UNIVERSIDADE DE BRASÍLIA
CENTRO DE FORMAÇÃO DE RECURSOS HUMANOS EM TRANSPORTES

TECNOLOGIAS DE CONTROLE DE ACESSO E SUA APLICAÇÃO NO SISTEMA DE SEGURANÇA AEROPORTUÁRIA

SÉRGIO SANTIAGO RIBEIRO

ORIENTADORA: YAEKO YAMASHITA

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DA AVIAÇÃO CIVIL

PUBLICAÇÃO: E-TA-002A/2008
BRASÍLIA/DF: JUNHO/2008

UNIVERSIDADE DE BRASÍLIA

CENTRO DE FORMAÇÃO DE RECURSOS HUMANOS EM TRANSPORTES

TECNOLOGIAS DE CONTROLE DE ACESSO E SUA APLICAÇÃO NO SISTEMA DE SEGURANÇA AEROPORTUÁRIA

SÉRGIO SANTIAGO RIBEIRO

MONOGRAFIA DO CURSO DE ESPECIALIZAÇÃO EM GESTÃO DA AVIAÇÃO CIVIL SUBMETIDA AO CENTRO DE FORMAÇÃO DE RECURSOS HUMANOS EM TRANSPORTES DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DA AVIAÇÃO CIVIL

APROVADA POR:

_____

YAEKO YAMASHITA, PhD (UNB)
(Orientadora)

_____

ADYR DA SILVA, PhD (UnB)
(Examinador)

_____

JOAQUIM JOSÉ GUILHERME DE ARAGÃO, PhD (UnB)
(Examinador)

BRASÍLIA/DF, 20 DE JUNHO DE 2008

FICHA CATALOGRÁFICA

RIBEIRO, SERGIO SANTIAGO

Tecnologias de Controle de Acesso e Sua Aplicação no Sistema de Segurança Aeroportuária

xiii, 82p., 210x297mm (CEFTRU/UnB, Especialista, Gestão da Aviação Civil, 2008).

Monografia de Especialização - Universidade de Brasília, Centro de Formação de Recursos Humanos em Transportes, 2008

1. Introdução	2. Segurança Operacional em Aeroportos
3. Tecnologias de Acesso	4. Análise da Tecnologia do Sistema Biométrico Utilizados para Controle de Acesso
I. CEFTRU/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

RIBEIRO, S. S. (2008). Tecnologias de Controle de Acesso e Sua Aplicação no Sistema de Segurança Aeroportuária. Monografia de Especialização, Publicação E-TA-002A/2008, Centro de Formação de Recursos Humanos em Transportes, Universidade de Brasília, Brasília,DF, 82 p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Sérgio Santiago Ribeiro

TÍTULO DA MONOGRAFIA: Tecnologias de Controle de Acesso e Sua Aplicação no Sistema de Segurança Aeroportuária.

GRAU/ANO: Especialista/2008

_____

Sérgio Santiago Ribeiro

DEDICATÓRIA

Dedico este trabalho a meus familiares, em especial aos meus Pais, meu Filho e Deus, que são as principais razões de felicidade em nossas vidas e por me guiar em todos os momentos.

AGRADECIMENTOS

A minha orientadora Professora. Yaeko Yamashita , PhD, aos nossos mestres e colegas de curso, que com suas experiências profissionais e conhecimentos nos permitiram crescer como pessoa e profissional.

.

RESUMO

TECNOLOGIAS DE CONTROLE DE ACESSO E SUA APLICAÇÃO NO SISTEMA DE SEGURANÇA AEROPORTUÁRIA

Países em desenvolvimento e de dimensões continentais utilizam o transporte aéreo para promoverem a integração nacional, uma vez que, em muitos casos, esta e a única modalidade de transporte disponível. A segurança dos Aeroportos é uma questão que deve ser tratada com muito cuidado e dedicação, visto os parâmetros mundiais, com atentados, utilização de aeronaves como armas e outras situações anormais dos nossos aeroportos. A melhoria continua da segurança deve ser um objetivo a ser atingido, e para isto, devemos buscar os avanços tecnológicos para auxiliar no alcance desse objetivo. A biometria já é utilizada em diversos campos, principalmente para controle de acesso a sistemas ou áreas restritas. Avanços tecnológicos de biometria são apresentados nesta monografia, além da sua utilização para controle de acesso e identificação de funcionários do Aeroporto visando o aumento da segurança e minimização dos riscos contra a aviação civil.

ABSTRACT

SECURITY OF TECNOLOGY

Developing countries with huge continental dimensions use air transportation to increase national unity, once that, in many cases, this is the only category of transportation available. The security of airports is a subject that needs to be treated carefully and with dedication, as it's seen on the international parameters of the countries that face attacks using airplanes as destructive arms and other unconventional situations in airports. The increasing security of airports is a goal to be reached, and for that, we shall look for technological breakthroughs to help in the achievement of this aim. The biometry is already used in many areas, mainly to control the access to systems or restricted areas. Technological advances in biometry are presented in this monograph, besides the use of access control and identification of airport employees aiming on the increase of security and the decrease of risks against civil aviation.

.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ACDT	Acidente
AIB	Aeroporto Internacional de Brasília
ANAC	Agência Nacional de Aviação Civil
CAT REQ	Categoria requerida
CBA	Código Brasileiro de Aeronáutica
DAC	Departamento de Aviação Civil
DIE	Divisão de Infra-estrutura
IAC	Instrução de Aviação Civil
ICA	Instrução do Comando da Aeronáutica
ICAO	International Civil Aviation Organization
IMA	Instrução do Ministério da Aeronáutica
INFRAERO	Empresa Brasileira de Infra-estrutura Aeroportuária
NSCA	Norma de Sistema do Comando da Aeronáutica
NSMA	Norma de Sistema do Ministério da Aeronáutica
NTSB	National Transportation Safety Board
OACI	Organização da Aviação Civil Internacional
OCSISCON	Órgão Central do Sistema Contra Incêndio
OSV	Oficial de Segurança de Vôo
PEAA	Plano de emergência Aeronáutica em Aeródromo
PPP	Parcerias públicas Privadas
SAC	Seção de Aviação Civil
SERAC	Segundo Serviço Regionais de Aviação Civil
SGSO	Sistema de Segurança da Segurança Operacional
SIE	Subdepartamento de Infra-estrutura do DAC
TPS	Terminal de Passageiros

1 INTRODUÇÃO

1.1 APRESENTAÇÃO

O dia 11 de setembro de 2001 ficará na história, não apenas como o do maior atentado terrorista a uma nação em tempo de paz, mas segundo alguns historiadores, como o do início efetivo do século XXI. Os estilhaços do World Trade Center feriram não só o coração e o orgulho americano, mas atingiram os negócios no mundo, principalmente o negócio da aviação. Os órgãos administradores e fiscalizadores dos aeroportos brasileiros, a partir desse dia se viram no meio de um fogo cruzado de informações e questionamentos da mídia, voltados principalmente para a segurança das viagens aéreas e dos aeroportos.

O avião, de um dos meios de transporte mais seguros do mundo, passou a ser questionado pela ameaça que representava para a segurança do País. O terrorismo transformou o aeroporto em um potencial risco à segurança das nações. Para que viajar de avião não fosse sinônimo de “pesadelo” foi preciso um cuidadoso trabalho de comunicação, que utilizou ferramentas básicas de gestão em tempo de crise. O resultado dessa estratégia acabou rendendo um subproduto: enfrentar uma crise com ações proativas e corretas pode ser uma boa oportunidade para maximizar a imagem da aviação aérea, mesmo depois da crise.

Até a década de 50, ninguém se preocupava com passageiros armados, porque nunca havia sido registrado um seqüestro de avião. Foi depois dos primeiros crimes que, em 1961, organismos internacionais proibiram a entrada de pessoas com armas de fogo nas aeronaves.

Porém, a discussão sobre a segurança na aviação comercial brasileira pouco avançou nos últimos anos, desde o primeiro atentado a bomba na história do país, em 9 de julho de 1997. Uma explosão em um vôo de um Fokker 100 da TAM, no qual viajavam 55 pessoas, feriu sete e matou uma arremessada para fora do avião.

O primeiro mandamento dos manuais de crise diz que para enfrentar situações difíceis é estar vigilante e preparado, prever situações difíceis que possam acontecer e estabelecer uma boa estratégia de comunicação.

Muitas situações perigosas e anormais à aviação civil podem ser evitadas, caso exista um bom sistema de controle de acesso e identificação de funcionários, tripulantes e até passageiros. Dessa forma, esta monografia destina-se a descrever e demonstrar, metodologicamente, o desenvolvimento tecnológico no controle de acesso e sua aplicação no sistema de segurança aeroportuária, a fim de sensibilizar as autoridades e a comunidade aeronáutica para soluções com aplicação do desenvolvimento tecnológico em benefício da segurança aeroportuária.

O estudo mostrará as características da biometria e suas variantes, buscando apresentar seus pontos positivos e negativos, propondo sua utilização no aeroporto Juscelino Kubitschek, administrado pela INFRAERO, para a sua melhoria nos sistemas de segurança e controle de acesso.

Este capítulo se compõe de 7 seções, onde na seção 2, após esta apresentação será abordada a contextualização da problemática que gerou este estudo. Assim, seguindo temos na seção 3 a hipótese que direcionou o desenvolvimento da pesquisa. Na seção 4, o objetivo que baseada na hipótese foi definido, na seção 5 a justificativa. A metodologia é explicada na seção 6 e finalmente na seção 7 é apresentada a estrutura dessa monografia.

1.2 PROBLEMA

A segurança em grandes aeroportos, de passageiros, funcionários e usuários vem se tornando cada vez mais sério, levando em conta questões como a segurança de vôo ou o terrorismo. Todo o acesso público ou restrito a um aeroporto é canalizado através do terminal, onde cada passageiro, usuário ou funcionário passa pelo detector de metal e todos os seus pertences passam por um equipamento de inspeção. Os seguranças do aeroporto também podem ordernar uma revista completa numa pessoa e/ou na bagagem desta. Além de objetos considerados de riscos à integridade fisica, (armas de fogo, facas, tesouras, etc), também são proibidos objetos que ponham em risco a integridade do vôo, (isqueiros, materiais inflamáveis ou explosivos, etc). Problemas como a falta de verbas podem fazer com que tais medidas de segurança não sejam tão efetivos como deveriam, aumentando muito a probabilidade de atentados, seqüestros ou outros atos ilicitos.

Uma das medidas de segurança mais importantes em um aeroporto é confirmar a identidade dos passageiros, credenciais de funcionários e tripulantes. Isso é feito pela verificação da foto

em um documento de identidade ou credencial. Entretanto, olhar rapidamente a foto do documento de identificação ou credencial não basta, é necessário uma tecnologia capaz de melhorar e facilitar a identificação e liberação de acesso dos usuários. Uma tecnologia imprescindível é a biometria, que verifica impressões digitais, o mapeamento da retina ou características faciais e pessoais usando sistemas complexos de computador para detectar se o passageiro ou funcionário é quem diz ser.

Sistemas de reconhecimento biométrico são utilizados quase sempre visando à garantia da segurança. Atualmente, existem várias estratégias biométricas de autenticação de usuários que já estão sendo utilizadas em aplicações comerciais. De forma a tornar os sistemas mais aceitáveis e utilizáveis, deve-se tanto buscar as soluções de menor custo, de maior confiabilidade e de maior simplicidade no que ser refere a seus procedimentos de utilização.
E assim a questão a ser respondida é: **Como aumentar a segurança de conferência de identidade e o controle de acesso, nos aeroportos brasileiros?**

1.3 HIPÓTESE

A maioria dos aeroportos não utiliza o desenvolvimento tecnológico em benefício do sistema de controle de acesso, devido à falta de investimento no setor, bem como de seus recursos externos. Conseqüentemente, vários atos ilícitos vêem ocorrendo no sistema de Aviação Civil. Assim adotou-se a premissa de que os sistemas biométricos podem auxiliar na melhoria da segurança no controle de acesso nos aeroportos brasileiros.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Analisar as tecnologias baseadas em controle de posse e biometria que auxiliem na melhoria da segurança no controle de acesso nos aeroportos brasileiros.

1.4.2 Objetivos Específicos

- Verificar a existência de legislação relativa ao assunto;

- Identificar as técnicas de reconhecimento biométrico disponíveis no mercado;
- Análise da necessidade de melhoria dos sistemas de controle de acesso no aeroporto Juscelino Kubistchek.

1.5 JUSTIFICATIVA

O sistema de segurança aeroportuária vem se modificando durante os tempos, o nível de ameaça vem aumentando a cada ano e o risco de atos ilícitos praticados contra a aviação civil. O terrorismo tem sido um problema para as companhias aéreas e para os passageiros desde os anos 70. Nessa época, seqüestros e bombas se tornaram a opção preferida pelas organizações extremistas em todo o mundo. Mesmo que a segurança nos aeroportos tenha se intensificado, os ataques de 11 de setembro fizeram muitas pessoas ficarem alertas para uma dura realidade: a segurança ainda não era suficiente. Nos sistemas atuais de inspeção de passageiros (figura 01.) não existe um sistema confiável de identificação de passageiros.

Figura 1.1 Imagem Cedida por Federal Aviation Administration (FAA). Milhões de Pessoas Viajam de Avião Todos os Dias

Quando se fala em aviação civil, deve-se ressaltar que os indicadores da movimentação de passageiros e aeronaves são bastante expressivos. O Brasil conta com a segunda maior frota de aviões do mundo, sendo menor apenas que a dos Estados Unidos da América, e está entre as maiores indústrias de transporte aéreo em termo de passageiros/km transportados.

Desde os primórdios da aviação comercial, buscou-se uma forma de aperfeiçoar o sistema de

controle de acesso, visando aumentar a confiança dos usuários e funcionários do aeroporto, o que era imprescindível para o bom desenvolvimento dos trabalhos realizados no aeroporto.

