Sitraer 7 (2008) 255-267 – Tr. 389

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

Sergio Santiago Ribeiro
Yaeko Yamashita

RESUMO
A segurança dos aeroportos é uma questão que deve ser tratada com muito cuidado, visto os parâmetros mundiais, com atentados, utilização de aeronaves como armas e outras situações anormais dos nossos aeroportos. A melhoria contínua de segurança deve ser um objetivo a ser atingido, e para isto, devemos buscar os avanços tecnológicos. A biometria já é utilizada em diversos campos, principalmente para controle de acesso a sistemas ou áreas restritas. Avanços tecnológicos de biometria são apresentados, 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
The security of airports is a subject that need to be worked carefully once it is seen on the international parameters with attacks using airplanes as a destructive arms and in unconventional situations in airports. The increasing security of aiports is a goal to be reached, in order this 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 system or restricted areas. Technological advances in biometry are presented, 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.

1. INTRODUÇÃO

A segurança de passageiros, funcionários e usuários em grandes aeroportos 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 recursos financeiros podem fazer com que tais medidas de segurança não sejam tão efetivos como deveriam, aumentando muito a probabilidade de atentados, seqüestros ou outros atos ilícitos.

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 conforme Ribeiro (2008). Assim, este estudo mostrará as características da biometria e suas

variantes, buscando apresentar seus pontos positivos e negativos, para a melhoria nos sistemas de segurança especificamente no controle de acesso.

2. SEGURANÇA OPERACIONAL EM AEROPORTOS

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.

3. CONTROLE DE ACESSO ÀS ÁREAS RESTRITAS DE AERÓDROMOS

Existe uma Instrução da Aviação Civil que 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. 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.

Sitraer 7 (2008) 255-267 – Tr. 389

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.

4. RESPONSABILIDADE E PRINCÍPIOS GERAIS DE PROCEDIMENTOS RELATIVOS AO ACESSO

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. 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 ARS 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 ARS definidas nos aeroportos está limitado: 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 ARS, 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.

5. 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.

6. TECNOLOGIAS DE ACESSO

Uma visão geral sobre os sistemas biométricos é apresentada como tecnologia baseada em medida dos seres vivos, ou seja, é a identificação de um indivíduo através de suas características físicas e comportamentais e seus principais aspectos de segurança.

6.1. Biometria

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).

6.2. Verificação e identificação

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

Sitraer 7 (2008) 255-267 – Tr. 389

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).

6.3. 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 1:

Tabela 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%

6.4. 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).

6.5. 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 possuírem 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.

6.5. Tipos de Tecnologias Biométricas

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.

6.6. 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 (Moreira, 2001):

Sitraer 7 (2008) 255-267 – Tr. 389

6.7. 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.

6.8. Tecnologias

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

6.8.1. 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. 1. (Costa, 2001):

