como já dissemos na seção 3.2, esta escolha de pesos privilegia os itens de importância alta, pois, uma vez que estamos trabalhando com desvantagens, queremos ressaltar quais são os pontos críticos de nossas alternativas.

A próxima ação é relacionar os mesmos itens de desvantagens às diversas tecnologias biométricas sob análise. A tabela *A* da figura 4.3 mostra, para cada tecnologia biométrica, o quanto é grande cada desvantagem considerada. As entradas textuais são convertidas em valores numéricos de penalidades ($\{\text{Alta}, \text{Média}, \text{Baixa}\} \longrightarrow \{10, 3, 1\}$). Com a finalização do processo para todas as tecnologias biométricas, obtemos o quadro de escores (tabela *D*), com o auxílio da qual podemos extrair algumas conclusões:

C_1 - A tecnologia de impressão digital é a que fornece o menor escore de penalidades, seguida de perto pela tecnologia baseada no padrão da íris.

C_2 - As outras quatro tecnologias (face, mão, voz e assinatura) formam um grupo com maiores escores de penalidades. As quatro tecnologias apresentam um ponto sensível em comum, em

Requisito	Desvantagem	Importância
Mobilidade	Baixa mobilidade	10
Resistência à fraude	Baixa resistência à fraude	10
Variação	Variação	10
Aceitação	Rejeição	3
Desempenho	Lentidão	3
Custo	Custo do sensor	3
Facilidade de uso	Dificuldade de uso	1
FA @ FR=1%	FA @ FR=1%	10
População coberta	População faltante	1
Tamanho do perfil	Tamanho do perfil	3

Tabela R – requisitos normalizados

Tabela A – atributos normalizados

Requisito	Desvantagem	Digital	Íris	Face	Mão	Voz	Assinatura
Mobilidade	Baixa mobilidade	1	3	3	10	1	10
Resistência à fraude	Baixa resistência à fraude	3	3	10	1	10	1
Variação	Variação	3	3	3	3	10	10
Aceitação	Rejeição	3	3	3	3	1	1
Desempenho	Lentidão	1	1	10	3	10	3
Custo	Custo do sensor	3	3	1	10	1	10
Facilidade de uso	Dificuldade de uso	1	3	1	3	1	10
FA @ FR=1%	FA @ FR=1%	1	1	10	10	10	10
População coberta	População faltante	3	1	1	3	3	10
Tamanho do perfil	Tamanho do perfil	3	3	10	1	3	3

Tabela D – escore das desvantagens

Desvantagem	Digital	Íris	Face	Mão	Voz	Assinatura
Baixa mobilidade	10	30	30	100	10	100
Baixa resistência à fraude	30	30	100	10	100	10
Variação	30	30	30	30	100	100
Rejeição	9	9	9	9	3	3
Lentidão	3	3	30	9	30	9
Custo do sensor	9	9	3	30	3	30
Dificuldade de uso	1	3	1	3	1	10
FA @ FR=1%	10	10	100	100	100	100
População faltante	3	1	1	3	3	10
Tamanho do perfil	9	9	30	3	9	9
Placar	**114**	**134**	**334**	**297**	**359**	**381**

Figura 4.3: Escore final de cada desvantagem de cada tecnologia biométrica, quando relacionada com nossa aplicação em particular.

relação a esta aplicação, que é a precisão na faixa de operação requerida pela aplicação.

C_3 - A tecnologia de face apresenta ainda uma forte sensibilidade em relação a esta aplicação, que é a baixa resistência à fraude. De fato, considerando um sistema simples de face sem supervisão, é possível a execução da fraude por meio da utilização de uma fotografia do usuário verdadeiro. Sistemas mais elaborados podem se valer de sinais de vitalidade, como o piscar de olhos ou o movimento da boca. No entanto, são mais caros e mais lentos.

C_4 - A tecnologia de mão apresenta ainda o ponto sensível da baixa mobilidade, pois os dispositivos de aquisição baseados no formato da mão são grandes. Afinal, a mão é grande.

C_5 - A tecnologia de voz pode ser fraudada com uma simples gravação da voz do usuário. Até mesmo para os sistemas de voz independentes do texto, existe a possibilidade de utilização de aplicativos de imitação de voz. Além disso, a voz pode sofrer grandes variações dependendo do estado de saúde ou estado emocional do usuário.

C_6 - A tecnologia de assinatura também peca pela falta de mobilidade, pois as *tablets* de assinatura, embora portáteis, são grandes e inconvenientes para transporte. Exceção pode ser feita ao acesso por intermédio de *palmtops* e PDA's. Além disso, a assinatura do usuário pode variar fortemente, dependendo do estado do usuário. Até mesmo a colocação correta do apoio do punho pode alterar a assinatura.

4.3 Implementação com a utilização de Serviços Web

4.3.1 Padrões de segurança para Serviços Web

Com a disseminação de serviços pela Internet, as empresas também passaram a perceber os benefícios que poderiam ser auferidos através da interação de seus sistemas computacionais com os sistemas de organizações parceiras como clientes e fornecedores, notadamente em relações como B2B (*business-to-business*) e B2C (*business-to-consumer*). Entretanto, a natural incompatibilidade entre sistemas que não foram originalmente projetados para suportar tais interações apresenta desafios à implementação desse tipo de relação. Diante desse cenário, foram propostas tecnologias com o objetivo de viabilizar a construção de aplicações distribuídas facilitando a integração dos sistemas já existentes. Os Serviços Web (WS) são uma das mais recentes e mais promissoras dessas tecnologias integradoras. Fundamentalmente, a tecnologia WS baseia-se na definição de **serviços**, que representam processos de aplicação, e de **documentos XML**, que encapsulam a informação processada e transmitida pelos serviços. A interoperabilidade decorre da definição de padroes adequados à orientação a servicos e do uso de outros amplamente estabelecidos, como XML e HTTP [Mello et al. 2006].

A exposição dos sistemas computacionais de uma organização (e das informações que eles processam) através de Serviços Web suscita naturalmente preocupações com a segurança. Visando minimizar tais preocupações, foram elaborados diversos padrões de segurança para WS. A principal especificação de segurança relacionada a Serviços Web é a WS-Security (da OASIS), que descreve melhorias e extensões nas mensagens SOAP para agregar as propriedades de confidencialidade (com base na XMLEncryption) e integridade (com base na XMLSignature). A especificação WS-Security visa garantir a segurança fim a fim no nível da mensagem e não somente no nível de transporte, possuindo três pontos principais: (1) credenciais de segurança que podem ser incluídas nas mensagens SOAP com informações de autenticação; (2) integridade da mensagem pela inclusão na mensagem SOAP de informações relacionadas a assinaturas digitais de toda ou de parte da mensagem; e, (3) confidencialidade da mensagem, pela cifragem total ou de partes da mensagem [OASIS 2006].

O esquema XML definido nas especificações WS-Security permite a existência de vários elementos `<wsse:Security>` dentro da mensagem SOAP. O conjunto de especificações XCBF, para troca de dados biométricos (seção 2), pode ser usado dentro das especificações WS-Security, segundo publicação da OASIS (*Web Services Security XCBF Token Profile*). O modelo de processamento para WS-Security com objetos XCBF não é diferente de outros formatos de *token* descritos no WS-Security. Objetos XCBF devem ser anunciados utilizando `<wsse:XCBFSecurityToken>` dentro do cabeçalho da mensagem SOAP. Os atributos do *token* são usados para indicar características do conteúdo do mesmo para a aplicação que processa o WS-Security. O processamento da biometria, da assinatura e da cifragem de objetos XCBF não é parte do modelo de processamento WS-Security, devendo ser tratado por manipuladores adicionais ligados à biometria. O exemplo da figura 4.4 ilustra uma mensagem SOAP cujo cabeçalho (linhas 2-12) contém um *token* de segurança XCBF (linha 4). Neste exemplo, o `XCBFSecurityToken` contém um objeto biométrico desprotegido, ou seja, nem cifrado e nem assinado (linha 6). Os dados biométricos (linha 9) são codificados em uma representação ASCII para transferência [WSS-XCBF 2002].

```
<S:Envelope xmlns:S="...">
  <S:Header>
    <wsse:Security xmlns:wsse="...">
      <wsse:XCBFSecurityToken
         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
         Id="biometric-objects"
         ValueType="wsse:XCBFv1"
         EncodingType="wsee:DER">
            MIIEZzMJMzCCA9CzPHGzAwIBA ...
      </wsse:XCBFSecurityToken>
    </wsse:Security>
   </S:Header>
   <S:Body>  ...  </S:Body>
```

Figura 4.4: Exemplo de mensagem SOAP contendo um *token* XCBF.