Este estudo surgiu da necessidade de comprovar a existência da falta de aplicação de recursos tecnológicos mais avançados nos sistemas de controle de acesso, identificando a importância para a segurança aeroportuária contra atos de interferência ilícita.

1.6 METODOLOGIA DE PESQUISA

O estudo adota a abordagem hipotética dedutiva com procedimentos de observação indireta. O método hipotético-dedutivo é lógico por natureza, não se limita à generalização empírica das observações realizadas, podendo-se, por meio dele, chegar à construção de teorias e leis.

A metodologia abrangeu a seguinte seqüência de atividades:

1- Revisão bibliográfica: aborda temas como segurança da aviação civil, tecnologias de segurança, legislação da aviação civil e biometria com controle de acesso utilizando teses, monografias, livros, internet
2- Análise da tecnologia de segurança da aviação civil baseada nos conceitos de biometria e custos.
3- Análise da necessidade de melhoria dos sistemas de controle de acesso nos aeroportos brasileiros baseada na legislação da aviação civil e pesquisa por meio do levantamento de dados junto às áreas de engenharia e financeira da INFRAERO, para que, depois de analisados, esses resultados sirvam de base para comprovar as hipóteses apresentadas, validando a metodologia escolhida.
4- Análise de adequação do uso da tecnologia baseada na biometria para aumentar a segurança nos aeroportos.

1.7 ESTRUTURA DA MONOGRAFIA

O estudo para atingir os seus objetivos foi estruturado em 5 capítulos identificados a seguir:

Capítulo 1 - Introdução. Este capítulo tem como objetivo apresentar o problema, hipóteses, objetivo geral e específico, a justificativa e a metodologia utilizada na pesquisa.

Capítulo 2 – Segurança Operacional em Aeroportos. Este capítulo tem como objetivo apresentar uma visão geral sobre a segurança aeroportuária e a legislação aeronáutica relacionada à segurança em aeroportos.

Capítulo 3 – Tecnologias de Acesso. Este capítulo tem como objetivo apresentar os principais conceitos envolvendo os sistemas biométricos.

Capitulo 4 – Análise da Tecnologia do Sistema Biométrico Utilizados para Controle de Acesso. Este capitulo faz uma análise da tecnologia aplicada, levando em consideração todo contexto.

Capitulo 5 - Conclusão

Capitulo 6 - Referência Bibliográfica

2 SEGURANÇA OPERACIONAL EM AEROPORTOS

2.1 APRESENTAÇÃO

Este capítulo tem como objetivo levantar informações sobre a segurança operacional em aeroportos e apresentar a legislação aeronáutica existente. Atualmente, o gerenciamento da segurança operacional tem um papel importante na moderna administração. Desta maneira, na seção 2.2 são apresentados alguns conceitos importantes relativos à segurança aeroportuária.

O Direito Aeronáutico aborda as relações jurídicas vinculadas com a navegação aérea, o transporte aéreo no campo doméstico e internacional e a aviação civil em geral. É um Direito dinâmico para poder acompanhar as constantes alterações e a modernidade que flui do progresso e da tecnologia aplicada à aviação civil. As seções 2.4, 2.5 e 2.6 apresentam a IAC 107-1004 que estabelece os procedimentos que devem ser adotados nos aeroportos civis brasileiros, a IAC 107-1003 que estabelece os procedimentos para ativação e funcionamento da Comissão de Segurança Aeroportuária (CSA) e o Código Brasileiro de Aeronáutica.

2.2 SEGURANÇA OPERACIONAL EM AEROPORTOS

A gerência de qualquer organização, seja de grande ou pequeno porte, exige atenção a diversos fatores: finanças, orçamento, pessoal, recursos materiais, equipamentos, etc. Mais recentemente, entre esses fatores, têm-se incluído nessa lista a segurança operacional. (Costa, 2007).

O quesito segurança nos aeroportos e nas atividades de transporte aéreo sempre ocupou uma posição de destaque e relevância nos assuntos debatidos pela comunidade aeroportuária. Autoridades aeronáuticas, companhias aéreas, administradoras de aeroportos e empresas de serviços de apoio em terra, cada vez mais direcionam investimentos no sentido de aprimorar e desenvolver melhores práticas nessa área.

Inúmeras ocorrências são registradas por dia em aeroportos de todo o mundo, desde tentativas de atos ilícitos, como embarque de artefatos explosivos, até acidentes na pista, envolvendo

equipamentos de rampa e operadores. Em um segmento onde um pequeno erro pode levar a conseqüências de grandes proporções, cada procedimento deve ser seguido e revisto rigorosamente e a proatividade na prevenção de acidentes deve ser prioridade na gestão dos aeroportos.

A segurança operacional em aeroportos é a situação no qual o risco de lesões às pessoas ou danos às propriedades é reduzido e mantido em, ou abaixo de, um nível aceitável, mediante um contínuo processo de identificação de perigos e gerenciamento de riscos (Costa, 2007).

O Perigo é condição, objeto ou atividade que potencialmente pode causar lesões ao pessoal, danos aos equipamentos ou estruturas, morte, ou redução da habilidade de desempenhar uma função determinada. E o risco é a possibilidade de perda ou dano, medida em termos de severidade e probabilidade.

A segurança dos aeroportos envolve toda a comunidade aeroportuária, principalmente as companhias aéreas e empresas que operam nos pátios ou estão instaladas no terminal de passageiros. Tem a ver com identificação e credenciamento de passageiros e empregados, rigor nos acessos a pátios, pistas e aeronaves, por parte de pessoas que ali prestam serviço, implica instalação de câmeras nas dependências dos terminais, fiscalização em todos os compartimentos do aeroporto, verificação de bagagens de mão, etc. Enfim, é uma série de procedimentos que visam dar tranqüilidade aos passageiros para embarcar e às empresas aéreas para operar as aeronaves com segurança. As suas premissas são as seguintes (Costa, 2007):

- Eliminar todos os acidentes e incidentes sérios é impossível;
- Falhas continuarão a ocorrer, mesmo com prevenção;
- Atividade humana ou sistema feito pelo homem estão sujeitos a riscos e erros; e
- Riscos e erros são aceitáveis quando sobre controle.

Não existe segurança absoluta. É impossível cobrir com cem por cento de eficiência todos os riscos possíveis. Por essa razão, é necessário, antes de decidir que medidas de proteção devem ser adotadas, identificar quais são os riscos que se corre ou os riscos prováveis. Sempre haverá uma proporção entre segurança e ameaça (Costa, 2007).

A Organização Internacional de Aviação Civil introduziu o conceito e a exigência de sistemas de gerenciamento da segurança operacional para aplicação às operações de aeroportos na Emenda 4 ao Anexo 14 – Aeródromos à Convenção Internacional de Aviação Civil, que entrou em vigor em novembro de 2001. Assim, a implementação de um SGSO – Sistema de Gerenciamento de Segurança Operacional, passa a ser uma norma internacional para os aeroportos certificados a partir de 24 de novembro de 2005, conforme estabelecido no item 1.4.6 do Volume I do Anexo 14 – Aeródromos (Costa, 2007).

2.3 LEGISLAÇÃO AERONÁUTICA

O Direito Aeronáutico é o complexo de normas disciplinadoras do transporte aéreo, aplicável às aeronaves, às suas tripulações, aos aeroportos e ao espaço aéreo (Gusmão, 1976).

No Brasil, o direito aeronáutico é regulado pelos Tratados, Convenções e Atos Internacionais de que o Brasil seja parte, pelo Código Brasileiro de Aeronáutica - lei 7.565, de 19.12.86 e pela legislação complementar. O artigo 22, I, da Constituição Federal, de 1988, estabelece, expressamente, que "*compete privativamente à União legislar sobre Direito Aeronáutico"*. (Pacheco, 2001).

Foi estabelecida a Organização da Aviação Civil Internacional – OACI, para servir de meio para se conseguir a compreensão e os acordos internacionais. Essa organização foi criada em 1944 com a assinatura da Convenção da Aviação Civil Internacional, chamada de Convenção de Chicago, e em 1947 tornou-se uma Agência da Organização das Nações Unidas - O.N.U., com sede em Montreal e escritórios regionais em Bangkok, Cairo, Dakar, Lima, México e Paris. A sua principal atividade é promover a padronização internacional das práticas e recomendações a serem observadas pelos países nos procedimentos técnicos da aviação civil, na qualificação e habilitação do pessoal navegante e de terra, nas regras de circulação no espaço aéreo, e prevenção de acidentes, ruído e segurança (Pacheco, 2001).

A Associação Internacional de Transporte Aéreo (IATA) é uma associação não governamental, ao contrário da Organização Internacional de Aviação Civil (OACI), que é uma organização governamental de direito privado da qual participam empresas de transporte aéreo internacional ou doméstico, regular ou não regular, sendo que muitas delas são

empresas cuja propriedade ou maioria do capital votante pertence ao Estado onde as mesmas estão sediadas, significando uma participação indireta mas efetiva de Governos em uma associação de direito privado. Entre os seus objetivos principais constam os de prover transporte aéreo com segurança, eficiência e economia (Pacheco, 2001).

2.4 CONTROLE DE ACESSO ÀS ÁREAS RESTRITAS DE AERÓDROMOS

A Instrução da Aviação Civil estabelece procedimentos a serem adotados nos aeroportos civis brasileiros, em especial pelas administrações aeroportuárias, no processo do controle de acesso de passageiro, tripulante, pessoal de serviço e outras pessoas, sob a responsabilidade do operador aeroportuário, tanto da administração federal indireta, quanto das administrações estaduais e municipais conveniadas com o Comando da Aeronáutica, e particulares concessionários ou autorizados.

Em caráter complementar, proprietários de aeródromos privados onde operam serviços de transporte aéreo público e empresas aéreas, poderão ser encarregados da implementação de medidas previstas nesta Instrução da Aviação Civil (IAC), quando determinado pelo Agência Nacional de Aviação Civil (ANAC), e tem como finalidade detalhar procedimentos específicos e obrigatórios, no controle de acesso às Áreas Restritas de Segurança (ARS), visando garantir que passageiro, devidamente processado, antecedendo ao embarque nas aeronaves e empregados funcionários e outras pessoas autorizadas tenham a sua presença permitida nessas áreas.

A Segurança da Aviação Civil (AVSEC) visa, essencialmente, proporcionar ao usuário do transporte aéreo a confiança e a credibilidade necessárias ao desenvolvimento deste importante segmento da economia nacional, com a aplicação de medidas preventivas e o uso de equipamentos, nos aeroportos, nas áreas e instalações vinculadas ao Sistema de Aviação Civil localizadas fora dos aeroportos e nos sistemas de comunicação e navegação aérea.

Estas ações envolvem providências das administrações aeroportuárias, devendo agir de forma cooperativa e coordenada com organizações policiais, empresas e entidades vinculadas ao Sistema de Aviação Civil, operadores de sistemas de navegação aérea, forças militares e outros órgãos públicos, assegurando assim, a manutenção de estados de segurança adequados

às ameaças identificadas, e contribuindo para a consecução de políticas de segurança pública e de defesa nacional.

A segurança aeroportuária constitui um componente de segurança da aviação civil, tendo como elemento fundamental os controles de acesso às Áreas Restritas de Segurança (ARS) dos aeroportos. Estes controles de acesso estão previstos no Plano de Segurança da Aviação Civil (PNAVSEC), exigindo pessoal devidamente qualificado e equipamentos adequados com o propósito principal de proteger a aviação civil contra atos de interferência ilícita.

2.4.1 Responsabilidade

A administração aeroportuária tem como responsabilidade as medidas preventivas de segurança, nos controles de acesso para o lado ar, a partir de suas instalações, coordenando e supervisionando os controles de segurança de responsabilidade de terceiros, devendo:

a) estabelecer as áreas restritas de segurança para aplicação dos procedimentos de controle de acesso e identificação de pessoas e veículos;

b) estabelecer um sistema de credenciamento de pessoas e veículos para terem acesso às áreas restritas de segurança;
c) planejar e prover os meios necessários para o sistema de controle de acesso aeroportuário, com equipamento de segurança apropriado e recursos humanos qualificados;

d) manter o serviço de controle, nos pontos de acesso ao aeroporto, bem como supervisionar esse serviço no caso das áreas de responsabilidade das concessionárias;

e) coordenar com o Departamento de Polícia Federal (Agência, Delegacias ou Superintendência Regional), a implantação e/ou funcionamento de Plantão de Polícia Federal, no respectivo aeroporto, para supervisão e acionamento dos procedimentos de controle de acesso às áreas restritas;

f) caso não haja disponibilidade de Plantão de Polícia Federal, buscar a participação das polícias estaduais e municipais;

g) estabelecer ponto de controle de acesso exclusivo para tripulante, pessoal de serviço e de outras pessoas, quando não for possível ou quando não for permitido, utilizar os canais de inspeção de passageiro;

h) coordenar, com os órgãos públicos e concessionários instalados no aeroporto, as medidas de segurança relacionadas ao controle de acesso, estabelecidas ou a serem estabelecidas no Plano de Segurança Aeroportuária (PSA);

i) coordenar, com os órgãos de segurança pública, as ações interagentes no processo de controle de acesso;

j) coordenar, com a Polícia Federal ou, na sua indisponibilidade, com outro órgão de segurança pública e a empresa aérea, o procedimento para o embarque de passageiro armado, estabelecido ou a ser estabelecido no Plano de Segurança Aeroportuário.

k) estabelecer, com as empresas aéreas, o trato com os materiais perigosos que não podem ser transportados por via aérea;

l) manter, em lugar visível, avisos permanentes referentes à material perigoso e à proibição de acesso à área restrita e aeronaves;

m) negar o acesso, às Áreas Restritas de Segurança, de passageiro que não se dispuser à inspeção ou portar materiais perigosos e/ou proibidos;
n) negar o acesso, às Áreas Restritas de Segurança, de passageiro, que não tenha obedecido às orientações e procedimentos relativos à arma a bordo;

o) estabelecer ponto de controle de acesso exclusivo e equipados com sistema de vigilância e alarme, para veículos;

p) negar o acesso de veículo sem credenciamento ou autorização, às áreas restritas de segurança;

q) manter as barreiras de segurança do sítio aeroportuário, patrimonial e operacional, com vigilância e proteção;

r) supervisionar os controles de acesso de pessoas e veículos às áreas restritas de segurança, sob a responsabilidade de concessionários;

s) manter o pessoal envolvido nas tarefas de controle de acesso atualizado em relação ao Plano de Segurança Aeroportuária, às resoluções da Comissão de Segurança Aeroportuária (CSA) e Diretrizes de Segurança da Aviação Civil, no que for aplicável;

t) controlar treinamento de reciclagem anual realizado pelas empresas contratadas para prestação de Serviços Auxiliares de Transporte Aéreo, no Serviço de Proteção da Aviação Civil;

u) manter um programa de manutenção, que especifique o funcionamento e a calibragem dos equipamentos de forma adequada ao nível de ameaça;

v) manter atualizados os procedimentos nos canais de controle de acesso quando nas situações normal, sob ameaça, de crise e de emergência;

w) adotar medidas adicionais de segurança tão logo tome conhecimento do nível de ameaça estabelecido pelo Diretor-Geral de Aviação Civil (DGAC), dentro dos procedimentos estabelecidos nos respectivos Planos de Contingência; e

x) estabelecer procedimentos alternativos para o caso de falha de equipamentos nos pontos de controle.

