CENTRO UNIVERSITÁRIO FEEVALE

ALEXANDRE NUNES DE OLIVEIRA

PROPOSTA DE UTILIZAÇÃO DA BIOMETRIA APLICADA NA SEGURANÇA DAS TRANSAÇÕES BANCÁRIAS

Novo Hamburgo, novembro de 2009.

ALEXANDRE NUNES DE OLIVEIRA

PROPOSTA DE UTILIZAÇÃO DA BIOMETRIA APLICADA NA SEGURANÇA DAS TRANSAÇÕES BANCÁRIAS

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Ciência da Computação
Trabalho de Conclusão de Curso

Professor Orientador: Msc. Edvar Bergmann Araujo

Novo Hamburgo, novembro de 2009.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial:

Aos familiares, amigos e às pessoas que convivem comigo diariamente, minha gratidão, pelo apoio emocional - nos períodos mais difíceis do trabalho.

Ao meu orientador por em nossos encontros, responder a todas as minhas perguntas, tirar todas as dúvidas, e a organizar as minhas idéias.

Aos meus professores que ao longo da minha graduação, colaboraram para meu crescimento pessoal e profissional.

RESUMO

O mercado bancário está cada vez mais competitivo. Hoje, agravado pela crise financeira, o setor tem que mostrar que está preparado para situações adversas, gerando a necessidade de uma maior eficiência na gestão dos recursos financeiros sob responsabilidade destas instituições. Por este motivo minimizar riscos é fundamental para dar continuidade aos negócios. O combate a fraudes e as transações irregulares ganham ênfase neste momento, pois o cenário exige a redução de perdas neste setor. Além disto, a crise fez com que o mercado analise novamente este segmento, fazendo com que não apenas os riscos de crédito sejam observados, mas também os riscos operacionais e de imagem. Este trabalho tem o objetivo de propor soluções viáveis para diminuir ou eliminar o sucesso de fraudes em transações financeiras, baseando-se em ferramentas computacionais aplicadas em conjunto com técnicas de Biometria. Pretende-se demonstrar os benefícios da utilização destas ferramentas para o aumento da segurança das transações financeiras realizadas junto aos bancos.

Palavras-chave: Biometria. Sistema Bancário. Ferramentas de TI. Segurança.

ABSTRACT

The banking market is each more competitive time. Today, aggravated for the financial crisis, the sector has that to show that it is prepared for adverse situations, generating the necessity of a bigger efficiency in the management of the financial resources under responsibility of these institutions. For this reason to minimize risks is basic to give continuity to the businesses. The combat the irregular frauds and transactions gain emphasis at this moment, therefore the scene demands the reduction of losses in this sector. Moreover, the crisis made with that the market analyzes this segment again, making with that not only the credit risks are observed, but also the operational risks and of image. This work has the objective to consider viable solutions to diminish or to eliminate the success of frauds in financial transactions, being based on applied computational tools in set with techniques of Biometrics. It is intended to demonstrate the benefits of the use of these tools for the increase of the security of the carried through financial transactions next to the banks.

Key words:Biometrics. Banking system. Tools of information technology. Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AFIS	*Automated Fingerprint Identification System*
ATM	*Automated Teller Machine*
CER	*Crossover Error Rate*
EE	*Equal Error*
EER	*Equal Error Rate*
FAR	*False Acceptance Rate*
FMR	*False Match Rate*
FRR	*False Rejection Rate*
FTE	*Failure to Enroll Rate*
HD	*Hard Disc*
IBG	*International Biometric Group*
ID	Impressão Digital
NEIA	Número de tentativas de identificação de usuário legitimo
NFA	Número de falsas aceitações
NFR	Número de falsas rejeições
NIIA	Número de tentativas de identificação do impostor
RG	Registro Geral

SUMÁRIO

INTRODUÇÃO

Nestes últimos anos tem-se observado os impactos da crise financeira na economia mundial. Crise esta, causada por falhas na gestão do crédito, que por conseqüência ocasionou uma falta de confiança nas práticas operacionais das empresas do setor financeiro. A crise e a competição entre as instituições financeiras, a nível mundial, estão gerando a necessidade de melhorias contínuas. Isto vem estimulando estas empresas a buscarem mudanças nos modelos de gestão, com a finalidade de identificar e minimizar os riscos do setor (KRUGMAN, 2009).

Os prejuízos deste mercado vão além das perdas financeiras oriundas de créditos fornecidos a pessoas e empresas que hoje estão claramente com dificuldades de honrar os compromissos assumidos, denominada de Risco de Crédito, é apenas um dos riscos que o setor enfrenta. Existem outros, como o Risco Operacional e o Risco de Imagem, que necessitam de uma atuação e posicionamento claro por parte dos gestores para reduzir a exposição das organizações a todos os riscos deste segmento (EL-ERIAN, 2008).