A WS-Trust é uma especificação que procura fornecer um ambiente confiável para os Serviços Web. Trata-se de um esforço que visa principalmente a troca de credenciais de segurança, para que possibilite a comunicação através de diferentes domínios de segurança. A especificação descreve as relações de confiança que podem ser estabelecidas: (1) direta, quando o domínio A confia nos atributos oriundos do domínio B; e (2) mediada, quando os domínios A e B possuem relações de confiança com um domínio C, mas não possuem relações entre si. Os STSs (*Security Token Services*) introduzidos na especificação WS-Trust como as autoridades responsáveis por emitir os atributos de credenciais. O próprio STS é um *web service*, e a comunicação com o mesmo se dá por meio de um protocolo de pedidos e respostas: RST (`RequestSecurityToken`) e RSTR (`RequestSecurityTokenResponse`). Os atributos de segurança emitidos pelo STS consistem em asserções SAML (*Security Assertion Markup Language*, da OASIS) [WS-Trust 2005].

Numa visão bastante concreta, SAML é um conjunto de especificações e esquemas XML para troca de informações de segurança, expressas na forma de asserções de segurança de três tipos: (1) asserções de autenticação realizadas por um sujeito, expressando, por exemplo, que a autenticação se deu sobre um mecanismo de segurança específico, com base em uma informação de identificação particular e num dado instante; (2) asserções de atributos atestando o valor de um ou mais atributos do sujeito, como o número do cartão de crédito ou a descrição do último serviço realizado pelo sujeito; e, (3) asserções de autorização que atestam que serviços o sujeito está autorizado a realizar [Kearney et al. 2004].

Para verificar se as asserções emitidas pelo STS embutem credenciais que permitam ativar serviços, é necessário consultar uma política de autorização no sistema. Geralmente, cada sistema se vale de linguagens próprias para a definição de políticas de autorização. Para promover a interoperabilidade, foi introduzida a XACML (*eXtensible Access Control Markup Language*, da OASIS) [Godik and Parducci 2002] fornecendo: (1) uma linguagem para políticas de controle de acesso, utilizada para definir quem possui acesso sobre que recursos; e, (2) o formato das requisições e respostas usadas para efetuar consultas à política de autorização. Este formato de requisições e respostas define as trocas entre o PEP (*Policy Enforcement Point*) e o PDP (*Policy Decision Point*) [Yavatkar et al. 2000]. O PDP é a entidade que toma a decisão de autorização. Para tanto, avalia os atributos do requisitante, da operação e do recurso solicitado, com base em uma política de

autorização. O PEP, por sua vez, é a entidade que aplica a decisão de acesso tomada pelo PDP. Desta forma, estas entidades atuam em conjunto para concretizar a política de autorização do sistema. Um pedido é composto por: (1) atributos do sujeito que origina a requisição; (2) identificação do recurso desejado; (3) ações que serão executadas no recurso; e, (4) atributos do ambiente [Mello et al. 2006].

4.3.2 Modelo para Autenticação Biométrica em *Web Banking*

4.3.2.1 Modelo Conceitual

A figura 4.5 apresenta o modelo proposto para um serviço de *web banking* com autenticação biométrica. Em linhas gerais, um cliente pretende utilizar um serviço que fornece acesso a um recurso, como uma transação bancária. Antes de requisitar o serviço, o cliente precisa se autenticar no sistema. A **autoridade de autenticação** assegura que o cliente se autenticou em um determinado instante usando um método específico de autenticação. Após o processo de autenticação, o cliente recupera atributos de credencial que estão armazenados no sistema (como o seu nome e CPF) e que são usados para determinar se o mesmo possui direito de acesso ao recurso. A emissão desses atributos é responsabilidade da **autoridade de atributos**.

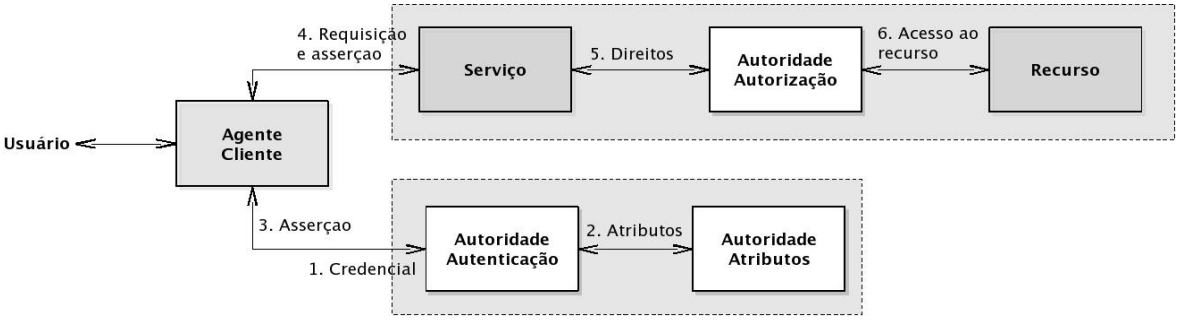


Figura 4.5: Modelo utilizado para descrever o caso de *web-banking*.

Tipicamente, um serviço de *web banking* é estruturado em pacotes de serviços adequados ao nível de confiança oferecido pela autenticação do usuário. Um usuário não autenticado pode ter acesso a serviços básicos, como informações, consultas e solicitações. No espaço autenticado, o usuário que apresenta uma credencial comum tem acesso a um pacote de serviços básicos, como saldos, extratos e transferências de pequeno valor. Já para um usuário que oferece informação de identificação especial, o processo de autenticação fornece um nível maior de confiança, o que permite a disponibilização de serviços de maior risco, como transferências de grandes valores, por exemplo. A decisão de qual pacote de serviços está disponível para um usuário do sistema é responsabilidade da **autoridade de autorização**, que se vale para isso das informações fornecidas pelas autoridades de autenticação e de atributos.

O funcionamento do modelo se baseia na seguinte dinâmica, ilustrada na figura 4.5. O agente cliente, após a captura, envia a informação biométrica do usuário para a autoridade de autenticação, que verifica a validade da mesma (1) e recupera atributos do mesmo (2). Caso a informação biométrica do usuário seja válida, a autoridade de autenticação fornece ao agente cliente credenciais para apresentar

aos mecanismos de controle de acesso (3). Após esta autenticação inicial, o agente cliente busca a execução do serviço desejado, por meio do envio de uma requisição acompanhada da asserção de autenticação (4). A autoridade de autorização verifica a validade das credenciais do requisitante do serviço e se o agente cliente possui a autorização necessária para a realização do serviço (5). A relação de confiança dentro do domínio do banco é direta, ou seja, existe confiança entre as autoridades de autenticação e de autorização. O serviço desejado é então executado, com base na decisão da autoridade de autorização (6).