2.4.2 Princípios Gerais de Procedimentos Relativos ao Acesso

Os procedimentos relativos ao acesso têm como princípio básico o estabelecimento de um número mínimo de pontos de controle às áreas aeroportuárias restritas, de forma a reduzir os custos associados, assim como garantir que apenas o efetivo autorizado tenha a sua presença permitida no lado ar e que somente os passageiros devidamente processados possam embarcar nas aeronaves.

A administração aeroportuária deve estabelecer um número mínimo de pontos de controle às áreas de segurança do aeroporto, objetivando um maior controle da segurança e redução dos custos associados, bem como garantir que apenas o pessoal autorizado tenha acesso ao lado ar;

A necessidade de pessoas e veículos entrarem na Áreas Restritas de Segurança dos aeroportos, será atendida por meio de um número mínimo de pontos de entrada, de acordo com as necessidades operacionais de cada sítio, com as seguintes características:

a) possam ser completamente fechados, quando necessário;
b) dependendo do tipo de acesso, sejam projetados de acordo com a localização e a freqüência com que serão usados; e
c) incorporando medidas para que as estruturas dos portões não sejam facilmente violadas.

O acesso às Áreas Restritas de Segurança definidas nos aeroportos está limitado a:

a) passageiros com posse de documentos de viagem legítimos, que tenham sido aceitos para vôos de uma empresa aérea;
b) tripulantes, empregados da administração aeroportuária, pessoal de serviço, veículos e equipamentos, devidamente credenciados; e
c) outras pessoas devidamente identificadas, com autorização específica, emitida pela Administração Aeroportuária Local, desde que acompanhadas por empregado da referida administração.

Os pontos de controle de acesso devem ser equipados com um sistema de comunicação e alarme interligado ao setor de segurança aeroportuária.

O responsável pelo setor de segurança aeroportuária, encarregado dos controles de acesso às Áreas Restritas de Segurança, deve:
a) assegurar que barreiras físicas demarcadoras dessas áreas sejam mantidas em boas condições operacionais; e

b) especificar os pontos de controle de acesso, garantindo que tais pontos tenham proteção física adequada, no mínimo com as mesmas características das barreiras.

As pontes de embarque de passageiros e outros meios utilizados para esta finalidade devem ser bloqueados ou vigiados, a fim de evitar o acesso não autorizado às aeronaves estacionadas.

2.4.3 Controle de Acesso de Pessoas - Identificação de Passageiro

Ao proceder o despacho de passageiro, a empresa aérea deve solicitar o seu documento legal de identidade compatibilizando a fotografia com o portador, bem como verificando validade e registrando o tipo, número e órgão expedidor, conciliando-o com o seu bilhete de passagem e bagagem.

Nos aeródromos civis, onde operam os vôos de empresas regulares de transporte aéreo, regidos por horário de transporte (HOTRAN), o responsável pela administração do aeroporto deve estabelecer a compatibilização do cartão de embarque com o documento legal de identidade, no posto de controle de acesso à sala de embarque.

Nos aeródromos onde somente operam aeronaves com 60 (sessenta) assentos ou menos e não existam administrações aeroportuárias instaladas, as empresa aéreas são responsáveis por proceder a conciliação do documento legal de identidade do passageiro com o cartão de embarque, no ponto de acesso ao lado ar ou na porta da aeronave.

2.4.4 Inspeção de Passageiro

A inspeção, como exigência das condições gerais de transporte, é o procedimento sob aplicação de meios técnicos ou de outro tipo, destinados a identificar ou detectar armas, explosivos ou materiais e/ou dispositivos perigosos ou proibidos que possam ser utilizados para cometer um ato de interferência ilícita, a que o passageiro se submete voluntariamente, visando a sua própria segurança e à incolumidade pública.

Quando houver suspeição de qualquer material perigoso e/ou proibido, deve ser acionada a Policia Federal, quando disponível, ou a força policial estadual ou municipal, para a busca pessoal (revista) do passageiro, tripulante, bagagem de mão e pessoal de serviço.

No caso de suspeição, a verificação limita-se aos objetos apresentados pelo passageiro, não cabendo nenhum contato físico entre o agente de proteção da aviação civil e a pessoa inspecionada.

Compete à empresa aérea realizar procedimentos adicionais de segurança, conciliando o documento legal de identidade, com o cartão de embarque e com a sua bagagem despachada, dentro da área estéril, antes do embarque, quando determinado ou julgado conveniente.

2.4.5 Identificação de Tripulantes, de Pessoal, de Serviço e de Outras Pessoas

A identificação de tripulantes, de pessoal de serviço e de outras pessoas que devam eventualmente ingressar na Áreas Restritas de Segurança, deve ser realizada nos pontos de controle de acesso, visando verificar, principalmente, a autenticidade da credencial ou documento legal de identidade, conciliando a fotografia com o rosto da pessoa identificada e a validade da autorização.

O uniforme do tripulante não é suficiente para permitir o seu acesso às áreas restritas, devendo, para isso, portar a credencial de sua empresa aérea, e ser submetido aos procedimentos de inspeção do aeroporto.

O tripulante pode apresentar as credenciais emitidas pelas respectivas empresas aéreas ou licença expedida pela ANAC ou órgão equivalente de outro país, quando a serviço de operadores aéreos.

O tripulante de empresa aérea que não possua credencial de identificação, quando no exercício de suas funções, têm acesso às Áreas Restritas de Segurança, mediante a apresentação da Licença e do Certificado de Habilitação Técnica (CHT) expedidos pela ANAC ou por órgão equivalente de outro país e de documento legal de identidade.

O funcionário, civil ou militar, de órgão público lotado no aeroporto, só pode ingressar nas Áreas Restritas de Segurança com credencial emitida pelos respectivos órgãos ou com credencial expedida pela administração aeroportuária, sendo os modelos explicitados no respectivo Plano de Segurança Aeroportuária.

A equipe que trabalha nas Áreas Restritas de Segurança e nas áreas controladas do aeroporto, na manutenção, no serviço de provisão de alimento de bordo e de abastecimento de combustível, nos terminais de passageiros e de carga aérea, bem como próximo às aeronaves, é obrigado a portar sua credencial, em local visível, na altura do peito ou em uma braçadeira.

2.4.6 Inspeção de Tripulantes, de Pessoal, de Serviço e Outras Pessoas

A inspeção é o procedimento sob a aplicação de meios técnicos ou de outro tipo, destinados a identificar ou detectar armas, explosivos ou materiais e/ou dispositivos perigosos ou proibidos que possam ser utilizados para cometer um ato de interferência ilícita, a que o tripulante, pessoal de serviço e outras pessoas que devam ingressar nas áreas estéreis se submetem, voluntariamente, visando a sua própria segurança e à incolumidade pública.

O tripulante de empresa de transporte aéreo regular, mesmo existindo ponto de acesso exclusivo, também pode utilizar os pontos de controle de acesso de passageiro, se for conveniente para a empresa aérea.

Quando houver suspeição de qualquer material perigoso e/ou proibido, a Polícia Federal ou, na sua indisponibilidade, outra força pública estadual ou municipal deve ser acionada para a busca pessoal (revista) de tripulante e sua bagagem de mão, de pessoal de serviço e de outras pessoas.

O agente de proteção da aviação civil, no caso de suspeição, limita-se à verificação de objetos apresentados pelas pessoas, não cabendo nenhum contato físico com o inspecionado. Entretanto, o líder da equipe desses agentes deve comunicar a ocorrência, imediatamente, ao responsável pela segurança aeroportuária, informando o nome da pessoa impedida de passar pelo posto de controle ou suas características físicas, quando não houver a possibilidade ou necessidade da intervenção policial.

Nos locais e horários em que não houver Plantão de Polícia Federal ou de outra organização policial, não deve ser procedida a busca pessoal (revista), cabendo ao agente de proteção da aviação civil negar o acesso da pessoa que se oponha a apresentar materiais perigosos e/ou proibidos e detectados ou não por inspeção.

Cabe à empresa aérea estabelecer procedimentos para verificar a credencial de pessoas que se aproximem ou ingressem em suas aeronaves, bem como dos operadores de equipamentos de apoio de solo.

O funcionário, civil ou militar, quando no exercício de suas funções, pode ingressar na Áreas Restritas de Segurança por qualquer posto de controle, devendo submeter-se à inspeção, visando a sua própria segurança e à incolumidade pública.

O acesso de outras pessoas não vinculadas ao sistema aeroportuário que eventualmente devam ingressar nas Áreas Restritas de Segurança deve ser realizado após contato prévio com o setor da administração aeroportuária encarregado da segurança ou com o supervisor de serviço, seguindo os procedimentos estabelecidos no Plano de Segurança Aeroportuária.

Os visitantes para ingressarem em áreas restritas ou controladas serão credenciados e acompanhados. Quando for esperado um número de visitantes superior à capacidade de processamento da equipe de segurança do aeroporto, é necessária uma solicitação de apoio da autoridade policial, militar ou outra julgada pertinente.

Nos aeroportos onde operam aeronaves com mais de 60 (sessenta) assentos e nos de transporte aéreo regular de passageiros, devem ser disponibilizados canais de controle de acesso exclusivos para inspeção de tripulantes, pessoal de serviço e outras pessoas que devam ingressar nas áreas estéreis, implementando as medidas com equipamentos e pessoal qualificado em quantidade compatível com o movimento.

O pessoal qualificado, denominado Agente de Proteção da Aviação Civil, deve ser empregado da administração do aeroporto ou da empresa de serviços auxiliares de transporte aéreo especializada em proteção da aviação civil, com treinamento adequado.

As empresas de táxi aéreo, entidades aerodesportivas, empresas de manutenção de aeronaves, operadores de aeronaves e demais entidades vinculadas ao Sistema de Aviação Civil e instaladas nos aeródromos servidos por serviços de transporte aéreo regular, com aeronaves de capacidade superior a 60 (sessenta) assentos, devem orientar o acesso de seus funcionários às Áreas Restritas de Segurança através dos pontos de controle de acesso disponibilizados pela administração aeroportuária.

Nos casos dos aeródromos com grande movimento de tripulantes e pessoas de serviço dos segmentos da aviação civil, pode ser necessário o estabelecimento de canais específicos de acesso às Áreas Restritas de Segurança, visando a facilitar o ingresso controlado de acordo com os procedimentos previstos nas Instruções da Aviação Civil, sob a supervisão e coordenação da administração do aeroporto.

2.4.7 Credenciamento

O credenciamento de pessoas, veículos e equipamentos, desde a sua formalização, até seu cancelamento, é um instrumento imprescindível para os controles de segurança de qualquer sistema, conseqüentemente do sistema aeroportuário. Dever ser gerenciado por um setor específico da administração aeroportuária, dotado de pessoal qualificado e instalado em área controlada.

O sistema de credenciamento consiste na concessão de uma credencial ou de outro documento emitido para veículos e para as pessoas que trabalhem no aeroporto ou para aqueles que tenham a necessidade de ingressar nas áreas controladas e restritas de segurança. Deve ser organizado usando um banco de dados para a emissão e controle de credenciais de leitura visual, magnética ou de outro método.

A administração aeroportuária é responsável pelo credenciamento de veículos, equipamentos e pessoas que têm acesso ao aeroporto e desenvolvem atividades nas áreas públicas, controladas e restritas de segurança. Nos grandes aeroportos, deve ser considerada a possibilidade de subdividir as áreas restritas de segurança, em zonas identificadas por letras, números ou cores. As credenciais devem conter a indicação da zona a que o indivíduo tem acesso.

A credencial é limitada à área cujo acesso seja permitido, em função das atividades exercidas por pessoas e de acordo com a utilização de veículo ou equipamento autopropulsionado. Providências administrativas de controle serão adotadas para evitar desvios e falsificações, bem como para reduzir o uso indevido por extravio ou não devolução. As credenciais de pessoas devem ser emitidas e revalidadas, periodicamente, no máximo a cada 2 anos, bem como a de veículos , anualmente. O cadastramento do sistema deve ser auditado periodicamente, internamente pela administração aeroportuária e, externamente pela Agência Nacional de Aviação Civil (ANAC), por delegação da Autoridade Aeronáutica, visando assegurar a confiabilidade dos dados.