O combate às fraudes e falhas no sistema financeiro está em ênfase, pois os Bancos para se fortalecerem neste momento de crise precisam dar respostas firmes ao mercado mundial, reduzindo a exposição aos riscos operacionais e de imagem (GREENSPAN, 2008).

A atual crise determina que todos refaçam suas análises do sistema financeiro global, revendo conceitos e práticas (WOLF, 2008). Os Bancos de Varejo são os bancos que atuam no atendimento direto aos clientes através dos mais diversos meios, como por exemplo: Internet, terminal de auto-atendimento, guichê de caixa, rede de lojistas conveniadas, etc. Neste contexto, cresce a importância sobre as ferramentas de segurança que os bancos utilizam em suas transações, principalmente nas eletrônicas, pois estas já correspondem pelo maior número de operações financeiras no mundo e principalmente no Brasil.

As tecnologias desenvolvidas estão se aperfeiçoando cada vez mais rapidamente, ano após ano, a ponto de muitas das ferramentas que há poucos anos atrás eram parte de filmes de ficção, hoje já são aplicadas no dia a dia. Estas inovações tecnológicas vêem sendo aplicadas no cotidiano com a finalidade de facilitar a vida das pessoas, gerando conforto e agilidade nas mais diversas situações (BARBIERI; SIMANTOB, 2008).

Os Bancos se apresentam na vanguarda da aplicação destas novas ferramentas, pois a automação bancária teve um crescimento gigantesco nas últimas décadas. Nesta mesma proporção estas instituições deixaram de ser apenas fomentadoras da economia, operadoras de crédito, onde captam recursos de um lado e aplicam os mesmos de outro, para, definitivamente, se tornarem o maior meio de pagamentos e de troca de valores entre as mais diversas operações financeiras realizadas no planeta.

Esta nova característica das empresas do setor financeiro fez com que nos últimos anos as tentativas de fraudes contra estas instituições fossem cada vez mais constantes, exigindo destas fortes investimentos em proteção para garantir a continuidade dos negócios (SANTOS, 2006).

Para combater as crescentes tentativas de fraudes, os bancos aplicam diversas ferramentas e sistemas de segurança com a finalidade de impedir ou minimizar a concretização das transações irregulares. Verifica-se no mercado várias medidas com este intuito, como a emissão de cartões com chip, senhas de letras, senhas numéricas, senhas diferentes para cada tipo de canal de atendimento, senhas complementares entre outros mecanismos de identificação do cliente.

Nos processos automatizados assim com nos semi-automatizados existe uma grande possibilidade de fraudes ou auto-fraudes vinculadas às transações financeiras. Os meios físicos que confirmam a presença do cliente no local da transação são passíveis de falhas. Observa-se que os sistemas de identificação mais utilizados como o cartão e a senha, possibilitam a clonagem e cópia destes para uso de pessoa não autorizada, ficando sujeito a falhas de segurança, deixando que transações fraudulentas possam causar prejuízos.

As falhas destes mecanismos de segurança predominantemente utilizados pela maioria das empresas do setor, induzem ao estudo de alternativas viáveis para diminuir os riscos apresentados no atual cenário (SANTOS, 2006). Dentre as diversas alternativas, pode-

se citar a Biometria como sendo uma técnica que tem características que podem atender as necessidades de validação da identificação dos clientes.

Este trabalho tem como objetivo propor alternativas para elevar os níveis de segurança através dos mais diversos tipos e técnicas de identificação de indivíduo. Propõe-se a utilização de ferramentas computacionais combinadas com Biometria como forma de aumentar a segurança de transações financeiras.

Os desafios são muitos, mas com eles vem à oportunidade de estudo e da construção de soluções para atender as fortes expectativas geradas nestes momentos de crise. Por este motivo, o esforço pelo auto-aperfeiçoamento e aprendizado contínuo é importante, pois só através do crescimento do homem como indivíduo é que se constrói uma sociedade mais justa.

O trabalho está organizado em seis capítulos. O primeiro capítulo descreve o conceito básico da Biometria, apresentando os requisitos necessários para sua utilização, seus componentes, funcionalidades e também um pouco de sua historia.

O segundo capítulo aprofunda o estudo da Biometria, pois trata das diferentes tipos de sistemas biométricos, descreve as características de cada tipo e o método de captura desta característica, demonstrando sua viabilidade na utilização como ferramenta de identificação e autenticação de indivíduos.