4.3.2.2 Mapeamento do modelo em padrões de Serviços Web

O modelo conceitual apresentado da seção anterior é mapeado em uma arquitetura orientada a serviços, como mostrado na figura 4.6. O usuário é representado por um **agente cliente**, que

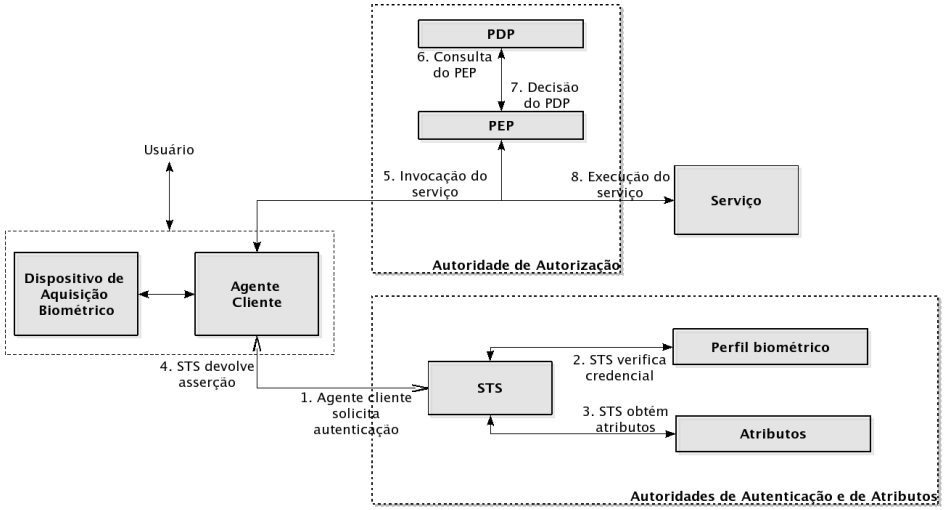


Figura 4.6: Modelo de implementação usando Serviços Web. O agente cliente é direcionado ao STS (1), que verifica a credencial do usuário (2), recupera seus atributos (3) e emite uma asserção de autenticação (4). O agente cliente invoca o serviço (5), que, com base na decisão de autorização (6 e 7), é executado (8).

é um *proxy* para intermediar as interações do usuário com os Serviços Web. As autoridades de autenticação e de atributos são implementadas por um STS (definido na especificação WS-Trust) e que é responsável por emitir, validar e trocar credenciais de segurança, representadas neste modelo por asserções SAML. O papel de autoridade de autorização é assumido pelo conjunto PEP/PDP: o PDP toma a decisão de autorização, com base nas credenciais do cliente e na política de autorização definida para o recurso, e o PEP aplica a decisão tomada pelo PDP. A figura 4.6 também ilustra a dinâmica de funcionamento do modelo de implementação, cujos passos são detalhados na tabela 4.2.

No modelo introduzido, a autenticação de usuários junto ao banco se dá por meio do processo de verificação biométrica (seção 2.1.1), fazendo uso da tecnologia baseada em **impressão digital**. A utilização da impressão digital é justificada pelos seus pontos fortes: (1) esta tecnologia proporciona suficiente precisão para trabalhar com sistemas de verificação de larga escala; (2) existe uma longa tradição legal no uso da impressão digital como identificador imutável; (3) as impressões digitais dos

vários dedos da mão são diferentes e as impressões digitais de gêmeos idênticos são diferentes; (4) a impressão digital pode ser colhida facilmente a baixo custo; e, (5) os sensores podem ser pequenos e portáteis, apropriados para um sistema de *web banking* e já existem até mesmo sensores de impressão digital embutidos em *smart cards* e diversos modelos de computadores portáteis.

Passos	Descrição
1. O agente cliente solicita autenticação	O agente cliente solicita autenticação, por meio do envio de uma mensagem SOAP, contendo um RST. Os dados do exemplar biométrico são encapsulados em um objeto XCBF. Isto implica o envio de um `XCBFSecurityToken` para ser tratado pelo STS.
2. STS verifica credencial	O STS recebe o RST (`RequestSecurityToken`) e o *token* biométrico, que contém a informação necessária para escolher o algoritmo de comparação. O STS busca o perfil biométrico do usuário no banco de dados e efetua o processo de verificação.
3. STS obtém atributos	O STS, agora atuando como autoridade de atributos, recupera os atributos desejados do usuário em um repositório de atributos.
4. O STS devolve as asserções	O STS devolve uma mensagem ao agente cliente, contendo uma RSTR (`RequestSecurityTokenResponse`), que contém as credenciais necessárias para que o agente cliente possa executar o serviço. A autenticidade da resposta é garantida por meio de assinaturas digitais e a resposta pode conter informações adicionais, como o tempo de vida das credenciais enviadas e mecanismos de proteção contra ataque de mensagens antigas.
5. Agente cliente invoca o serviço	O agente cliente efetua a requisição ao serviço, enviando também as credenciais obtidas junto ao STS. A invocação é interceptada (por um *handler*) para o devido processo de autorização.
6. Consulta do PEP	O PEP monta um pedido XACML e encaminha o pedido ao PDP, para que este decida sobre a tentativa de acesso.
7. Decisão do PDP	O PDP analisa os atributos relacionados ao usuário e ao recurso e consulta a política de autorização associada ao serviço. Tomada a decisão, o PDP monta uma resposta XACML e envia a mesma para o PEP.
8. Execução	O PEP então aplica a decisão de autorização do PDP, autorizando ou negando a execução do serviço.

Tabela 4.2: Dinâmica de funcionamento.

4.3.2.3 Implementação e Resultados

A aplicabilidade do modelo proposto foi verificada através da implementação de um protótipo, que compreende uma aplicação simplificada de *web banking* e um serviço de autenticação biométrica construídos sobre um suporte de Serviços Web (figura 4.7). Os módulos do cliente, STS e serviço, se valem de manipuladores desenvolvidos em Java. Os manipuladores são responsáveis por capturar, de forma transparente à aplicação, as mensagens SOAP trocadas e realizar o devido processamento nos dados contidos nas mesmas. A troca de mensagens SOAP se vale do protocolo de transporte HTTP.

As escolhas tecnológicas que compõem o protótipo se baseiam no uso de padrões abertos. O Apache [ASF 2004a] é um servidor *web* de código aberto. O Tomcat [ASF 2005b] é sua extensão para um servidor de aplicações Java (*servlets*). Oficialmente endossado pela Sun Microsystems como a implementação de referência para as tecnologias Java Servlet e Java Server Pages, o Tomcat também pode atuar como servidor *web/http* em separado ou pode funcionar integrado a um servidor *web* dedicado, como o `httpd` do Apache ou o Microsoft IIS. O Apache Axis [ASF 2005a] [1] (*Apache eXtensible Interaction System*) é uma extensão com a habilidade de tratar mensagens SOAP por meio

[1] Utilizamos a versão 1.3 do Axis, disponível desde out/2005, por questões de compatibilidade, muito embora já esteja disponível a primeira versão do pacote Axis2, mais eficiente e mais modular que seu antecessor.

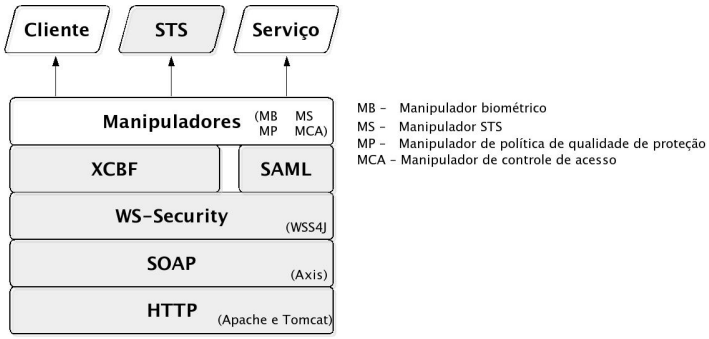


Figura 4.7: Arquitetura do protótipo, com módulos utilizados (fundo cinza) e módulos implementados(fundo branco).

de manipuladores (*handlers*). WSS4J [ASF 2004b] é um módulo que fornece as funcionalidades especificadas na WS-Security, e consiste na implementação de uma biblioteca Java que pode ser usada para assinar e verificar mensagens SOAP. A implementação Apache WSS4J pode ser usada ainda para prover segurança para *web services* desenvolvidos em qualquer servidor de aplicação, mas com suporte especial para Apache Axis. Conta, ainda, com um STS que emite credenciais (*tokens*) nos formatos `UsernameToken`, `TimeStamp` e SAML. Este trabalho acrescentou a funcionalidade de tratamento de credenciais baseadas em dados biométricos. Assim, o protótipo também pode tratar *tokens* no formato `XCBFSecurityToken`. A tabela 4.3 resume a utilização de ferramentas de código aberto por nosso protótipo.