A credencial é de porte obrigatório e ostensivo, na altura do peito ou em braçadeira, sem obstrução, sendo o seu portador submetido aos controles de segurança, inclusive à inspeção, para o acesso às áreas restritas de segurança e/ou controladas. O Plano de Segurança Aeroportuária deve estabelecer os modelos de credenciais para acesso e circulação nas áreas restritas de segurança e/ou controladas, sendo de conhecimento das equipes dos pontos de controle de acesso e do patrulhamento móvel.

Quando necessário e como medida adicional de segurança, a credencial tem que ser confrontada, nos pontos de controle, com o documento legal de identidade do credenciado e com a documentação do veículo. As credenciais de Inspetor de Aviação Civil, outros Inspetores do Comando da Aeronáutica e agentes de órgãos públicos, no exercício de suas funções, não necessitam de conciliação com outros documentos.

2.4.8 Equipamento e Meio de Inspeção

A inspeção dos passageiros e de suas bagagens de mão deve ser realizada com a utilização de detectores de metais, aparelhos de raios-X e outros meios, de forma manual, ou por meio de combinação de ambos. Para facilitar o fluxo de embarque, sempre deve ser dada preferência aos equipamentos automáticos de detecção.

No treinamento do pessoal e na operação dos equipamentos devem ser considerados os fatores humanos, de forma que limitações de tempo de atenção e outros aspectos não possam contribuir para o cometimento de erros que degradem a segurança.

No caso de ocorrência de ato ilícito ou do estabelecimento de situação de emergência determinada pela Agência Nacional de Aviação Civil (ANAC), o setor responsável pela manutenção acionará equipe capacitada e os meios necessários à realização das operações de manutenção corretiva dos equipamentos e dispositivos de segurança, mantidos em condição de prontidão operacional permanente, para atuar sob a coordenação do Centro de Operação de Emergência (COE).

As administrações aeroportuárias devem manter um controle atualizado, apresentado em planilha (quadro geral), contendo a relação dos equipamentos de segurança utilizados no respectivo aeroporto e descrevendo a sua identificação, designação, número de série, data de aquisição, local de uso, as datas e os responsáveis técnicos pelas últimas revisões de manutenção e de calibração, atualizando-o anualmente e arquivando-o por cinco anos.

Desde o dia 01 de janeiro de 2006, o sistema detector de traços de explosivos é dispositivo obrigatório na inspeção de bagagens de mão de passageiros, tripulantes e pessoal de serviço, nos aeroportos em que operam serviços de transporte aéreo regular internacional, com aeronaves de capacidade superior a 60 (sessenta) assentos, para a detecção da presença de resíduos ou vapores de materiais explosivos, em amostras coletadas pelo operador.

Caso a Administração Aeroportuária considere aplicável a implantação de outro método/tecnologia que atenda aos objetivos inerentes à detecção de explosivo em bagagem de mão, a referida proposta deverá ser submetida à aprovação da Agência Nacional de Aviação Civil (ANAC).

O sistema detector de objetos – Raios-X é um dispositivo obrigatório em todos os aeroportos em que operam serviços de transporte aéreo público, com aeronaves de mais de 60 (sessenta) assentos, que permitem inspecionar visualmente o conteúdo de bagagens, sem necessidade de abri-las. Sempre que aplicável, os administradores aeroportuários deve utilizar equipamentos que possibilitem a identificação e distinção de elementos orgânicos e inorgânicos através da diferenciação de cores no monitor. Os operadores devem permanecer por um tempo máximo de 20 minutos diante dos monitores, revezando as funções no posto de controle de acesso com os outros membros da equipe de inspeção.

O sistema detector de metais é um dispositivo obrigatório em todos os aeródromos em que houver operação de serviços de transporte aéreo público com a utilização de aeronaves de capacidade superior a 30 (assentos), e nos aeródromos em que a Agência Nacional de Aviação Civil (ANAC) determinar, devido a sua situação e nível de ameaça. Devem ser empregados equipamentos detectores de metais, dos tipos pórtico e manual de acordo com os módulos mínimos dos pontos de controle de acesso.

Em caso de elevação do nível de alerta, fazer ajuste para disparar com a presença de massas metálicas de aproximadamente 15g, ou capaz de detectar objeto teste (lâmina com 3 cm, de ponta arredondada), em qualquer parte do seu campo de indução. A utilização de detectores de metais manuais é recomendada nos aeródromos servidos por operadores de transporte aéreo regular e com ligações sistemáticas, com aeronaves de capacidade inferior a 31 assentos, mesmo quando não houver estrutura da administração aeroportuária instalada no aeródromo.

A utilização de cães farejadores deve restringir-se à inspeção de bagagens, tomados os cuidados para que o pessoal inspecionado não seja submetido a qualquer tipo de constrangimento ilegal. Os administradores aeroportuários devem considerar que o amestrador e o cão fazem parte de um conjunto inseparável, que deve ser adequadamente selecionado e treinado para a obtenção dos resultados esperados. As restrições relacionadas à capacidade de identificação pelo faro dos animais e os fatores limitadores decorrentes da fadiga dos cães, devem ser avaliados no emprego deste recurso.

O sistema de TV e vigilância deve ser instalado nos aeroportos mais movimentados, conforme disposições contidas nos módulos padronizados da Instrução da Aviação Civil. É constituído de uma unidade central de comando e controle, conjunto de câmeras, unidade de gravação de vídeo e sistemas de cabos de energia e transmissão de dados, podendo incluir, também, sistemas de impressão em papel. Deve ser instalado nos pontos de controle de acesso, de forma que as lentes focais tenham a capacidade de identificar pessoas e placas de veículos.

O sistema automatizado de controle de acesso pode ser empregado sistema automático de leitura de credenciais, nos pontos de controle de acesso de tripulantes e pessoal de serviço ou de outras pessoas. Pode ser empregado, nos pontos de controle de veículos, sistema

automatizado de detecção e de leitura de credenciais, combinado com barreiras físicas, portões ou cancelas. O emprego de tal dispositivo exige o monitoramento constante por um agente de proteção da aviação civil, no local.

2.4.9 Aquisição de Equipamento

A seleção de equipamentos de segurança a serem adquiridos pelas administrações aeroportuárias e empresas aéreas deve ser submetida à aprovação prévia da Agência Nacional de Aviação Civil (ANAC), contendo as informações e dados técnicos de operação, de calibração e de manutenção, recomendados pelos respectivos fabricantes. A administração aeroportuária e as empresas aéreas devem estabelecer uma programação de manutenção preventiva para os equipamentos de segurança, incluindo procedimentos alternativos para os casos de falhas, visando a assegurar sua eficiência e eficácia operacional.

As autoridades públicas instituídas dos poderes Executivo, Legislativo e Judiciário, bem como o visitante oficial estrangeiro e as representações diplomáticas, serão submetidos às medidas de segurança de caráter especial, desde que, com oportunidade e em tempo hábil, haja solicitação e coordenação com a administração aeroportuária, que deve interagir quando necessário com os demais órgãos de segurança pública e, em particular com a Polícia Federal. O acesso dos Inspetores de Aviação Civil às áreas de responsabilidade de outros órgãos públicos lotados no aeroporto está condicionado à coordenação prévia com os referidos órgãos.

As adequações específicas pretendidas pelas Administrações Aeroportuárias e os desvios pretendidos pela Instrução da Aviação Civil devem ser solicitados à Agência Nacional de Aviação Civil (ANAC) e submetidos à aprovação, mediante justificativa escrita, de acordo com a situação de cada aeródromo.

A Administração Aeroportuária é objeto de notificação de infração e de aplicação das sanções previstas no Código Brasileiro de Aeronáutica e legislação ou regulamentação complementar, no caso de não atendimento ao disposto na Instrução da Aviação Civil. Os casos não previstos na Instrução da Aviação Civil devem ser submetidos à apreciação do Diretor-Geral de Aviação Civil.

2.4.10 Comissão de Segurança Aeroportuária

A Instrução da Aviação Civil 107-1003 estabelece procedimentos para ativação e funcionamento da Comissão de Segurança Aeroportuária, nos aeródromos civis públicos que atendem à aviação civil nacional e/ou internacional, onde operam empresas aéreas regulares e não regulares.

A Comissão de Segurança Aeroportuária é um fórum de assessoramento, onde são tratadas e avaliadas as medidas de segurança de um aeroporto, sendo os seus trabalhos realizados com a coordenação entre todos os envolvidos na segurança da aviação civil, visando a proteger as suas atividades contra atos de interferência ilícita.

A sua finalidade é regulamentar a ativação e o funcionamento da Comissão de Segurança Aeroportuária, nos aeroportos civis brasileiros, objetivando a implementação coordenada das medidas de segurança para a proteção da aviação civil contra atos de interferência ilícita.

Em cada aeroporto público que atenda à aviação civil nacional e/ou internacional, onde operam empresas aéreas regulares e não regulares, com aeronaves acima de 60 assentos, por ato do administrador aeroportuário, deverá ser ativada a Comissão de Segurança Aeroportuária em cumprimento ao previsto no item 5, do art. 6º do Decreto nº 72.753, de 06 de setembro de 1973, que institui a Conselho Nacional de Segurança da Aviação Civil (CONSAC).

Nos aeroportos nacionais e/ou internacionais, onde operam empresas aéreas regulares ou não regulares, com aeronaves de 31 até 60 assentos, a ativação da Comissão de Segurança Aeroportuária será facultativa. Neste caso, a entidade responsável pela administração aeroportuária deverá realizar, anualmente, uma análise das condições de segurança do respectivo aeroporto, apresentando à Agência Nacional de Aviação Civil (ANAC), solicitando, se for o caso, o adiamento para sua implantação.

Nos aeroportos nacionais e/ou internacionais, onde operam empresas aéreas regulares ou não regulares, com aeronaves de menos de 31 assentos, ficará a cargo da empresa aérea

providenciar relatório de segurança para o administrador aeroportuário, encaminhando cópia ao setor competente da Agência Nacional de Aviação Civil.

A implantação da Comissão de Segurança Aeroportuária e demais peculiaridades para seu funcionamento serão estabelecidas pelo Administrador do Aeroporto, baseado na presente Instrução de Aviação Civil.

A Comissão de Segurança Aeroportuária se reunirá, ordinariamente, a cada 03 (três) meses e, extraordinariamente, plena ou setorial, quando convocada pelo seu Presidente, por sua iniciativa ou no atendimento de sugestões de um de seus membros, secretariado pelo responsável no gerenciamento da segurança do aeroporto.

A freqüência das reuniões ordinárias poderá ser semestral, nos aeroportos onde somente operam empresas aéreas com vôos não regulares, dependendo de autorização prévia da Agência Nacional de Aviação Civil.

As reuniões da CSA serão de caráter restrito e realizadas com exclusividade, sem o envolvimento com as atividades relacionadas com a Comissão de Coordenação Aeroportuária (CCA) e da Sub-Comissão de Facilitação (S/COMFAL).

Nos aeroportos com movimento de aeronaves com mais de sessenta assuntos, a CSA será implementada em caráter obrigatório, devendo se reunir ordinariamente a cada 06 (seis) meses e, extraordinariamente, tendo em vista as suas características de localização e operação.

A ANAC, independentemente do tipo e freqüência das operações, poderá requisitar a instalação de uma CSA, em qualquer aeroporto civil nacional.

Os membros da CSA poderão ser responsabilizados pela omissão de fatos de seu conhecimento que comprometam a segurança da aviação civil e resultem em perdas materiais e humanas, tanto no setor público como no privado.

Os casos não previstos nesta Instrução serão submetidos à apreciação do Diretor-Geral da Aviação Civil.

3 TECNOLOGIAS DE ACESSO

3.1 APRESENTAÇÃO

O objetivo deste capítulo consiste em apresentar uma visão geral sobre os sistemas biométricos e seus principais aspectos de segurança como uma tecnologia de controle de acesso. Desta maneira, nas seções 3.2 e 3.3 apresentam os principais conceitos envolvendo sistemas biométricos. Não existe uma tecnologia melhor, mas sim a tecnologia mais adequada perante cada aplicação, em vista disso, a seção 3.4 analisa a variedade de aplicações e as categorias existentes.

Embora, essencialmente todos os sistemas biométricos se encaixem em um mesmo modelo conceitual, a implementação desse modelo pode diferir de um sistema para o outro. As seções 3.5, 3.6 e 3.7 apresentam os sistemas biométricos típicos, fatores para a escolha da tecnologia biométrica mais adequada e a importância da padronização das tecnologias para a sua ampla aceitação.

A seleção de uma tecnologia biométrica adequada para uma finalidade específica envolve muitos fatores. Para uma primeira análise podem ser estudados os pontos fortes e fracos de cada tecnologia biométrica. Desta forma, na seção 3.8 são identificados os tipos de avaliação necessária para a seleção da tecnologia mais adequada. Qualquer sistema biométrico cometerá erros e o verdadeiro valor associado às diversas taxas de erro não pode ser estabelecido teoricamente, por cálculo, somente por estimativas estatísticas de erros e na seção 3.9 são apresentados os tipos desses erros.

Os tipos de autenticação biométrica levam à diferenciação dos sistemas de identificação e de verificação, 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 na seção 3.10 que são as seguintes: reconhecimento da voz, reconhecimento facial, impressão digital, geometria da mão, assinatura, retina e íris.

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. No caso de haver risco para o usuário, a biometria deve ser utilizada como acessório.

Cada tecnologia biométrica é potencialmente utilizável em seu nicho apropriado. Na seção 3.11 é apresentado um panorama geral entre as tecnologias. Na seção 3.12 são apresentados os sistemas de reconhecimento misto e multimodal que consiste na reunião de tecnologias biométricas com outras tecnologias.

Nas seções 3.13, 3.14, 3.15 e 3.16 são apresentados os seguintes temas biometria cancelável, utilização de smart cards, problemas abertos e arquitetura e armazenamento.