O terceiro capítulo apresenta a segurança do sistema bancário, descrevendo os métodos e ferramentas aplicadas atualmente como solução para combate a fraudes nas transações financeiras.

O quarto capítulo descreve alguns estudos de casos, que utilizam sistemas biométricos como ferramenta de segurança e de identificação de usuários, inclusive propondo a substituição dos cartões de créditos atuais pela impressão digital do cliente.

O quinto capítulo tem como objetivo o entendimento da importância da seleção do sistema biométrico, demonstrando fatores que devem ser abordados para correta escolha do tipo de biometria mais adequado para cada situação.

O sexto capítulo apresenta a proposta deste trabalho com a aplicação da biometria nas transações bancárias, explicando as características das soluções escolhidas.

1 BIOMETRIA

A Biometria originada do grego Bios(vida) e metron(medida) é o uso de características biológicas em mecanismos de identificação. Entre essas características tem-se a íris, a retina, a impressão digital, a voz, a face, a geometria da mão, etc. O uso de características biológicas para identificação se mostra como uma idéia viável porque cada pessoa possui as características mencionadas diferentes umas das outras (PINHEIRO, 2008).

Pode-se definir a Biometria como sendo as mensurações fisiológicas e/ou características de comportamentos que podem ser utilizadas para verificação de identidade de um indivíduo. Com está possibilidade de medir as particularidades dos seres vivos, abre-se uma grande gama de opções, para confirmar a identificação de um indivíduo, permitindo ampliar cada vez mais os tipos de ferramentas para a área de segurança.

1.1 História da biometria

Ao contrário do que se pensa a biometria não é um conceito novo. Inédito é apenas sua aplicação em sistemas computacionais. Sabe-se, por exemplo, que na época dos faraós do Egito, já se usava características físicas de pessoas para distinguir-las (VIGLIAZZI, 2006).

Existem diversas referências sobre indivíduos sendo identificados por características físicas e parâmetros como cicatrizes, critérios de mensuração física ou a combinação de características mais complexas como cor dos olhos, altura e assim por diante. Estas seriam freqüentemente utilizadas no setor de agricultura onde grãos e provisões seriam estocados em uma central de reposições e aguardavam por movimentações futuras após identificação dos proprietários. Com certeza eles não estavam lidando com um número de indivíduos que se lida hoje, mas os princípios básicos são similares (PINHEIRO, 2008).

Os governantes chineses no século II a.C. já usavam as impressões digitais para lacrar documentos importantes. Na dinastia Tang (618-907 d.C.) estas impressões eram grafadas em placas de barro para confirmar a identidade do indivíduo em transações comerciais, sendo um dos primeiros registros históricos onde esta técnica identificou positivamente uma pessoa. Desde então a impressão digital evoluiu e passou a ser empregada em grandes escala, tornando-se o principal método para comprovar de forma inegável a identidade de uma pessoa. Mas somente mais tarde, no final do século XIX, o sistema de impressão digital criado pelo britânico William James Herschel, baseado nos trabalhos do antropólogo inglês Francis Galton, provou cientificamente que as impressões digitais não mudam no curso da vida de um indivíduo e nenhuma digital é exatamente igual à outra (PINHEIRO, 2008).

Neste período houve um pico de interesse em pesquisas criminalísticas na tentativa de relacionar características físicas com tendências criminais, passando a ser utilizadas para trabalhos de cunho judicial. Isto resultou em uma variedade de dispositivos para mensuração sendo produzidos e muitas informações sendo coletadas (PINHEIRO, 2008).

A partir do século XX, a biometria passou a ser usada em documentos de identidade, como é o caso do RG (Registro Geral) no Brasil.

Hoje em dia, os recursos tecnológicos permitem uma grande evolução em relação às técnicas de biometria passíveis de utilização, pois as novas ferramentas de captura, armazenamento e comparação possibilitam o desenvolvimento e aplicação de novas técnicas biométricas.

1.2 Sistema biométrico

Atualmente os agentes motivadores para desenvolvimento dos sistemas biométricos é o aumento de tentativa de fraudes nos mais diversos tipos de transações eletrônicas. Para combater estas tentativas, procuram-se mecanismos que diminuam os riscos. Os sistemas biométricos podem reduzir consideravelmente os problemas relacionados com a segurança, principalmente com o objetivo de resolver dois deles: a identificação e o acesso de usuários aos sistemas computacionais (PINHEIRO, 2008).

Na identificação de seres humanos pode-se utilizar características corporais únicas como: impressões digitais, traços faciais, olhos e mãos, e características comportamentais como: fala e assinatura manuscrita, entre outros possíveis de mensuração.