Módulo	Funçao	Referência
Apache	Servidor HTTP	[ASF 2004a]
Tomcat	Extensão do Apache para *servlets* Java	[ASF 2005b]
Axis	Implementação de SOAP	[ASF 2005a]
WSS4J	Implementação de WS-Security	[ASF 2004b]

Tabela 4.3: A implementação do protótipo se baseou amplamente na utilização de ferramentas de código aberto.

Uma característica do Axis que foi bastante usada na construção do protótipo é o uso de **manipuladores** (*handlers*), que são módulos responsáveis por manipular tipos específicos de objetos contidos em uma mensagem SOAP. No lado do cliente, o protótipo consiste em um *applet* Java e um manipulador biométrico. O *applet* é responsável por solicitar os dados de autenticação (agência/conta e credencial biométrica) e invocar as operações bancárias (saldo, extrato, transferências). Os manipuladores são acionados pelo arquivo descritor `wsdd` do Axis, que contém uma referência que explicita quais os manipuladores estão ativos na aplicação [Camargo 2006]. Vários manipuladores foram utilizados: (1) o manipulador STS, que efetua a troca de mensagens entre o cliente e o STS; (2) o manipulador de cifragem e assinatura; (3) o manipulador de política de qualidade de proteção; e, (4) o manipulador de controle de acesso, que incorpora as funções do PEP e do PDP e se responsabiliza pelo controle de acesso. Os manipuladores a seguir foram implementados neste protótipo: (1) o manipulador biométrico cliente, que toma a figura da impressão digital, extrai as minúcias da mesma, efetua a transformação de rotação, cifra e asina os objetos XCBF; e, (2) o manipulador biométrico de verificação, que efetua o processo de decifragem e verificação de assinatura dos objetos XCBF recebidos e efetua a comparação biométrica com o perfil armazenado.

Os manipuladores biométricos são implementações de uma `Interface` Java definida na biblioteca WSS4J, a `Interface CallBackHandler`. Estes manipuladores criam e interpretam o *token* biométrico no formato definido por XCBF. Encapsulando os dados biométricos, existe um identificador único (CBEFF) que permite ao manipulador decidir qual dos comparadores será chamado para tratar os dados biométricos. Os comparadores, tipicamente, são algoritmos proprietários fornecidos por fabricantes especializados em tecnologias biométricas. As chamadas aos comparadores e o formato de dados transferidos são regidos pelas especificações BioAPI (funções), e CBEFF&XCBF (dados). Os comparadores devem seguir tais especificações para alcançar a necessária interoperabilidade ou, em caso contrário, deve ser construída uma camada de tradução. Assim, os dados biométricos gerados no cliente, pelo uso de um determinado dispositivo de aquisição e determinado algoritmo de extração, poderão ser tratados pelo algoritmo de comparação adequado no servidor. A figura 4.7 resume os módulos implementados e utilizados.

O processo de comparação típico da impressão digital é amplamente baseado nos métodos desenvolvidos por especialistas humanos, que 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. A comparação por meios automatizados não segue, necessariamente, os mesmos detalhes de tais orientações, embora esteja baseada nelas de uma maneira estrutural.

A comparação baseada em minúcias é o método mais conhecido e mais largamente usado, 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.

Para contornar a dificuldade de acesso a um dispositivo real de aquisição de impressões digitais, utilizamos um gerador automático. Na nossa implementação, imagens de impressões digitais 288x384 pixels, com resolução de 500dpi, foram geradas pelo programa SFinGe 2.5 (*Synthetic Fingerprint Generator*), um programa livre, gerador automático de impressões digitais e disponibilizado pela Universidade de Bolonha [BIOLAB 2005].

Assim, para se autenticar, o usuário simplesmente escolhe uma das digitais geradas previamente. O manipulador biométrico do agente cliente se encarrega de processar a impressão digital selecionada e encapsular o resultado desse processamento em XCBF. O processamento da digital consiste em extrair características notáveis usadas para comparação (chamadas **minúcias**) e aplicar uma transformação sobre essas características.

Para processamento dos dados biométricos, foi usada parte de um pacote de utilitários de código aberto disponibilizado pelo NIST. O pacote NFIS (*NIST Fingerprint Image Software*) é um conjunto de utilitários com funções de segmentação, extração e comparação de imagens de impressões digitais

[Watson et al. 2002]. 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. Na nossa implementação, utilizamos o detetor de minúcias MINDTCT e o comparador BOZORTH3. MINDTCT localiza e registra terminações bifurcações de linha numa imagem de impressão digital, atribuindo para cada ponto de minúcia uma localização, orientação, tipo e qualidade. BOZORTH3 foi configurado para trabalhar no modo de verificação, e calcula um escore de similaridade entre dois conjuntos de minúcias.

A implementação do STS com suporte a credenciais biométricas foi baseada no STS previamente desenvolvido no nosso grupo de pesquisa, que disponibilizava manipuladores para troca de mensagens entre o cliente e o STS, de cifragem e assinatura de mensagens, de política de qualidade de proteção e de controle de acesso, incorporando as funções do PEP e do PDP [Camargo 2006]. A esta base de código existente foi acrescentado um manipulador para credenciais biométricas, desenvolvido especificamente para este fim. Este manipulador é responsável por extrair a impressão digital (representada por suas minúcias) encapsulada em um objeto XCBF e efetuar a comparação biométrica com o perfil armazenado. Esta comparação é feita invocando o BOZORTH3 que, operando em modo de verificação, é capaz de calcular um escore de similaridade entre dois conjuntos de minúcias. No nosso protótipo, considerou-se que duas impressões são coincidentes quando a similaridade entre elas é igual ou superior a 98%. Os perfis ficam guardados em um repositório simples, tendo sofrido a mesma transformação de rotação e translação aplicada pelo manipulador biométrico do cliente antes de serem armazenados.

Como descrito neste trabalho, na seção 2.1.8, uma transformação não-reversível é útil para alcançar uma característica de revogabilidade para a biometria. Apenas para simular uma transformação nos dados biométricos, foi construído um módulo de rotação e translação, agindo logo após a algoritmo de extração de minúcias, para inserir a transformação desejada. No caso, para cada conjunto de minúcias obtido no cliente, (x, y, θ) foi acrescentada uma translação (Δ_x, Δ_y) e uma rotação Δ_θ. Esta mesma transformação foi aplicada previamente aos perfis biométricos armazenados. Obviamente esta transformação é reversível e não é aplicável na prática.

Os testes realizados tiveram por objetivo uma análise dos resultados considerando a latência média introduzida pelo processamento das mensagens por parte dos manipuladores. Os resultados, que podem ser visualizados na tabela 4.4, foram obtidos após o processamento de 50 interações com o usuário, em 5 datas distintas. Os tempos foram medidos entre o envio da mensagem SOAP para autenticação no STS e a recepção da reposta do serviço pelo agente do usuário, e foram obtidos por meio de pesquisa nos registros em um arquivo de *log* centralizado na máquina A. O esquema de *round trip* foi utilizado para calcular os tempos. Os testes foram realizados em uma rede local Fast Ethernet de 100Mbps, com três computadores dedicados: (A) Pentium IV 2.4 GHz com 512 MB de memória RAM, tendo como sistema operacional o Windows XP; (B) Pentium IV 3 GHz com 1GB de memória RAM e sistema operacional GNU/Linux; e, (C) Athlon XP 2.6 GHz com 512 MB de memória RAM e sistema operacional GNU/Linux. Todas as máquinas se valeram de J2SDK v.1.5.0-01, do servidor

Tipo de objeto biométrico	Latência média (*ms*)
Descoberto	340
Cifrado	437
Cifrado e assinado	527

Tabela 4.4: Resultados - latência média na troca de mensagens.

de aplicações Tomcat v.5.5 e do pacote Axis v.1.3. O cliente foi hospedado na máquina A, o provedor de serviços foi hospedado na máquina B e o STS foi hospedado na máquina C.