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, dessa forma na seção 3.17 discute a segurança na biometria

No capitulo 4 é apresentado um estudo de caso realizado no aeroporto Juscelino Kubistchek em que são avaliados a tecnologia biométrica mais adequada para a aplicação na segurança aeroportuária contra atos de interferência ilícita.

3.2 BIOMETRIA

Biometria, em sentido literal, é a ciência que estuda a medida dos seres vivos, ou seja, é a identificação de um indivíduo através de suas características físicas e comportamentais. A natureza desenvolveu diversos mecanismos biométricos para o reconhecimento entre os seres vivos, por meios sensoriais combinados com registros em memória, os quais são hoje considerados pela ciência como habilidades de alta sofisticação que servem hoje como parâmetro de referência de crescentes pesquisas e desenvolvimento de cunho tecnológico na área de biometria (Couto, 2007).

O simples ato de identificar indivíduos diferentes, algo que até mesmo crianças são capazes de realizar. A capacidade de afirmar que uma determinada pessoa é ou não quem afirma ser, é algo que as modernas tecnologias só foram capazes de reproduzir de modo minimamente satisfatório na história recente, pois só então os dispositivos informáticos atingiram o necessário grau de processamento, armazenamento e segurança para tanto.

Não é tarefa simples para um poderoso computador reconhecer um indivíduo, pois seu *software* deverá ser minuciosamente instruído a reconhecer quais elementos e parâmetros físicos e comportamentais produzem efeitos distintivos entre seres humanos, bem como o equipamento informático que deve dispor de dispositivos eletrônicos que façam a medição adequada destas características biológicas. O desafio final, talvez o maior, para estes aparatos de recepção de dados biométricos, é a capacidade de resistir às deliberadas tentativas humanas de enganar estes equipamentos.

A capacidade de identificação segura de um determinado sujeito é denominada como autenticidade. Existem diversos meios de autenticação, sendo o mais conhecido e ainda utilizado a assinatura autógrafa, em que, de próprio punho, o indivíduo posta sinal identificador exclusivo seu. Este meio, na verdade, também é um método de natureza biométrica, que pode ser realizado de forma manual ou automático (Costa, 2004).

3.3 VERIFICAÇÃO E IDENTIFICAÇÃO

A tecnologia cumpre um papel de força de transformação na sociedade humana, seja como instrumento de alteração da natureza, seja como criadora de novos modelos societários humanos. As novas tecnologias de informação, comumente denominadas genericamente como *informática*, muito mais do que meros meios de eficiência e eficácia com fins de aprimoramento de produtividade e segurança, constroem novos paradigmas de sociabilidade que devem ser constantemente avaliados pelo Direito, à medida que o avanço tecnológico exige novos posicionamentos jurídicos (Moreira, 2001).

Percebe-se que as tradicionais formas de documentação civil, tais como cédulas de identidade, crachás e assemelhados, vêm sendo postos em segundo plano ou até mesmo recusados como meios de identificação pessoal. Crescentemente, seguradoras de saúde, instituições bancárias,

empresas privadas de diversas áreas e até governos vêm exigindo a identificação de usuários e funcionários por meio de equipamentos de reconhecimento biométrico.

Os sistemas biométricos são usados para a autenticação de pessoas. Nestes sistemas, existem dois modos de autenticação: a verificação e a identificação. 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” (Moreira, 2001).

Esta abordagem de autenticação é dita uma busca 1:N, ou busca aberta, em um banco de dados de perfis biométricos. O sistema busca todos os registros do banco de dados e retorna uma lista de registros com características suficientemente similares à característica biométrica apresentada. A lista retornada pode ser refinada posteriormente por comparação adicional, biometria adicional ou intervenção humana. Basicamente, a identificação corresponde a responder à questão: “Quem é o usuário?” (Moreira, 2001).

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 (Moreira, 2001).

3.4 APLICAÇÕES

As tecnologias biométricas podem ser utilizadas em uma ampla variedade de aplicações, para proporcionar controle de acesso físico e lógico e fornecimento de unicidade. As categorias existentes e o percentual de utilização são apresentadas na tabela 3.1 (Rich, 1998):

Tabela 3.1 - Distribuição Horizontal (por Finalidade) das Principais Aplicações Biométricas (Rich, 1998)

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

3.5 SISTEMA BIOMÉTRICO TÍPICO

Seja qual for a característica biométrica utilizada, ela deve estar enquadrada em um 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 (Moreira, 2001).

• 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 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. 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 (Moreira, 2001).

• Registro e perfil - O processo de registro obtém previamente os dados biométricos do usuário para cadastramento no sistema. O perfil biométrico obtido é armazenado para uma comparação posterior.

• Comparação, limiar e decisão - O processo de comparação 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, a decisão é aceitar o usuário, ou seja, uma autenticação válida. Caso a similaridade seja inferior ao limiar, a decisão é não aceitar o usuário, e então temos um usuário não autenticado.

3.6 CARACTERÍSTICAS BIOMÉTRICAS

As características fisiológicas ou comportamentais do ser humano podem ser usadas como característica biométrica desde que ela satisfaça alguns requisitos básicos, tais como (Costa, 2004):

• Universalidade: toda a população (a ser autenticada) deve possuir a característica, que são as impressões digitais. Na prática, temos pessoas que não possuem impressões digitais, por exemplo;

• Unicidade**:** uma característica biométrica deve ser única para cada indivíduo, ou seja, a possibilidade de pessoas distintas possuirem características idênticas, deve ser nula ou desprezível. Assim, a altura de uma pessoa não é uma boa característica para autenticação, já que várias pessoas podem possuir a mesma altura. Na prática, as características biométricas podem apresentar maior ou menor grau de unicidade, mas nenhuma delas pode ser considerada absolutamente única para cada indivíduo;

• 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, todas as características biométricas utilizadas comercialmente atendem a este requisito;

• Aceitação: a coleta da característica deve ser tolerada pelo indivíduo em questão. Na prática, existem preocupações com higiene, com privacidade e questões culturais que diminuem a aceitação da coleta. Na prática, porém, nenhuma característica biométrica consegue atender com perfeição aos requisitos de uma característica biométrica ideal. Ao longo do tempo, diversas tecnologias biométricas foram desenvolvidas.

As tecnologias biométricas existentes são classificadas em dois grupos:

a) 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. Outras características estáticas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa, como a impressão palmar , o DNA, o formato das orelhas,o padrão vascular da retina, o odor do corpo, o padrão da arcada dentária e o padrão de calor do corpo ou de partes dele (Rich, 1998).

b) 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. Outras características dinâmicas também são utilizadas em menor grau ou estão em estágios iniciais de pesquisa, como dinâmica de digitação, modo de andar, movimento labial, som da assinatura, vídeo da assinatura e imagens mentais

3.7 PADRONIZAÇÃO

A padronização é necessária para a ampla aceitação de tecnologias biométricas. Atualmente, os dispositivos não possuem interoperabilidade. Padrões internacionais relativos a tecnologias

biométricas têm sido propostos e estão em fase de amadurecimento. Estes padrões pretendem dar suporte à troca de dados entre aplicações e sistemas e tentam evitar os problemas e custos oriundos dos sistemas proprietários , são os seguintes (Moreira, 2001):

BioAPI - O consórcio BioAPI4 foi fundado para desenvolver uma API (Application Programming Interface) para proporcionar independência de dispositivo e de plataforma. O consórcio é formado por cerca de 120 companhias (pelo menos uma delas brasileira) interessadas em promover o crescimento do mercado biométrico. A BioAPI é a API mais popular na área biométrica. Suas primitivas se referem a tarefas de registro, identificação e verificação numa plataforma cliente/servidor e aquisição do sinal numa plataforma cliente. No nível mais alto, é definido um BSP (Biometrics Service Provider), que lida com todos os aspectos do processamento do sinal. Os diversos componentes se registram durante a instalação. O módulo de registro pode ser usado pelas aplicações para verificar os BSPs instalados e suas funcionalidades. Baseado na BioAPI, foi também definida uma API específica para Java Cards,5 para dar suporte a funcionalidades biométricas em smart cards, principalmente quanto à segurança dos algoritmos e do perfil biométrico eventualmente armazenado no cartão.

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

XCBF - Desenvolvido sob orientação de um comitê do OASIS, o XML Common Biometric Format (XCBF) 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.

3.8 ERROS

De uma maneira geral, a comunidade biométrica diferencia vários tipos de erros, conforme a localização lógica de sua ocorrência. As diferentes aplicações biométricas podem ter diferentes definições dos erros associados. Conseqüentemente, há muita terminologia para expressar a precisão de uma aplicação. O que é bastante claro e aceito por toda a comunidade biométrica é que qualquer sistema biométrico cometerá erros e que o verdadeiro valor associado às diversas taxas de erro não pode ser estabelecido teoricamente, por cálculo, mas somente por estimativas estatísticas dos erros, que são expressos em taxas e percentagens. Há dois tipos de erros nos quais o comparador pode incorrer (Moreira, 2001).

• 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).

Devido à possibilidade de calibrar o sistema por meio do ajuste do limiar, as taxas de erros possuem conseqüências opostas. FA resulta em brechas na segurança, com a admissão de usuários não autorizados. Por outro lado, FR resulta em problemas de conveniência, já que usuários genuínos terão acesso negado até uma verificação posterior.

As taxas de erro FAR e FRR podem ser plotadas uma ao lado da outra, como apresentado na figura 2. 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 *Tempo (T)* = Tempo Esperado (*TE)* para o qual FAR(*T*) = FRR(*T*). Este ponto é conhecido como ponto de operação EE (*Equal Error*), ao qual também está associado uma taxa EER (*Equal Error Rate*) (Moreira, 2001).

As taxas FAR(*T*) e FRR(*T*) também podem ser comparadas uma contra a outra para produzir uma curva bi-dimensional característica conhecida por *Receiver Operating Characteristic* (ROC). 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. 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.

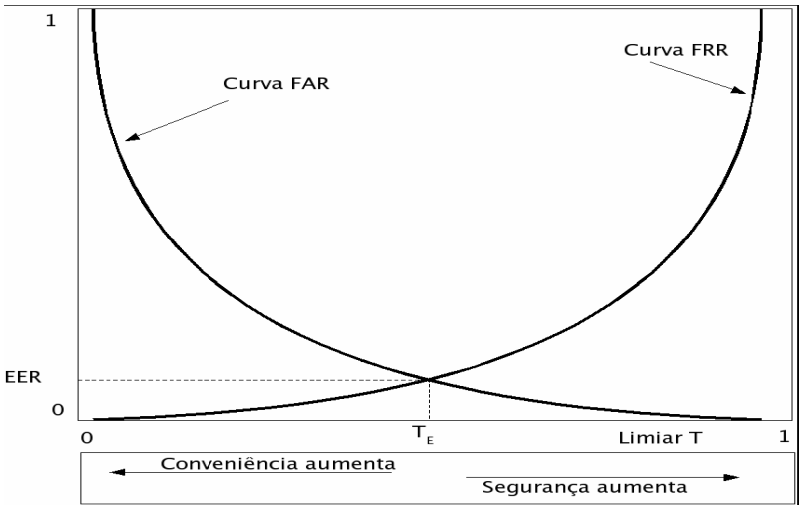


Figura 3.2 - Curvas Típicas das Taxas de Erro FAR e FRR

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

Existem outros conceitos úteis para avaliação mais delicada de comparadores, como a separação das densidades de probabilidade e o conceito de Erro Total Esperado, com seu refinamento associado a Funções de Custo para cada tipo de erro. 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 autoatendimento de um banco, no qual FRs não são aceitáveis por falta de pessoal de suporte, mas FAs podem ser tolerados, já que existiria uma segunda fase de autenticação por senha (Moreira, 2001).

3.9 TECNOLOGIAS

Existem várias técnicas de reconhecimento biométrico disponíveis no mercado, as principais formas atualmente utilizadas são as seguintes (Costa, 2001):

3.9.1 Tecnologia de Reconhecimento da 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, conforme demonstrado na Fig. 3.3. (Costa, 2001):

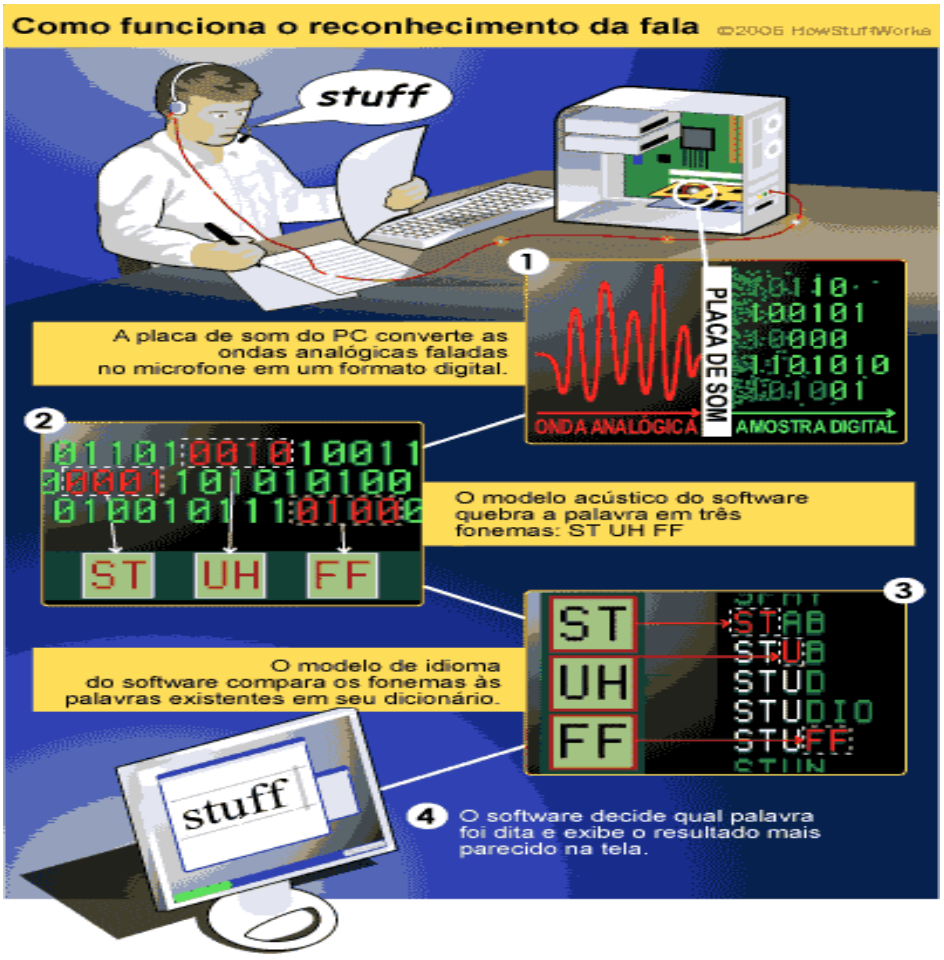


Figura 3.3 - Funcionamento do Sistema de Captação e Reconhecimento de Voz (Internet)

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

- 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.
- Independente do texto. O usuário pronuncia frases conforme seu desejo. O sistema processa qualquer discurso do usuário.
- 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 (Moreira, 2001).