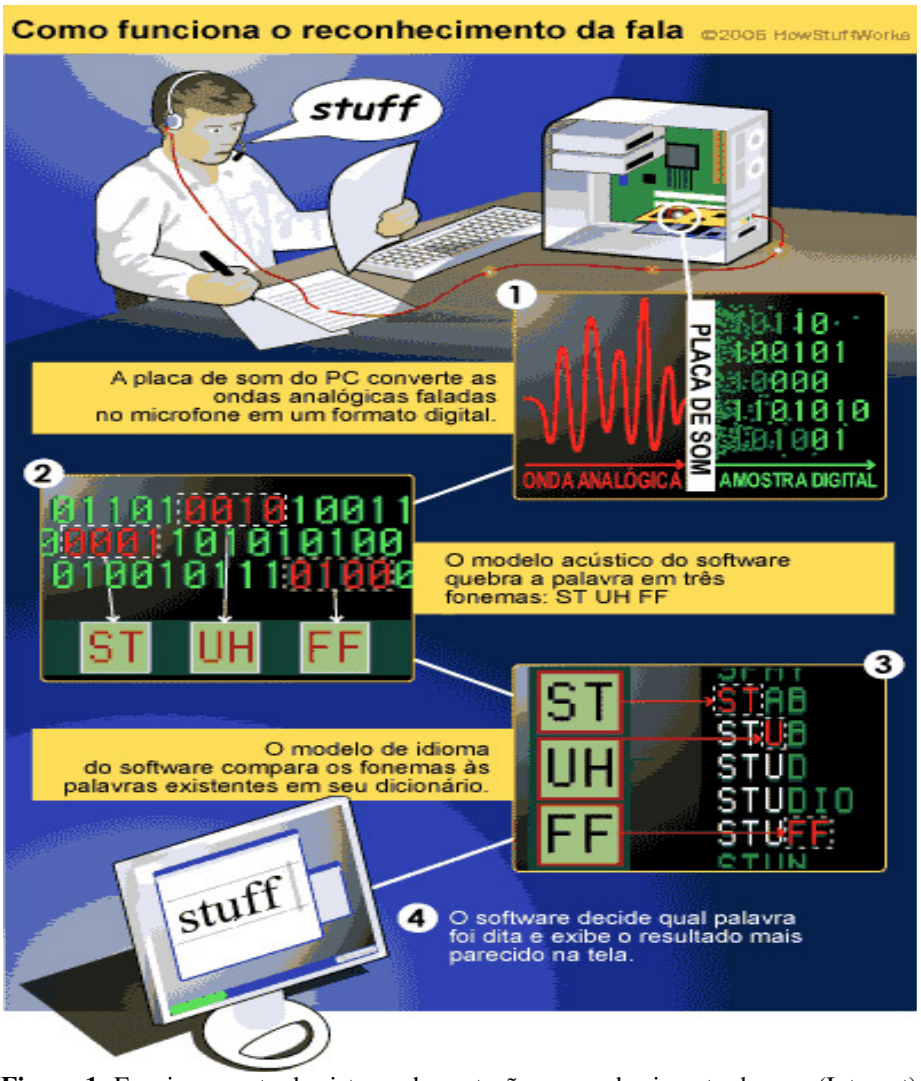

Figura 1: Funcionamento do sistema de captação e reconhecimento de voz. (Internet)

6.8.2. 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):

O processo de aquisição de imagens da face possui abordagens que podem ser divididas nos seguintes grupos, conforme demonstrado na Fig. 2:

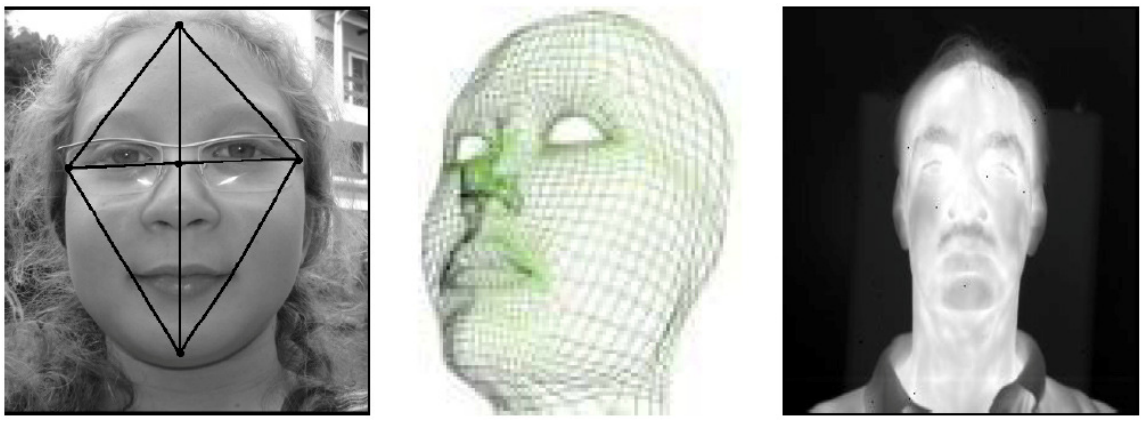

Figura 2: Funcionamento de 3 sistemas diferenciados de captação de imagem e reconhecimento facial.

6.8.3. 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.

Figura 3: Funcionamento do sistema de captação de imagem e reconhecimento através da digital. (internet)

6.8.4. 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

Sitraer 7 (2008) 255-267 – Tr. 389

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. 4. (Costa, 2001).

Figura 4: Funcionamento do sistema de captação de imagem e reconhecimento através geometria da mão. (internet)

6.8.5. 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. 5.(Costa, 2001).

Figura 5: 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.

6.8.6. 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. 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. 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). O funcionamento e o sistema de captação de imagem e reconhecimento são apresentados na Fig. 6.