4.4 Considerações sobre a segurança

O canal *web banking* está sujeito a uma série de riscos, incluindo fraudes na autenticação de clientes. A autenticação biométrica caracteriza unicamente um indivíduo e não pode ser esquecida ou perdida. A introdução de biometria produz reforço na segurança por meio do aumento de confiança na autenticação dos usuários do canal. Mas e quanto a outros aspectos de segurança envolvidos? A seção 2.1.8 apresenta algumas vulnerabilidades específicas relacionadas a sistemas biométricos em geral. No caso desta aplicação hipotética de *web banking*, vamos tecer algumas considerações sobre estas vulnerabilidades.

- Vulnerabilidades no processo de aquisição - Dadas as características da aplicação de *web banking*, é muito difícil impedir ataques de coerção. No entanto, é possível a utilização de contra-medidas diversionistas. Por exemplo, pode ser analisada a utilização, pelo usuário, de um dos dedos destacado previamente como ”dedo de alarme”. A utilização deste dedo em especial (por exemplo, o dedo médio direito) provocaria a emissão de dados forjados pelo banco para desestimular o criminoso a prosseguir com a coerção (por exemplo, a informação de um saldo muito baixo). Quanto a ataques de personificação e impostação, é necessário que o sistema biométrico esteja equipado para efetuar a detecção de vitalidade, garantindo que um dedo vivo seja apresentado, ao invés de uma cópia artificial ou um dedo arrancado de seu dono.

- Vulnerabilidades nos processos de extração e comparação - Ataques de *hill-climbing* e *swamping* podem ser evitados com contra-medidas simples. Os ataques de *hill-climbing* são evitados com a exibição de respostas sumárias, evitando fornecer informações sobre o escore de comparação ao fraudador ou a qualquer processo por ele introduzido na máquina do cliente. O ataque de *swamping* é evitado com a utilização de algoritmos de comparação de qualidade testada e comprovada. Como persiste a possibilidade de introdução de código malicioso por um potencial fraudador, o ambiente computacional do cliente continua sendo um ponto cujas vulnerabilidades não são mitigadas pela introdução de biometria. No entanto, a segurança nesta ponta pode ser aumentada significativamente por meio da utilização de *smart cards* com dispositivo de aquisição embutido, assunto que tem sido objeto de várias pesquisas. Outras técnicas para aumentar a segurança do sistema cliente são propostas em [Langweg and Kristiansen 2006].

- Vulnerabilidades no processo de registro - Um importante aspecto considerado na proposta é o armazenamento dos perfis biométricos, que é centralizado. Esta decisão possui justificativas

estreitamente ligadas ao perfil de utilização do canal *web banking*. Dentre a totalidade dos clientes do banco, apenas uma parcela se vale destes serviços. Assim, não se justifica a adoção de métodos custosos ou inovadores para a distribuição dos perfis biométricos para os usuários. A criação e gerenciamento, pelo próprio banco, de um banco de dados de perfis biométricos dos usuários se mostra a alternativa mais eficaz. Uma possível alternativa para a geração e distribuição dos perfis seria a contratação de empresa dedicada a este trabalho. No entanto, esta alternativa também não é aconselhável por incluir uma terceira parte no processo de segurança bancária. O armazenamento de perfis biométricos desperta preocupações com privacidade e segurança, uma vez que uma característica biométrica não pode ser revogada. Para evitar tais problemas, pode-se utilizar uma técnica conhecida como biometria cancelável, em que uma transformação não reversível é aplicada sobre os dados biométricos de forma a proteger a característica biométrica original. Em caso de comprometimento, o perfil armazenado pode ser cancelado, e outra variante pode ser criada por meio de outra transformação. Neste modelo, aplica-se uma transformação ao perfil colhido durante o processo de registro dos usuários. A mesma transformação é aplicada no lado do usuário (pelo agente cliente) durante o processo de autenticação. Desta forma, os dados biométricos ficam protegidos tanto no banco de dados de perfis quanto durante a sua transmissão.

- Vulnerabilidade nos canais entre os processos - Uma vez que estamos utilizando biometria cancelável, a transmissão dos perfis está protegido de potenciais fraudadores. Ataques de repetição pasarriam a ser os mais comuns. Para evitar ataques de repeticão, podem ser usadas contramedidas como detecção de repetição e detecção de perfeição, embora estas medidas possam demandar recursos de armazenamento e processamento em nivel proibitivo, dependendo da quantidade de usuários do canal *web banking*. Protocolos de desafio e resposta e estampilhas de tempo, utilizadas em conjunto, tornam-se ferramentas eficazes contra tais ataques.

4.5 Trabalhos relacionados

A literatura acadêmica envolvendo soluções amplas para os sistemas de banco eletrônico em geral e *web banking* em particular, se mostra limitada. A maioria dos documentos disponíveis sobre o assunto consiste em artigos na imprensa, seguindo um estilo informal. Exemplos dessa diversidade de utilização de tecnologias biométricas para a autenticação de pessoas vão desde fechaduras de casas, prédios e portões *high-tech* [Teixeira 2005], passando por acesso e configuração de carros de luxo, como [WebMotors 2005] e [Audi 2005], empresas de planos de saúde [Unimed 2005] e [Making 2005] e acesso privilegiado de cidadãos que desembarcam em um aeroporto internacional [BBC 2006], entre numerosos outros exemplos. Quanto a instituições financeiras em particular, temos um grande banco brasileiro de varejo que iniciou um projeto de autenticação de clientes em seus terminais de auto-atendimento por meio da utilização do padrão vascular da palma da mão descrito por [Lin and Fan 2004], mesma tecnologia utilizada nos terminais de auto-atendimento de alguns bancos japoneses [Celent 2006].

Em termos de trabalhos acadêmicos, uma das exceções é [Shan 2004], onde o autor examina o

ambiente computacional bancário e discute como os Serviços Web podem ser aplicados em sistemas de *e-banking*. Entretanto, a discussão se restringe a aspectos genéricos, sem descrever uma arquitetura de implementação nem detalhar a implementação de processos específicos, como a autenticação de usuários. Embora a capacidade de interoperabilidade proporcionada pela utilização de Serviços Web seja extremamente valiosa, esta tecnologia ainda está imatura e em constante evolução, o que cria dificuldades para os usuários finais para um planejamento realista de larga aplicação desta tecnologia.

Como a Internet é percebida como um meio tipicamente inseguro e promíscuo, permanece o receio de utilização do canal de negócios *web banking*, não somente no Brasil, como em outras partes do mundo. [Hole 2006], descreve cenários de ataque a sistemas de *web-banking* pertencentes a um banco da Noruega. Baseado em tal análise, ele ilustra algumas questões de segurança, a principal das quais aborda a política de segurança com base no desconhecimento dos procedimentos e mecanismos de segurança, como um fator extremamente perigoso tanto para o banco quanto para seus clientes. Ele aponta a necessidade de rforço de segurança no canal de *web banking*, sem no entanto fazer uma proposta concreta de utilização de credenciais biométricas.

Em [Weaver 2004] encontramos socorro à nossa decisão de utilização de Serviços Web, pois ele percebe esta tecnologia como o meio preferencial para conectar aplicações dentro e fora da organização e sugere a representação numérica da confiabilidade da tecnologia de autenticação subjacente, por meio de um Serviço Web que se vale do conceito de níveis de confiança. Por exemplo, é um consenso geral que o nível de confiança NC da íris é maior que o NC da impressão digital, e assim por diante. Esta característica poderia então ser associado ao *token* de autenticação emitido pelo STS, permitindo decisões de autorização baseadas nestes níveis de confiança. Contudo, sua abordagem é bastante genérica e focada na segurança de dados distribuídos, não contemplando análise mais aprofundada do canal *web banking* ou das tecnologias biométricas disponíveis.