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: na abordagem tradicional, por meio de PCA (*Principal Component Analysis*) e FA (*Factor Analysis*); na abordagem de estimativa de médias e covariâncias; e na estimativa de divergências (Moreira, 2001).

3.9.1.1 Métodos de Comparação de Reconhecimento de Voz

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 (Moreira, 2001).

• *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.

3.9.2 Tecnologia de Reconhecimento Facial

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 (Costa, 2001):

3.9.2.1 Processo de Aquisição de Imagem

O processo de aquisição de imagens da face possui abordagens que podem ser divididas nos seguintes grupos, conforme demonstrado na Fig. 3.4:

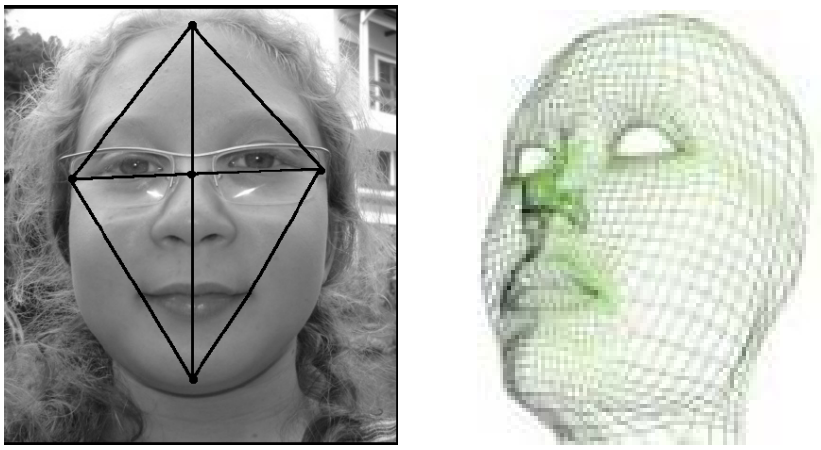
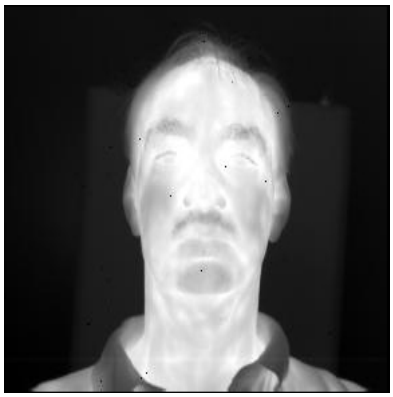


Figura 3.4 - Funcionamento de 3 Sistemas Diferenciados de Captação de Imagem e Reconhecimento Facial



- 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.

- 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. A combinação multimodal de abordagens 2D e 3D pode incrementar a precisão total do sistema. 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. Para a obtenção de imagens 3D da face, podemos utilizar: 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; técnicas baseadas em projeção de um padrão de luz conhecido, cuja distorção pode ser capturada para reconstruir a aparência 3D da face; e técnicas baseadas em varredura a laser, que proporciona um mapa tridimensional pela amostragem de cada ponto da superfície da face (Moreira, 2001).

- 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.

- 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 (Moreira, 2001)

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. Existem duas abordagens para a extração de características das imagens da face (Costa, 2001):

- Abordagem global/ Aparência da Face. A idéia básica é reduzir uma imagem de milhares de pixels para um conjunto de números. A distintividade da face pode ser capturada, independentemente do "ruído" produzido pelas variações de luminosidade, textura da pele, reflexos e outros fatores. Para isto, a imagem da face é transformada, dentro de um espaço composto por funções básicas de imagens. Falando simplesmente, as funções básicas de imagens, conhecidas como *eigenfaces*, 10 são usadas ponderadamente para compor a imagem da face em questão. 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*).

- 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.

3.9.2.2 Método de Comparação de Reconhecimento Facial

O processo de comparação está baseado em três tipos de métodos (Costa, 2001):

- Métodos holísticos, que usam toda a região da face. Dentre as várias técnicas existentes, a PCA, baseada em *eigenfaces*, é a mais utilizada.
- 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.
- 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. 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 (Moreira, 2001).

3.9.3 Tecnologia da Impressão Digital

É uma das formas de reconhecimento biométrico de menor custo, juntamente com o reconhecimento pela voz. Talvez seja por esse motivo, que se constitui, atualmente, na técnica mais utilizada, conforme demonstrado na Fig. 3.5:

Figura 3.5 - Funcionamento do Sistema de Captação de Imagem e Reconhecimento Através da Digital (Internet)

Existem três tipos de leitores de digitais (Costa, 2001):

• Ópticos: O dedo é colocado sobre uma plataforma de vidro e uma imagem do dedo é capturada. Estes dispositivos tornaram-se pequenos e baratos;

• Ultra-som: O dedo é colocado sobre uma plataforma de vidro e uma varredura de ultra-som é efetuada;

• Baseados em chip: O usuário coloca seu dedo direto em um chip de silício. Diversas empresas estão realizando grandes investimentos na evolução dessa tecnologia. Um dos empregos que já se nota é o acesso de usuários a sistemas operacionais, no lugar de se fornecer uma identificação e senha.

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 (Moreira, 2001).

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 (Moreira, 2001).

3.9.3.1 Processo de Aquisição de Impressão Digital

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 (Costa, 2001):

- 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”×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”×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 um captador de imagem digital.

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 a seguir (Costa, 2001):

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

- A abordagem local está relacionada com detalhes marcantes das próprias linhas, conhecidos como minúcias (*minutiae*). Embora exista mais de uma centena de tipos de detalhes catalogados, os mais utilizados em sistemas automatizados são a terminação de linha e a bifurcação de linha. 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;

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

3.9.3.2 Método de Comparação de Impressões Digitais

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:

- 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;
- Concordância qualitativa, ou seja, os detalhes de minúcias devem ser idênticos;
- 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.

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

- 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;

- técnicas baseadas em características, onde a comparação baseada em minúcias é o método mais conhecido e mais largamente usado para comparação, graças à analogia com a maneira pela qual os especialistas comparam impressões digitais em aplicações forenses e graças à aceitação legal como prova de identidade na maioria dos paises. Os algoritmos de comparação mais comuns consideram cada minúcia como uma tripla $m = (x,y,q)$, contendo a informação de localização espacial 2D (x,y) e de orientação q. 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.

3.9.4 Tecnologia da Geometria da Mão

Esta técnica já é utilizada desde a década de 70. Considera-se que é baixíssima a probabilidade de que existam pessoas com a geometria da mão idêntica e que o formato da mão, a partir de uma determinada idade, não sofre alterações. Neste tipo de técnica realiza-se uma análise tridimensional do comprimento e largura da mão para que seja possível a identificação de um indivíduo. Após o reconhecimento de voz e da impressão digital, a geometria da mão é a técnica mais utilizada. Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai destas medidas um identificador matemático único na criação do modelo, conforme demonstrado na Fig. 3.6 (Costa, 2001).

Figura 3.6 - Funcionamento do Sistema de Captação de Imagem e Reconhecimento Através Geometria da Mão (Internet)

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 (Moreira, 2001).

3.9.4.1 Processo de Aquisição de Tecnologia da Geometria da Mão

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. 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. 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 imagem lateral da mão (Moreira, 2001).

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

3.9.4.2 Método de Comparação da Geometria da Mão

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 (Moreira, 2001).

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×FRR (ou seja, a EER) em torno de 1,5% para esta tecnologia (Moreira, 2001).

3.9.5 Tecnologia da Assinatura

Nesta forma de reconhecimento biométrico o usuário pode ter de repetir diversas vezes a sua assinatura para que o sistema possa obter um padrão médio, possibilitando o reconhecimento posterior. Este fato se constitui em um fator de inconveniência desta forma de reconhecimento biométrico.Existe uma outra forma de reconhecimento através da assinatura que se constitui na dinâmica da assinatura. Nesse método o equipamento utilizado é a caneta óptica, conforme demonstrado na Fig. 3.7(Costa, 2001).

Figura 3.7 - Funcionamento do Sistema de Captação e Reconhecimento Através Assinatura Digital (Internet)

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.

3.9.5.1 Processo de Aquisição da Assinatura

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 (Moreira, 2001).

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

O processo de extração de características se baseia principalmente na componente temporal. Na análise dinâmica, são introduzidas as noções de tempo e pressão, além do espaço

bidimensional do papel. Os dispositivos utilizados podem, por exemplo, registrar um fluxo de vetores penta-dimensionais colhidos em pontos temporais equidistantes.

Esses vetores poderiam, por exemplo ser compostos por $A = (x,y, p,qx,qy)$, onde x e y correspondem à posição, p corresponde à força axial exercida pela caneta e qx e qy 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 (Moreira, 2001).

3.9.5.2 Método de Comparação de Assinatura

Na análise de assinaturas dinâmicas, as abordagens de comparação incluem as medidas de distâncias euclidianas entre as trajetórias de canetas, medidas de correlação regional e reconhecimento temporal-probabilístico como as cadeias de Markov ocultas. Afinal, o problema pode ser reduzido à classificação temporal. Durante os últimos 30 anos, numerosos algoritmos e modelos foram desenvolvidos. O conjunto de características no qual o processo de decisão está baseado, é constituido de funções temporais como pressão, posição, velocidade e aceleração, representadas por conjuntos de valores discretos periódicos e representadas por valores paramétricos obtidos com base no processamento de tais funções. Os métodos podem ser acomodados em quatro grupos (Moreira, 2001):

- 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.

- Classificadores elásticos: Esta técnica mais antiga, obscurecida desde o advento das cadeias de Markov ocultas, é baseada na utilização de DTW (*Dynamic Time Warping*). 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.

- 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.

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

3.9.6 Tecnologia da Retina

Pode-se dizer que é forma biométrica mais segura, ou seja, a que apresenta mais dificuldades para o acesso de um usuário não autorizado. Mesmo que uma pessoa tenha doenças graves como glaucoma, ainda assim é possível sua correta identificação. Isso é possível porque o padrão de veias da retina é a característica com maior garantia de singularidade. O funcionamento e o sistema de captação de imagem e reconhecimento é apresentado na Figura 3.8.

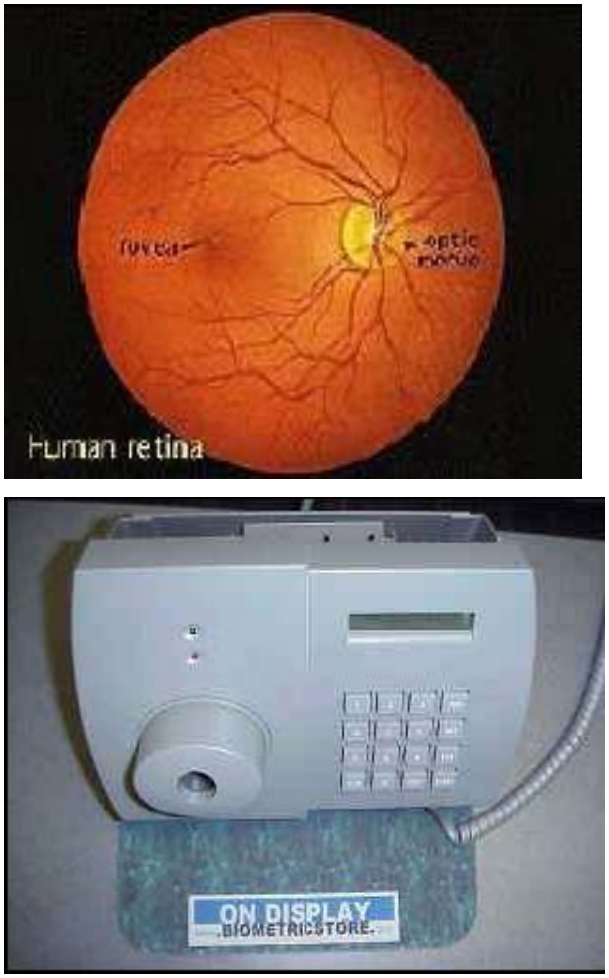


Figura 3.8 - Funcionamento do Sistema de Captação de Imagem e Reconhecimento Através Retina (Internet)

3.9.7 Tecnologia da Íris

A íris é o anel colorido que circunda a pupila do olho. A íris possui um padrão único que permite a identificação de um indivíduo. Também é uma técnica bastante segura e apresenta menor exigência na captura de imagens do que a técnica da retina. A captura da imagem é feita através de uma câmera preto e branco e a identificação da pessoa é realizada através de um scanner que realiza o mapeamento da íris. A pessoa olha a uma distância aproximada de 30 cm por alguns segundos. Mesmo que esteja usando lentes de contato, o sistema realiza a identificação com segurança, conforme demonstrado na Fig. 3.9.