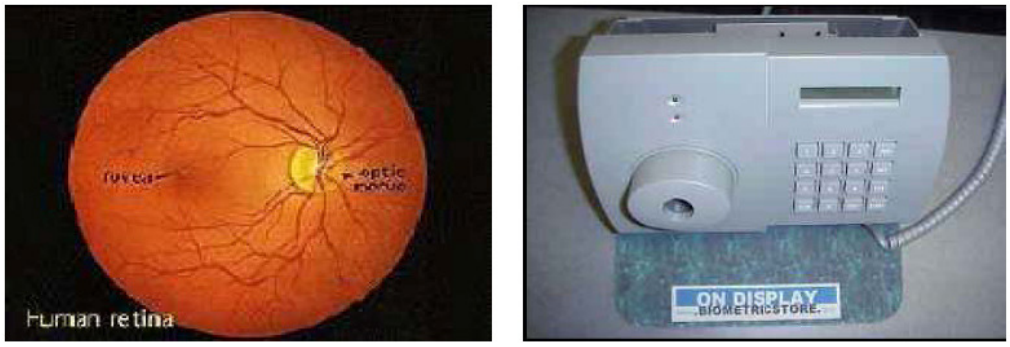

Figura 6: Funcionamento do sistema de captação de imagem e reconhecimento através retina. (internet)

6.8.7. 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. 7.

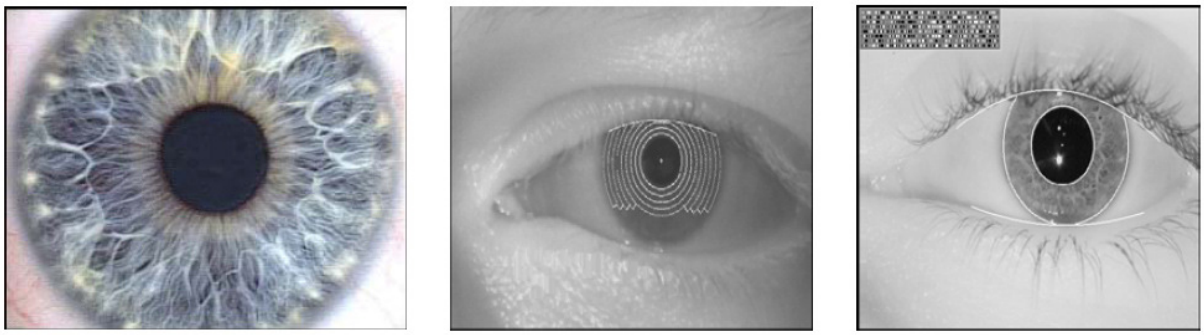

Figura 7: Funcionamento do sistema de captação de imagem e reconhecimento através íris. (internet)

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

Sitraer 7 (2008) 255-267 – Tr. 389

precisa e estável. Dentre poucos sistemas descritos na literatura, o mais conhecido é o IrisCode (Costa, 2001).

7. ANÁLISE DA TECNOLOGIA DO SISTEMA BIOMÉTRICO UTILIZADOS PARA CONTROLE DE ACESSO

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.

7.1. 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).

- *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.

7.2. 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 2.

Tabela 2: Análise 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 3.

Tabela 3: 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

8. CONCLUSÃO

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.

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

Sitraer 7 (2008) 255-267 – Tr. 389

de brechas de segurança do próprio sistema biométrico. 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).

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.

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.(2001) *Código Brasileiro de Aeronáutica.* São Paulo: EAPAC, 2001.
Brasil. IAC 107-1004A (2005) - *Controle de Acesso ás Áreas Restritas de Aeródromos Civis Brasileiros com Operação de Serviços de Transporte Aéreo.* 14 jun.2005
Brasil. IAC 107-1003 (2002) *Comissão de Segurança Aeroportuária.* 29 nov..2002
Costa, D. V. (2007) *Segurança Operacional em Aeroportos.* ANAC. Disponível na internet. 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, S. M. F.(2001) *Classificação e Verificação de Impressões Digitais.* São Paulo
Couto, P. (2007) *Biometria brasileira.* FórumPCs. Disponível em <http://www.forumpcs.com.br/coluna.php?b=149332>. Acesso em: 07 dez.. 2007.
Gusmão, P. D. (1976) *Introdução à Ciência do Direito.* Forense, Rio de Janeiro.
Moreira, N. S. (2001) *Segurança Mínima – Uma Visão Corporativa da Segurança de Informação.* Axcel Books, Rio de Janeiro.
Pacheco, J. S. (2001) *Comentários ao Código Brasileiro de Aeronáutica.* Forense, Rio de Janeiro.
Rich, E. (1998) *"Inteligências Artificial"* – Editora McGRAW HILL.
Ribeiro, S. S. (2008) *Tecnologias de Controle de acesso e sua aplicação no sistema de segurança aeroportuária.* Universidade de Brasília, Monografia do Curso de Especialização em Gestão da Aviação Civil. Brasília.