A utilização das tecnologias biométricas para autenticação de usuários no canal *web banking* ainda é um assunto aberto para discusões. Um sistema para autenticação biométrica através da *web*, usando como característica biométrica o formato da mão é descrito em [Jain et al. 1998]. Em vez de uma arquitetura distribuída como a proposta neste artigo, os autores consideram uma arquitetura centralizada, onde um único servidor *web* se encarrega de autenticação, autorização e do provimento do serviço. Além disso, não há preocupação com a proteção dos perfis biométricos armazenados, apenas com a dos perfis em trânsito, que são cifrados. Outro exemplo pode ser apreciado em [Everitt and McOwan 2003], onde é apresentado um sistema de verificação biométrico para uso na Internet, dispensando o uso de sensores especiais. A autenticação é efetuada por meio da comparação com o padrão de dinâmica da digitação e movimentação do mouse. No entanto, apenas o sistema biométrico de autenticação é descrito, faltando sua inserção numa arquitetura mais ampla de *web banking*.

Por serem instalações controladas pelos bancos, os terminais de auto-atendimento surgem naturalmente como candidatos à introdução de autenticação biométrica em sistemas bancários. Além do já citado projeto piloto com uso de padrão vascular palmar, [Coventry et al. 2003] discute algumas questões relacionadas com a usabilidade, a partir de uma perspectiva do usuário, de uma implementação piloto de um sistema de autenticação biométrica baseada no padrão da íris neste tipo

de terminal.

Um aspecto não contemplado neste trabalho é a análise do nível de segurança proporcionado pela aplicação típica de *web banking* existente, em comparação com o nível de segurança proporcionado pelo modelo aqui proposto. [Hole 2006], por exemplo, descreve cenários de ataque a sistemas de *web-banking* pertencentes a um banco da Noruega e [Curphey and Araujo 2006] descreve algumas ferramentas e métodos recomendados para testar a segurança de *web sites* e aplicações *web* em geral e [O'Gorman 2003] faz uma comparação entre os pontos fortes e fracos entre as credenciais de conhecimento, posse e biometria.

4.6 Conclusões do capítulo

Este capítulo apresentou uma visão resumida do ambiente computacional de um banco de varejo típico e do canal *web banking* em particular, demonstrando que sua complexidade de plataforma e dependência de sistemas legados clamam por soluções que proporcionem interoperabilidade, como é o caso dos Serviços Web. Um modelo para a autenticação em *web banking* por credenciais biométricas suportadas pelos padrões de Serviços Web foi apresentado, detalhado, e teve um protótipo implementado. A extensão do modelo estudado neste trabalho para um modelo com autenticação baseada em um conjunto mais amplo de credenciais poderia atender melhor as necessidades imediatas dos bancos de varejo.

A introdução de um método de autenticação biométrico pode requerer um contato presencial com cada cliente, para capturar inicialmente o perfil. Ademais, pode ser necessária a presença do cliente para atualização dos perfis biométricos, com o passar do tempo. Alguns clientes podem ser incapazes de produzir um identificador biométrico, temporariamente ou permanentemente, devido a alguma deficiência natural ou adquirida. É sugestão para um trabalho futuro a extensão do modelo aqui proposto, para um modelo mais amplo, que represente uma aplicação de *web banking* com autenticação alternativa baseada em uma credencial obrigatória de conhecimento (como uma senha), o que poderia atender melhor as necessidades imediatas dos bancos de varejo.

Capítulo 5

Conclusão

O serviço de autenticação é fundamental para a segurança de sistemas. A autenticação é geralmente baseada em credenciais de conhecimento, posse e biometria. A biometria é fortemente vinculada a uma identidade e não precisa ser memorizada, nem pode ser esquecida ou emprestada. No entanto, a biometria não é revogável e não é segredo. As credenciais biométricas são as que melhor associam uma identidade a uma pessoa, e sua adoção cresce a cada dia. Pesquisas têm sido levadas a cabo no sentido de eliminar ou amenizar os pontos fracos desta tecnologia.

A escolha de 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. Os fatores de seleção devem ser extraídos dos requisitos da aplicação, de modo a orientar a escolha da tecnologia biométrica mais adequada. A metodologia proposta no capítulo 3 permite comparar tecnologias e escolher a mais adequada. A metodologia é simples e facilmente automatizável. Pode ser calibrada para trabalhar com pontos fortes, na escolha por eleição, ou com pontos fracos, na escolha por eliminação.

Independentemente de qual tecnologia biométrica tenha sido escolhida para compor um sistema biométrico de autenticação, a arquitetura de armazenamento é um aspecto importante no projeto de um sistema biométrico. A comparação entre arquiteturas centralizadas e distribuídas efetuada na seção 2.1.7 possibilita uma melhor compreensão dos pontos positivos e negativos de cada uma.

Os sistemas de *web banking* são uma aplicação popular com fortes requisitos de segurança, dentre os quais a autenticação do usuário é um requisito essencial. O estudo de caso do capítulo 4 mostra como a utilização de tecnologias biométricas pode contribuir para aumentar a confiabilidade da autenticação em sistemas de *web banking*. A tecnologia de Serviços Web permite a incorporação de novas funcionalidades a sistemas de aplicação crítica já existentes, onde é extremamente importante a introdução novas funcionalidades sem impacto significativo na continuidade de funcionamento dos sistemas . Este estudo de caso não encerra a questão da biometria em sistemas de *web banking*. Dentre as possibilidades que podem ser exploradas, a extensão do modelo estudado neste trabalho, que se vale apenas de autenticação biométrica, para um modelo mais amplo, é sugestão para um trabalho futuro. Este modelo mais amplo poderia ser usado para representar uma aplicação de *web banking*

com autenticação baseada em um conjunto mais amplo de credenciais, o que poderia atender melhor as necessidades imediatas dos bancos de varejo. Outro assunto que não foi explorado é a análise do modelo de ameaças, riscos e contra-medidas dos modelo proposto, o que seria extremamente útil no projeto dos sistemas de autenticação biométrica em *web banking*.

A utilização de tecnologias biométricas tem o potencial para se tornar parte importante em sistemas que requerem a autenticação confiável de pessoas. Enquanto tem sido bem sucedida em alguns nichos de mercado, a biometria ainda não cumpriu a sua promessa de autenticação automática e eficiente. Embora haja disponibilidade de sensores biométricos mais baratos e maior poder de computação, a adoção de biometria em larga escala ainda depende da compreensão de três problemas fundamentais: (1) a precisão, ou seja, como representar e reconhecer padrões biométricos com precisão e eficiência; (2) a segurança, ou seja, como garantir que as medidas dos sensores não são fraudulentas; e (3) a privacidade, ou seja, como garantir que a aplicação está de fato usando o reconhecimento de padrões exclusivamente para o propósito declarado. O encaminhamento destes três problemas básicos alavancará a utilização de biometria. Por isso, a biometria poderia ser considerada "um grandioso desafio" [Jain et al. 2004], ou seja, um problema fundamental na ciência e engenharia, com amplo impacto científico e econômico [UKCRC 2005].

De uma maneira geral, as tecnologias biométricas caminham para o amadurecimento. 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. Para sistemas de verificação, a utilização de biometria deve ser cuidadosamente analisada. No caso de haver risco para o usuário, a biometria deve ser utilizada como acessório, ou seja, em conjunto com outras credenciais de conhecimento ou posse. Em particular para instiruições financeiras de grande porte, aspectos relacionados a tecnologias biométricas que precisam ser resolvidos são: (1) a biometria não é revogável, o que exige técnicas de cancelamento de credenciais biométricas em caso de vazamento, e (2) a biometria não é segredo, o que exige técnicas que aumentem a resistência dos sistemas contra a fraude de personificação.

Companhias fabricantes e usuárias que planejam implementar a tecnologia de sistemas biométricos automatizados devem refletir sobre as principais questões que desafiam tais sistemas. Tais desafios necessitam de uma solução abrangente que satisfaça às legítimas preocupações dos usuários [Chandra and Calderon 2005]. As recomendações a seguir são fruto da reflexão proporcionada por este trabalho:

- Estimativa de erros - o material promocional de sistemas biométricos relata pobremente as taxas de erros e as aplicações de laboratório relatam taxas de erros obtidas em condições ideais e controladas. Em aplicações reais, é bem provável que as taxas de erros encontradas sejam muito superiores às documentadas.