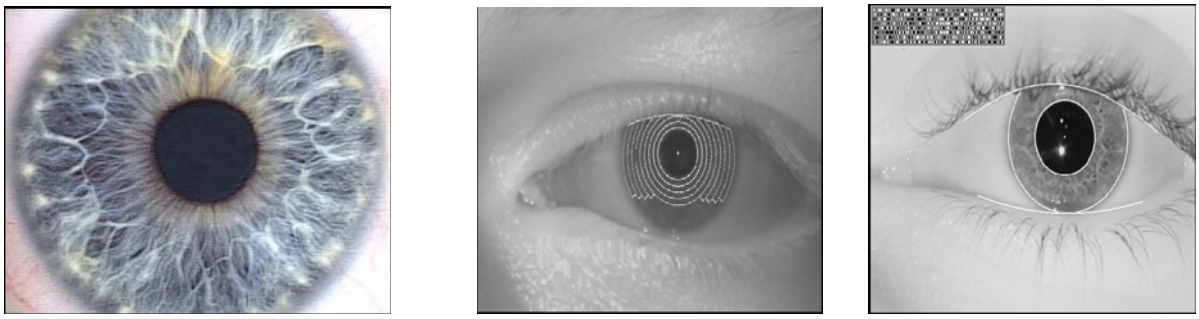


Figura 3.9 - Funcionamento do Sistema de Captação de Imagem e Reconhecimento Através Íris (Internet)

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 (Costa, 2001).

3.9.7.1 Processo de Aquisição da Imagem da Íris

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 (Moreira, 2001).

O processo de extração das características da íris para a criação de um *IrisCode* funciona simplificadamente da seguinte maneira (Costa, 2001):

- É localizada a imagem da íris na imagem adquirida, pela estimativa do centro da pupila;
- O padrão da íris é isolado da pupila;
- 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.

3.9.7.2 Métodos de Comparação das Imagens da Íris

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. 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 (Moreira, 2001).

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%) (Moreira, 2001).

4 ANÁLISE DA TECNOLOGIA DO SISTEMA BIOMÉTRICO UTILIZADOS PARA CONTROLE DE ACESSO

4.1 APRESENTAÇÃO

De um lado, as tecnologias biométricas disponíveis possuem atributos, aos quais podem ser vinculados valores numéricos. De outro lado, a aplicação possui requisitos. Também podem ser atribuídos valores numéricos para a importância de tais requisitos. A união entre requisitos e atributos resulta em valores de avaliação para cada tecnologia. A interpretação dos pesos simbólicos como fatores numéricos pode ser ajustada arbitrariamente. Esta matriz de avaliação é especialmente útil em estágios preliminares de análise, para apontar as sensibilidades críticas do suposto sistema. Entretanto, um sistema biométrico pode ser suficientemente grande para incorrer em grandes investimentos. Nestes casos, uma avaliação mais consistente se mostra necessária. Biometria é uma tecnologia emergente com forte competição de mercado e é desejável a existência de métricas precisas e procedimentos de teste bem definidos (Costa, 2004).

4.2 SELEÇÃO DA TECNOLOGIA

Selecionar uma tecnologia biométrica adequada para uma dada aplicação específica é um processo que envolve muitos fatores. A precisão é um fator importante, mas de maneira alguma é o fator mais importante. De uma maneira simplista, fatores de seleção são extraídos dos requisitos da aplicação. Estes fatores de seleção orientam a escolha da tecnologia biométrica mais adequada. Estes fatores, embora não sejam diretamente quantificáveis, são extremamente úteis no processo de seleção (Costa, 2004).

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

A tecnologia biométrica automatizada ainda é suficientemente emergente para produzir definições duvidosas de precisão e desempenho. Normalmente, as avaliações são implementadas por meio de uma competição entre os interessados (fabricantes ou grupos de pesquisa). Existem três metodologias proeminentes de avaliação (Costa, 2004):

- Avaliação de tecnologia: A avaliação 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.

- Avaliação de cenário: O objetivo da avaliação de cenário é determinar o desempenho geral do sistema numa aplicação prototipada ou simulada. Este tipo de avaliação ocorre em uma instalação especial, um ambiente de teste que simula um ambiente de produção. O ponto fraco desta avaliação fim-a-fim é que os dispositivos não são realmente atacados, o que leva a valores irreais de FAR

- Avaliação operacional.: 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, que dependem de características. Embora seja a avaliação mais realista, não pode medir a verdadeira FAR, já que os eventos de falsa aceitação serão de conhecimento exclusivo dos fraudadores. No entanto, ainda há a possibilidade de estimativa da verdadeira FAR por intermédio de complemento a esta avaliação, por meio da utilização de algo parecido com a contratação de testes de invasão, a exemplo do que é feito com segurança de redes de computadores.

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. Um teste de avaliação pode ser

caracterizado por cinco passos: planejamento, aquisição dos dados, análise, estimativa das incertezas e relatório final de desempenho (Costa, 2004).

4.3 ANÁLISE DAS VANTAGENS E DESVANTAGENS DAS TECNOLOGIAS DO SISTEMA BIOMÉTRICO

Para cada uma das técnicas apresentadas, ferramentas estão sendo disponibilizadas em profusão. Para cada uma delas existem mais de dois ou três fornecedores de reconhecimento mundial que colocam no mercado, a cada ano, novas versões de suas ferramentas. Porém, mais importante do que a escolha de dispositivo físico para ser utilizado como identicação, semelhante a um cartão de crédito magnético. Ferramentas é a determinação das políticas que serão implementadas em cada ambiente informatizado.

A definição das políticas deve preceder a escolha de qualquer ferramenta, sendo que as ferramentas devem apoiar e facilitar a implementação das políticas escolhidas para a organização, podendo implicar na escolha de diferentes tecnologias e diferentes ferramentas até para o mesmo ambiente de rede de computadores. A utilização das ferramentas disponíveis nos próprios sistemas operacionais garantem que vários itens descritos anteriormente possam ser implementados, como o que trata de administração de acesso. Mecanismos próprios para testar a expiração de senhas, inibir tentativas sucessivas de adivinhação, bloquear ID de usuário com ataques e induzir a mudança periódica de senhas, devem estar ativados pelos administradores de segurança em qualquer ambiente de informática.

A elaboração de algoritmos para mudança de senha deve ser particularmente destacada e sugestões de resolução deste problema através de métodos numéricos e equações matemáticas ajudam a elaborar senhas difíceis de serem descobertas, mas de fácil assimilação pelo usuário.

A determinação do que deve ser feito é estabelecida pela política de acesso lógico. A questão de como fazer deve se nortear pela mesma política, mas admite várias possibilidades de resolução.

4.3.1 Vantagens da Tecnologia de Reconhecimento de Voz

Os pontos fortes da tecnologia de autenticação biométrica baseada no padrão de voz são (Costa, 2001):

- 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 encontrar barreiras ao usuário, mas em situações onde o usuário já utiliza a voz, 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.

4.3.2 Desvantagens da Tecnologia de Reconhecimento de Voz

Quanto aos pontos fracos, podemos citar (Costa, 2001):

- 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. Os exemplos mais comuns de dos diversos banco de dados disponíveis são (Moreira, 2001):

• 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 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++.25 É capaz de reconhecer vários tipos de características e tem sido usado nas avaliações do NIST. Pode servir como base de comparação com outros sistemas.

As taxas de erro para sistemas de autenticação por meio da voz são muito dependentes da aplicação. Isto quer dizer que bons resultados obtidos em competições de avaliação ou publicados em especificações de fabricantes, não significam necessariamente que os mesmos serão obtidos na prática, nas aplicações específicas. Esta tecnologia está amadurecida por meio de 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 (Moreira, 2001).

4.3.3 Vantagens e Desvantagens da Tecnologia de Reconhecimento Facial

Os pontos fortes da tecnologia de autenticação biométrica baseada na aparência da face são (Costa, 2001):

- 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 (Costa, 2001):

- Em sistemas automatizados de autenticação por meio da face, as condições de iluminação precisam ser controladas. Outros desafios técnicos ainda precisam ser vencidos.
- É uma tecnologia biométrica suficientemente boa para aplicações de verificação de pequena escala. No entanto, é uma biometria pobre para aplicações de identificação de larga escala.
- Uma maneira óbvia e fácil de fraudar o sistema, em aplicações de *screening*, é a utilização de disfarces.

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

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

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

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

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

Competições internacionais envolvendo reconhecimento de face também são costumeiras. Existem competições documentadas desde 1995, com base nos três bancos de dados citados (BANCA, FERET e XM2VTS). A competição FVC2004 (*Face Verification Contest* 2004) foi baseada no banco de dados BANCA. A competição FRVT2006 (*Face Recognition Vendor Test* 2006) 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. Por exemplo, o OSCVL (*Intel Open Source Computer Vision Library*), contém algoritmos de detecção e reconhecimento de faces. A iniciação em experimentos de avaliação de sistemas de reconhecimento de face também não é difícil. Um sistema completo de avaliação é fornecido pela Colorado State University, compreendendo implementações de quatro algoritmos de reconhecimento que servem como ponto de partida.

4.3.4 Vantagens e Desvantagens da Tecnologia de Impressão Digital

Os pontos fortes da tecnologia de autenticação biométrica baseada em impressão digital são (Costa, 2001):

- Esta tecnologia pode proporcionar bastante precisão;
- Existe uma longa tradição legal no uso da impressão digital como identificador imutável;

- Existem grandes bancos de dados legados de impressões digitais;
- A impressão digital pode ser colhida facilmente a baixo custo.

Quanto aos pontos fracos, podemos citar (Costa, 2001):

- 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 digital pode desaparecer com o envelhecimento.

4.3.5 Vantagens e Desvantagens da Tecnologia da Assinatura

Os pontos fortes da tecnologia de autenticação biométrica baseada na dinâmica da assinatura são (Costa, 2001):

- A assinatura dinâmica é uma combinação de informação e biometria. O conteúdo e modo da escrita podem ser escolhidos e até mesmo alterados pelo usuário.
- Possui grande aceitação por parte do usuário.
- A assinatura dinâmica é bastante difícil de ser fraudada. A comunidade interessada em autenticação por meio da dinâmica de assinatura define o nível de sofisticação do fraudador em categorias, como *zero-effort forgery*, *home-improved forgery*, *over-the-shoulder forgery* e *professional forgery*. Esta divisão em categorias por nível de sofisticação ainda não existe em outras tecnologias biométricas.

Quanto aos pontos fracos, podemos citar (Costa, 2001):

- 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. Poreste 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%) (Moreira, 2001).

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. O projeto BISP21 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 (Moreira, 2001).

Resultados relatados na primeira competição internacional de verificação por dinâmica da assinatura (SVC 2004) relatam taxas de erro 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 (Moreira, 2001).

4.3.6 Vantagens e Desvantagens da Tecnologia da Retina

Os pontos fortes da tecnologia de autenticação biométrica baseada no padrão da retina são (Costa, 2001):

Não existem casos relatados de falsa rejeição ou fraudes através deste método de reconhecimento biométrico. Justamente por este aspecto da segurança na identificação é que a análise de retina tem sido uma alternativa de grande interesse no mercado. Os analisadores de retina medem o padrão de vasos sangüíneos, usando um laser de baixa intensidade e uma câmera.

Quanto aos pontos fracos, podemos citar (Costa, 2001):

O custo para a implantação deste método é alto, além do que para a captura da imagem da retina, o usuário deve olhar fixamente para um ponto infravermelho por cerca de 5 segundos, sem piscar. Algumas pessoas temem que tal operação possa causar danos à vista. Este aspecto representa uma inconveniência desta técnica (Costa, 2001).
Existem relatos de modificação dos vasos da retina com o envelhecimento.

4.3.7 Vantagens e Desvantagens da Tecnologia da Imagem da Íris

Os pontos fortes da tecnologia de autenticação biométrica baseada no padrão da íris são (Costa, 2001):

- 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.
- 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 (Costa, 2001):

- 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.

- 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 (Moreira, 2001):

• 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.

• 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.

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

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

Existe pelo menos um sistema de reconhecimento baseado em íris de códigofonte aberto. O sistema, implementado em MATLAB, basicamente usa como entrada uma imagem do olho e devolve como saída um perfil biométrico em código binário (Moreira, 2001).

4.4 COMPARATIVO SUMÁRIO DAS TECNOLOGIAS UTILIZADAS PELA BIOMETRIA PARA CONTROLE DE ACESSO

A identificação da tecnologia para controle da entrada de serviço para pessoas pode ser feito pela comparação do grau (alto, médio ou baixo) com que cada tecnologia satisfaz as propriedades desejáveis de características biométricas, embora resumida, ela permite obter um panorama geral dessas tecnologias, conforme demonstrado na Tabela 4.1

Tabela 4.1 - Analise Comparativa dos Principais Sistemas Biométricos

Tipo de Tecnologia	Objeto	Característica	Função
Reconhecimento da voz	Voz	Amigável e Não-intrusivo	Analise do som
Reconhecimento facial	Face humana	Amigável e Intrusivo	Analise da Face
Impressão digital	Dedos	Amigável e Nào-intrusivo	Analise da Digital
Geometria da mão	Mão	Amigavel e Não-intrusivo	Analise da Mão
Assinatura	Escrita	Amigável e Não-intrusivo	Analise da escrita
Retina	Veias da retina	Não amigável e Intrusivo	Analise das veias
Íris	Contorno da iris	Não amigável e Intrusivo	Analise do formato

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, conforme demonstrado na Tabela 4.2.