- Identificação x Verificação - Instituições financeiras de grande porte, que normalmente possuem aplicações com grande número de usuarios e cujo processo de autenticação requer uma resposta imediata, devem usar sistemas de verificação (busca $1:1$) em detrimento dos sistemas de identificação (busca $1:N$), cujo desempenho pode comprometer a aplicação.

- Procedimentos de avaliação - a avaliação de tecnologia é um meio razoável e barato de comparar os números de precisão de diferentes comparadores, mas para projetos reais de grande porte é necessário conduzir uma avaliação de cenário ou avaliação operacional, quando então o sistema pode ser testado quanto ao desempenho, usabilidade e robustez.

- Utilização conjunta - é altamente recomendável a utilização de credenciais biométricas em conjunto com outras credenciais de conhecimento ou posse. Isso não apenas aumenta o nível de confiança na autenticação do usuário como permite um ajuste menos rigoroso do limiar de comparação biométrica, oferecendo assim um nível aceitável de conveniência para o usuário mesmo em um momento pioneiro em que a precisão da tecnologia adotada esteja abaixo da ideal.

- Registro - o processo de registro deve ser projetado com especial cuidado para preservar a segurança da autenticação e a qualidade do banco de dados dos perfis biométricos.

- Biometria cancelável - deve ser utilizada esta técnica como um meio de proporcionar uma resposta às questões de segurança e privacidade oriundas do armazenamento e gerenciamento de perfis biométricos, particularmente no cenário de utilização pioneiro apresentado na seção 2.1.7.

Alguns resultados concretos podem ser extraídos desta dissertação. A metodologia apresentada na seção 3.2 pode ser adotada para a avaliação preliminar de sistemas biométricos em aplicações específicas, particularmente em instituições financeiras de grande porte. O modelo de *web banking* com autenticação biométrica e utilização de Serviços Web apresentado na seção 4 é uma alternativa de solução para sistemas bancários via Internet. A pesquisa efetuada durante a dissertação resultou na publicação de um minicurso [Costa et al. 2006] e de um artigo [Costa et al. 2007]. Fica como sugestão para trabalhos futuros investigar técnicas para reforçar a segurança da plataforma cliente, assunto pouco explorado no modelo apresentado. Uma alternativa promissora é a abordagem de utilização dos processos de aquisição, extração e comparação embutidos em *smart cards*, o que pressupõe dispositivos de aquisição construidos no próprio cartão. Esta alternativa pode apresentar um alto nível de confiabilidade, desde que apropriadamente construida levando em consideração as particularidades do sistema de *web banking*.

Referências Bibliográficas

[Akkermans et al. 2005] Akkermans, A. H. M., Kevenaar, T. A. M., and Schobben, D. W. E. (2005). Acoustic ear recognition for person identification. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*, 0:219–223.

[ANSI 2003] ANSI (2003). Biometric information management and security for the financial services industry. Standard 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.

[ASF 2004a] ASF (2004a). *The Apache Software Foundation Homepage*. Disponível em `http://www.apache.org`.

[ASF 2004b] ASF (2004b). *WSS4J Project Documentation*. The Apache Software Foundation. Documentação disponível em `http://ws.apache.org/wss4j/`.

[ASF 2005a] ASF (2005a). *Axis Architecture Guide v1.3*. The Apache Software Foundation. O pacote Axis pode ser encontrado em `http://ws.apache.org/axis`.

[ASF 2005b] ASF (2005b). *Tomcat Project Documentation*. The Apache Software Foundation. Documentação disponível em `http://tomcat.apache.org`.

[Ashborn 2004] Ashborn, J. (2004). *Practical Biometrics: from Aspiration to Implementation*. Springer Professional Computing, 1st edition.

[Audi 2005] Audi (2005). Site institucional. Audi USA - The 2005 Audi A8 Sedan - Available on-line at http://www.audiusa.com, acessed on July 31 2005.

[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 *4^{th} 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.

[BBC 2006] BBC (2006). Heathrow eye scan checks extended. Available on-line at `http://news.bbc.co.uk/1/hi/england/london/4792206.stm`.

[BC 2006] BC (2006). Biometric Consortium. Site disponível em `http://www.biometrics.org`, acessado wm nov/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.

[BioAPI 2001] BioAPI (2001). *BioAPI Specification Version 1.1*. The BioAPI Consortium. Disponível em www.bioapi.org.

[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, 1^{st} 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.

[Bonastre 2005] Bonastre, J.-F. (2005). LIA_RAL . Disponível no site da l'Université d'Avignon, em http://www.lia.univ-avignon.fr/heberges/ALIZE/LIA_RAL/index.html.

[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.

[BWG 2001] BWG (2001). Biometric device protection profile (bdpp). Technical Report Draft Issue 0.82, Biometrics Working Group, UK.

[Camargo 2006] Camargo, E. T. (2006). Transposição de autenticação e de autorização em arquiteturas orientadas a serviços. Dissertação de mestrado, PGEEL/UFSC, Florianópolis, SC.

[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.

[CASIA 2006] CASIA (2006). Casia (Chinese Academy of Sciences, Institute of Automation) Iris Image Database. Disponível em http://nlpr-web.ia.ac.cn/english/irds/resources.htm, acessado em julho/2006.

[Celent 2006] Celent (2006). Biometric ATMs in Japan: Fighting fraud with vein pattern authentication. avalilable on-line at http://www.celent.com.

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

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

[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.

[Costa et al. 2006] Costa, L. R., Obelheiro, R. R., and Fraga, J. S. (2006). Introdução aos sistemas biométricos. In *Minicursos do SBSeg 2006*, Santos, SP.

[Costa et al. 2007] Costa, L. R., Obelheiro, R. R., and Fraga, J. S. (2007). Autenticação em *Web Banking* por credenciais biométricas suportadas pelos padrões de Serviços Web. In *SBRC 2007*. Aceito para publicação.

[Coventry et al. 2003] Coventry, L., Angeli, A. D., and Johnson, G. (2003). Usability and biometric verification at the atm interface. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 153–160, New York, NY, USA. ACM Press.

[CSU 2003] CSU (2003). Colorado State University Face Identification Evaluation System. Disponível em http://www.cs.colostate.edu/evalfacerec/.

[CUHK 2006] CUHK (2006). CUHK Iris Image Dataset. Disponível em http://www2.acae.cuhk.edu.hk/~cvl/main_database.htm, acessado em julho/2006.

[Curphey and Araujo 2006] Curphey, M. and Araujo, R. (2006). Web application security assessment tools. *IEEE Security and Privacy*.

[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 1999] Daugman, J. G. (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 2004] Daugman, J. G. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30.

[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.

[Decoster et al. 2001] Decoster, W., Gysel, A. V., Vercammen, J., and Debruyne, F. (2001). Voice similarity in identical twins. *Acta oto-rhino-laryngologica belgica*, 55(1):1–42.

[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.

[Everitt and McOwan 2003] Everitt, R. A. J. and McOwan, P. W. (2003). Java-based Internet biometric authentication system. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1166–1172.

[Febraban 2006] Febraban (2006). Setor bancário em números. Technical report, Federação Brasileira de Bancos, Disponível em `http://www.febraban.org.br`.

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

[Godik and Parducci 2002] Godik, S. and Parducci, B. (2002). OASIS eXtensible Access Control 2 Markup Language (XACML) 3. Technical report, OASIS.

[Grgic and Delac 2007] Grgic, M. and Delac, K. (2007). Face recognition homepage. Portal com inúmeros recursos disponível em `http://www.face-rec.org`, acessado em fevereiro/2007.

[Gross 2005] Gross, R. (2005). Face databases. In S.Li, A., editor, *Handbook of Face Recognition*. Springer, New York.

[Gruber et al. 2006] Gruber, C., Hook, C., and Sick, J. K. G. S. B. (2006). A flexible architecture for online signature verification based on a novel biometric pen. *IEEE Mountain Workshop on Adaptive and Learning Systems*, 1-4244-0166-6/06:110–115. BISP Projetc disponível em `http://www.bisp-regensburg.de/`.

[Gupta et al. 2004] Gupta, M., Rao, R., and Upadhyaya, S. (2004). Electronic Banking and Information Assurance Issues. *Journal of Organizational and End User Computing*, 16(3):1–21.

[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.

[Hole 2006] Hole, K. (2006). Case study: Online banking security. *IEEE Security and Privacy*, 4(2):14–20.

[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.

[iAfB 2007] iAfB (2007). International association for biometrics glossary. Glossário disponível em `http://www.afb.org.uk/docs/glossary.htm`, acessado em janeiro/2007.

[IBG 2005] IBG (2005). Independent testing of iris recognition technology. Technical Report NB-CHC030114/0002, International Biometric Group.

[IBIA 2006] IBIA (2006). International biometric industry association. Site disponível em /urlhttp://www.ibia.org, acessado em dez/2006.

[INTEL 2000] INTEL (2000). Open source computer vision library. Disponível em `http://www.intel.com/technology/computing/opencv/index.htm`.

[ISO 2006] ISO (2006). *ISO 19092-1 e 19092-2. Financial Services – Biometrics – Part 1: Security Framework and Part 2: Message syntax and cryptographic requirements.* International Organization for Standardization, Disponível em `http://www.iso.org`.

[Jain et al. 1999] Jain, A. K., Prabhakar, S., Hong, L., and Pankanti, S. (1999). FingerCode: A filterbank for fingerprint representation and matching. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2:187–195.

[Jain et al. 1998] Jain, A. K., Prabhakar, S., and Ross, A. (1998). Biometrics-based web access. Technical Report MSU-CPS-98-33, Michigan State University.

[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.

[Kearney et al. 2004] Kearney, P., Chapman, J., Edwards, N., Gifford, M., and He, L. (2004). An overview of Web Services security. *BT Technology Journal*, 22(1):27–42.

[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.

[Kong et al. 2006] Kong, A., Zhang, D., and Guangming, L. (2006). A study of identical twins' palmprints for personal authentication. In *International Conference on Biometrics*, volume 3832, pages 668–674, Berlin. Springer.

[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".

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

[Langweg and Kristiansen 2006] Langweg, H. and Kristiansen, T. (2006). Extending the Trusted Path in Client-Server Interaction. *arXiv:cs.CR/0611102*, 1.

[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.

[Lin and Fan 2004] Lin, C.-L. and Fan, K.-C. (2004). Biometric verification using thermal images of palm-dorsa vein patterns. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:199–213.

[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.

[Making 2005] Making (2005). Unimed - caso de sucesso. http://www.making.com.br. Acessado em 20.jul.2005.

[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.

[Matsumoto et al. 2002] Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. (2002). Impact of artificial gammy fingers on fingerprint systems. In *Proceedings of SPIE*, volume 4677.

[Mello et al. 2006] Mello, E. R., Wangham, M. S., Fraga, J. S., and Camargo, E. S. (2006). Segurança em serviços web. In *Minicursos do SBSeg 2006*, Santos, SP.

[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 1999] NIST (1999). *The Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm*. As especificações do codificador/decodificador WSQ podem ser encontradas em `ftp://wwwc3.lanl.gov/pub/misc/WSQ/`.

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

[NIST 2002] NIST (2002). *Biometric Application Programming Interface (API) for Java Card*. NIST/Biometric Consortium Biometric Interoperability, Assurance, and Performance Working Group, 1.1 edition. Doc 02-0019.

[NIST 2003a] NIST (2003a). Facial recognition technology database. Disponível em `http://www.nist.gov/humanid/colorferet/home.html`.

[NIST 2003b] NIST (2003b). 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.

[NIST 2007] NIST (2007). Nist Fingerprint Image Software 2 (NFIS2). Disponível em /urlhttp://fingerprint.nist.gov/NFIS/, acessado em fevereiro/2007.

[Nordin 2004] Nordin, B. (2004). *Match-on-Card Technology*. Precise Biometrics Inc., `http://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/`.

[OASIS 2006] OASIS (2006). *Web Services Security: SOAP Message Security 1.1*. Organization for the Advancement of Structured Information Standards (OASIS).

[O'Gorman 2003] O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040.

[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.

[PIDS 2001] PIDS (2001). *CORBA Person Identification Service Specification v1.1*. Object Management Group, Disponível em `www.omg.org`.

[Proença and Alexandre 2005] Proença, H. and Alexandre, L. A. (2005). Ubiris: A noisy iris image database. In *Proceed. of ICIAP 2005 - Intern. Confer. on Image Analysis and Processing*, volume 1, pages 970–977.

[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.

[Rhodes 1956] Rhodes, H. T. F. (1956). *Alphonse Bertillon: Father of Scientific Detection*. Abelard-Schuman, New York.

[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.

[Shan 2004] Shan, T. (2004). Building a service-oriented eBanking platform. *Proceedings of the IEEE International Conference on Services Computing (SCC'04)*, pages 237–244.

[Sklira et al. 2003] Sklira, M., Pomportsis, A., and Obaidat, M. (2003). A framework for the design of bank communications systems. *Computer Communications*, 26(15):1775–1781.

[Tarbell 2005] Tarbell, I. M. (2005). Identification of criminals: The scientific method used in France. http://chnm.gmu.edu/courses/magic/plot/bertillon.html.

[Teixeira 2005] Teixeira, C. A. (2005). Meu corpo é minha senha. http://www.revistaoi.com.br. Acessado em 15.jul.2005.

[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.

[Turney 1993] Turney, P. D. (1993). Exploiting context when learning to classify. *Proceedings of the European Conference on Machine Learning*.

[UCL 2005] UCL (2005). M2VTS project: Multi-modal biometric person authentication. http://www.tele.ucl.ac.be/PROJECTS/M2VTS/. Université Catholique de Louvain (Belgium), acesso em 23.nov.2005.

[UKCRC 2005] UKCRC (2005). Grand challenges: The background. Site do UK Computing Research Committee. Disponível on-line em http://www.ukcrc.org.uk, acessado em 31.out.2005.

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

[Unimed 2005] Unimed (2005). Site institucional. UNIMED - https://www.unimedflorianopolis.com.br. Acessado em 20.jul.2005.

[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.

[Watson et al. 2002] Watson, C., Garris, M., Tabassi, E., Wilson, C., McCabe, R., and Janet, S. (2002). Users Guide to NIST Fingerprint Image Software 2 (NFIS2). *NIST, Tech. Rep.,(Available at http://fingerprint. nist. gov/NFIS/)*.

[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.

[Weaver 2004] Weaver, A. (2004). Enforcing distributed data security via Web Services. *Proceedings of the IEEE International Workshop on Factory Communication Systems*, pages 397–402.

[WebMotors 2005] WebMotors (2005). O site do carro. Disponível on-line em http://www.webmotors.com.br/wmpublicador/Testes.vxlpub?hnid=32318, acessado em 15.julho.2005.

[Woodard and Flynn 2005] Woodard, D. L. and Flynn, P. J. (2005). Finger surface as a biometric identifier. *Computer Vision Image Understanding*, 100(3):357–384.

[WS-Trust 2005] WS-Trust (2005). *Web Services Trust Language (WS-Trust)*. `http://msdn.microsoft.com/library/en-us/dnglobspec/html/WS-Trust.asp`.

[WSS-XCBF 2002] WSS-XCBF (2002). *Web Services Security XCBF Token Profile*. OASIS, working draft 1.0 edition.

[XM2VTS 2006] XM2VTS (2006). The extended M2VTS database. Disponível em no site da Surrey Univesity, em `http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/`, acessado em julho/2006.

[Yavatkar et al. 2000] Yavatkar, R., Pendarakis, D., and Guerin, R. (2000). A framework for policy-based admission control. IETF RFC 2753.

[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.

[Yörük et al. 2006] Yörük, E., Konukoglu, E., Sankur, B., and Darbon, J. (2006). Shape-based hand recognition. *IEEE Transactions on Image Processing*, 15(7):1803–1815.

[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.