Tabela 4.2. Comparativo Entre as Características de Alguns Identificadores Biométricos para Controle de Acesso

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

4.5 SELEÇÃO DE SOLUÇÕES MISTAS

Um sistema de reconhecimento misto reúne as tecnologias de biometria com outras tecnologias de identificação automática, como por exemplo, um relógio de ponto que utiliza um leitor de cartão de acesso, senha e impressão digital. Neste caso, combinam-se três fatores: uma coisa que se possui (cartão), uma coisa que se conhece (senha) e uma coisa que se é (biometria). O conjunto destas tecnologias multiplica a segurança do equipamento, pois dificulta o êxito de fraudes, contudo aumenta a possibilidade de erro e freqüentemente diminui a eficiência do seu uso, pois cada usuário leva mais tempo para completar as várias etapas da operação (Costa, 2004).

Já um sistema de reconhecimento multimodal aplica dois ou mais parâmetros biométricos para confirmar a identidade do indivíduo como, por exemplo, um portão eletrônico que possui equipamento de análise simultânea de geometria facial, voz e do movimento dos lábios. Esta é a mais forte tendência de sistemas biométricos de controle de acesso, contudo apresenta limitações de desempenho (velocidade de reconhecimento) à medida que aumenta a quantidade de usuários autorizados (Costa, 2004).

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. A obtenção de multiplicidade pode se dar em diversos pontos do sistema (Rich, 1998) :

- Múltiplas biometrias podem ser utilizadas (voz e face, por exemplo) ou múltiplas unidades da mesma biometria (dedos diferentes ou olhos diferentes, por exemplo).
- Múltiplos sensores, como sensores óticos e capacitivos para impressão digital.
- Múltiplas amostras da mesma biometria; por exemplo, múltiplas impressões do mesmo dedo.
- 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 (Rich, 1998):

- Fusão na amostra, ou seja, os diversos dados obtidos são concatenados em um único vetor de características com maior poder de diferenciação.
- Fusão na comparação, ou seja, os diversos escores de similaridade obtidos são combinados por meio de médias ponderadas.
- 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 (Rich, 1998).

4.6 ARMAZENAMENTO DE DADOS

Existem várias possibilidades de distribuição dos processos componentes de um sistema biométrico. Num caso extremo, pode-se 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 (Rich, 1998)

Noutro extremo, pode-se ter um ampla distribuição dos processos. Supondo um sistema de larga escala, com centenas de milhares de perfis registrados e diversos locais de aquisição de

biometria, como é o caso de um sistema de autenticação de clientes bancários em máquinas de auto-atendimento. O processo de aquisição pode se dar em diversos pontos do sistema. O armazenamento dos perfis pode se dar em *smart cards* em poder do usuário. Uma cópia do perfil pode ou não ser armazenado em servidor central para o caso de uma reemissão de cartões extraviados. Os processos de extração e comparação também podem estar distribuídos, dependendo da conveniência para a arquitetura do sistema. Estes processos podem ser locais (junto ao dispositivo de aquisição) ou remotos (em servidor ou até mesmo no próprio *smart card*) (Rich, 1998).

4.6.1 Forma de Armazenamento de Dados

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

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

O sistema armazena os perfis dos usuários candidatos a acesso a determinado local. A quantidade de usuários pode variar de unidades, no caso de acesso a uma residência, ou centenas, no caso de controle de acesso a academias, ou milhares, para controle de acesso a grandes prédios ou instalações.

O armazenamento remoto corresponde ao armazenamento em um servidor, o que quase sempre quer dizer uma base de dados centralizada. Esta solução é adequada para aplicações onde o número de usuários é grande ou quando é necessária verificação remota. Este processo pode ser comprometido quando a segurança dos dados é ameaçada por sistemas de comunicação ou redes vulneráveis ou por abuso de privilégios na manipulação da base de dados. Os sistemas de identificação (busca 1:N) de larga escala geralmente se utilizam da modalidade de armazenamento remota. Este sistemas geralmente comportam milhões de usuários e possuem requisitos mais refinados de precisão e desempenho. Os sistemas de verificação (busca 1:1) de larga escala podem ou não se valer desta modalidade de armazenamento (Moreira, 2001).

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

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

Quanto à entidade armazenadora, podemos considerar dois tipos de entidades, que chamamos de agentes autorizados e agentes de confiança. Um agente autorizado é uma organização que adota a autenticação biométrica e assume a responsabilidade por registrar e administrar os perfis biométricos de seus usuários conforme os requisitos dessa autenticação (Rich, 1998).

4.7 SEGURANÇA DOS DADOS

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 (Moreira, 2001).

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.

4.7.1 Vulnerabilidade dos Dados

Outra abordagem, que integra conceitos de gerenciamento e de segurança, propõe uma metodologia estruturada (*BASS model*) bastante abrangente na análise de vulnerabilidades A lista a seguir apresenta apenas alguns exemplos de vulnerabilidades (Moreira, 2001):

• 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.

• 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. 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 (Moreira, 2001).

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

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

4.7.2 Riscos de Fraudes

Assim como outros mecanismos de segurança, qualquer sistema biométrico pode ser fraudado com um adequado investimento em tempo e dinheiro. Do ponto de vista do gerenciamento de riscos, a tarefa do projetista de segurança é fazer com que o custo para se violar a segurança do sistema seja superior ao benefício obtido com a violação.

A única coisa que pode ser feita a favor da segurança é o incremento dos custos envolvidos para a consecução da fraude. A vantagem do projetista é que ele pode investir tempo e

dinheiro previamente para tentar proteger o sistema contra todo ataque possível e imaginável. A vantagem do impostor é que ele apenas necessita usar a criatividade para encontrar um ataque ainda não pensado. Esta luta entre ataques e contramedidas pode ser bem exemplificado por meio de uma coletânea de ataques e contramedidas referente a um sistema hipotético baseado no padrão da íris (Costa, 2001).

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 (Moreira, 2001).

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

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

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

• Resposta sumária - As respostas sumários ou ocultação dos dados (*hiding data*), servem para evitar ataques *hill-climbing*. Assim, o sistema deve fornecer apenas uma resposta ao usuário não autenticado (NÃO), abstendo-se de explicar qual o motivo da recusa e abstendo-se, é claro, de informar qualquer valor de escore obtido.

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

• Detecção de vitalidade (*liveness detection*) - A detecção de vitalidade (ou detecção de vivacidade) num sistema biométrico de autenticação deveria assegurar que somente características reais, pertencentes a pessoas vivas, fossem aceitas como válidas. Isto tornaria o sistema mais seguro e aumentaria também o poder de não repudiação. No entanto, até mesmo pequenos esforços podem levar à fraude em sensores biométricos atuais. Trabalhos descrevendo fraudes em impressões digitais, 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 (Costa, 2001).

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* (Moreira, 2001).

4.7.3 Aplicação dos Sistemas Biométricos nos Aeroportos/Aeroporto de Brasília

Um sistema de reconhecimento misto ser facilmente aplicado em um aeroporto, a utilização de um sistema misto pode ser utilizado em acesso de funcionários, utilizando como por exemplo a catraca associada ao sistema biométrico da digital. No momento da aplicação da digital, um monitor mostraria a face do funcionário, com seus dados e acesso autorizados.
Se falou da impressão digital, por trata-se do sistema mais economicamente viável para aplicação imediata em um aeroporto. Para os passageiros, a impressão digital também poderia ser utilizada na liberação de acesso, através de cadastramento antecipados dos dados dos clientes, compondo um grande banco de dados.

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. A obtenção de multiplicidade pode se dar em diversos pontos do sistema (Rich, 1998):

No aeroporto de Brasília, devido as suas características fisicas o Sistema Biométrico pode ser utilizado facilmente na entrada de serviço do terminal principal e também no acesso de funcionários pelo terminal II. Pode-se utilizar também o sistema nos portões de acesso de veículos, através da liberação de cancela, após a confirmação da identidade do funcionário e conferência pelo sistema da autorização de acesso nos referidos locais.

5 CONCLUSÃO

5.1 APRESENTAÇÃO

A tecnologia biométrica nas suas diversas formas (impressão digital, face, íris, retina, entre outras) tem se mostrado eficiente no aspecto segurança. A utilização isolada de cada uma dessas técnicas, não garante uma segurança absoluta. O conjunto de técnicas a ser escolhido dependerá do grau de segurança que se pretende alcançar.

Uma área de pesquisa a ser melhor explorada, está relacionada ao estudo dos níveis de segurança que podem ser obtidos, considerando-se a utilização conjunta de duas ou três técnicas de reconhecimento biométrico de forma simultânea.

Os pontos fortes das tecnologias biométricas em geral são: a biometria é fortemente vinculada a uma identidade e a biometria não precisa ser memorizada, nem pode ser esquecida ou emprestada. No entanto, estes pontos fortes levam também a fraquezas correspondentes, que são: a biometria não é revogável e a biometria não é segredo. Pesquisas têm sido levadas a cabo no sentido de eliminar ou amenizar os pontos fracos.

De um lado, as tecnologias biométricas disponíveis possuem atributos, aos quais podem ser vinculados valores numéricos. De outro lado, a aplicação possui requisitos. Também podem ser atribuídos valores numéricos para a importância de tais requisitos. A união entre requisitos e atributos resulta em valores de avaliação para cada tecnologia. A interpretação dos pesos simbólicos como fatores numéricos pode ser ajustada arbitrariamente. Esta matriz de avaliação é especialmente útil em estágios preliminares de análise, para apontar as sensibilidades críticas do suposto sistema. Entretanto, um sistema biométrico pode ser suficientemente grande para incorrer em grandes investimentos. Nestes casos, uma avaliação mais consistente se mostra necessária. Biometria é uma tecnologia emergente com forte competição de mercado e é desejável a existência de métricas precisas e procedimentos de teste bem definidos (Costa, 2004).

Uma mensagem final sobre a utilização de sistemas biométricos não pode deixar de lado 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.

Selecionar uma tecnologia biométrica adequada para uma dada aplicação específica é um processo que envolve muitos fatores. A precisão é um fator importante, mas de maneira alguma é o fator mais importante. De uma maneira simplista, fatores de seleção são extraídos dos requisitos da aplicação. Estes fatores de seleção orientam a escolha da tecnologia biométrica mais adequada. Estes fatores, embora não sejam diretamente quantificáveis, são extremamente úteis no processo de seleção (Costa, 2004).

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

5.2 SUGESTÃO E RECOMENDAÇÃO DE PESQUISA

Além da larga utilização em investigação criminal, as tecnologias biométricas estão sendo rapidamente sendo adotadas numa grande variedade de aplicações de segurança, como controle de acesso físico e lógico, comércio eletrônico, gestão digital de direitos autorais, segurança de prédios e residências e bloqueio de equipamentos. Em geral, essas aplicações requerem, dos subsistemas biométricos, alta precisão, alto desempenho e baixo custo (Couto, 2007).

Entretanto, embora tenha havido grandes avanços recentes, ainda é necessário um vigoroso esforço de pesquisa para resolver muitos problemas desafiadores.

O uso da biometria para a identificação de pessoas já é realidade e é pouco provável que outro conceito a substitua. O constante avanço das tecnologias de comunicação faz com que haja cada vez mais interação entre as pessoas e aumente a utilização de serviços, principalmente os que estão ligados ao setor financeiro. O fato é que à medida que o acesso à informação aumenta, parece haver a mesma proporção em golpes. Além disso, deve-se considerar que a biometria também pode representar uma comodidade ao usuário, uma vez que está se tornando insuportável ter uma senha para cada serviço utilizado em nosso cotidiano. Por outro lado, há quem acredite que a biometria chegará ao extremo de um sistema conseguir identificar cada ação de uma pessoa, aspecto esse que passa a envolver questões éticas. Apesar disso, é certo que a biometria vai ser cada vez mais parte do dia-a-dia das pessoas. Prova disso é que as tecnologias envolvidas ganham aprimoramentos constantes. Chegará o dia em que você será sua senha.

6 REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Organização do texto: Juarez de Oliveira. 4. ed. São Paulo: Saraiva, 1990. (Série Legislação Brasileira).

BRASIL. **Código Brasileiro de Aeronáutica**. São Paulo: EAPAC, 2001.

BRASIL. IAC 107-1004A - **Controle de Acesso ás Áreas Restritas de Aeródromos Civis Brasileiros com Operação de Serviços de Transporte Aéreo**. 14 jun.2005

BRASIL. IAC 107-1003 – **Comissão de Segurança Aeroportuária**. 29 nov..2002

SILVA, Adyr da, Aeroportos e Desenvolvimento, INCAER, 1990

COSTA, Doris Vieira da. **Segurança Operacional em Aeroportos**. ANAC, 2007. Disponível nainternet.URL:http://www.aviationlatam.com/files/c8462ad16f5521178a66f5521178a66f706564bc769/c_apresentacao_doris.pdf Acesso em: 09 dez. 2007.

COSTA, Marcos da. Criptografia assimétrica, assinaturas digitais e a falácia da "neutralidade tecnológica". Direito em Bits. São Paulo: Fiúza Editores, 2004.

COSTA, Silvia Maria Farani**. Classificação e Verificação de Impressões Digitais**. São Paulo, 2001.
COUTO, Paulo. **Biometria brasileira**. FórumPCs. Disponível em <http:// www.forumpcs.com.br/coluna.php?b=149332>. Acesso em: 07 dez.. 2007.

GUSMÃO, Paulo Dourado de. **Introdução à Ciência do Direito**. Rio de Janeiro:Forense. 1976

MOREIRA, N.S. **Segurança Mínima – Uma Visão Corporativa da Segurança de Informação**. Rio de Janeiro: Axcel Books, 2001.

PACHECO, José da Silva. **Comentários ao Código Brasileiro de Aeronáutica**. Rio de Janeiro: Forense, 2001.

RICH, Elaine. **"Inteligências Artificial"** – Editora McGRAW HILL, 1998.