Segundo Pinheiro (2008. p. 44), a biometria, quando utilizada na segurança de um sistema computacional, busca verificar a identidade de um indivíduo através das características únicas desta pessoa, pois

> um sistema biométrico pode ser encarado como um conjunto de hardware e software para o reconhecimento de padrões de propósito específico, que opera através de aquisição automática de uma coleção de informações biométricas do indivíduo, extraindo um modelo a partir dessas informações e comparando esse modelo com um conjunto de outros modelos armazenados em uma base de dados.

No modelo conceitual simples o usuário é previamente registrado (aquisição) e seu perfil biométrico (exemplar) fica armazenado. No momento que o usuário utilizar novamente o sistema, o processo de aquisição obtém os dados biométricos apresentados, assim as características particulares dos dados são extraídas para comparação com o perfil armazenado. Então o processo de comparação decide se os dados apresentados são similares (limiar) ao perfil registrado, confirmando ou não a autenticação do usuário (COSTA, 2007).

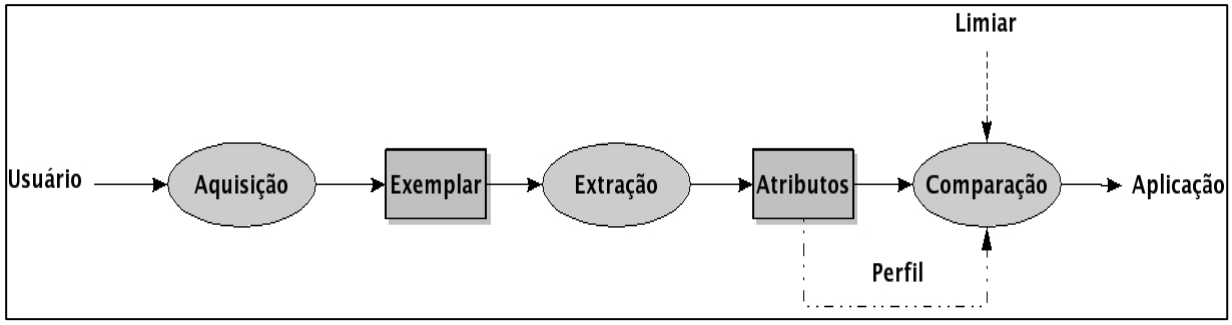

Figura 1.1: Um modelo simples de sistema biométrico.
Fonte: Pinheiro, 2008 p. 44

1.3 Funcionamento do sistema biométrico

O sistema biométrico funciona como ferramenta de identificação e controle. Para atingir este objetivo ele primeiramente faz a aquisição do exemplar e através da utilização de um algoritmo transforma o exemplar em um registro digital da característica física ou comportamental capturada.

1.3.1 Aquisição e exemplar

Aquisição é o processo de obtenção dos dados da característica biométrica apresentada ao sistema (COSTA, 2007). Os dispositivos de aquisição obtêm os dados através de sensores especiais junto com um software que converte esta informação em um modelo digital.

Neste processo a dificuldade é ajustar a qualidade da amostra sem causar incômodo ao indivíduo, por este motivo é adicionado um controle de qualidade de amostra chamado de pré-processamento. O exemplar é o resultado do processo de aquisição (PINHEIRO, 2008).

1.3.2 Atributos e extração de características

O processo de extração produz uma representação digital do exemplar, chamado de atributo, característica ou *template* (COSTA, 2007). Este atributo é associado ao identificador do usuário do sistema o qual será utilizado.

A extração é efetuada por um algoritmo que tem a função de filtrar e compactar as características relevantes do exemplar adquirido, com a finalidade de redução do volume de dados sem comprometimento da qualidade. Após este processo é estabelecido o modelo representativo do registro para armazenamento em banco de dados.

1.3.3 Registro e perfil

O processo de registro é resultado da extração de características dos dados biométricos do indivíduo (*template*) para cadastramento no sistema. Embora o processo seja realizado apenas uma única vez, este perfil obtido e armazenado é de fundamental importância para futuras comparações. A linha pontilhada na figura 1.1 significa que o processo de registro, embora realizado raramente, é necessário para o estabelecimento do perfil para posterior comparação (COSTA, 2007).

1.3.4 Comparação, limiar e decisão

O processo de comparação é responsável pela verificação do grau de similaridade entre as características extraídas da amostra e o perfil armazenado. Este processo fornece uma pontuação representativa da similaridade entre os dois conjuntos de dados. Caso o resultado

seja superior a certo limite previamente determinado, conhecido como limiar, a decisão é considerar a autenticação válida, e caso seja inferior ao limiar a decisão é não validar, assim negando o acesso (COSTA, 2007).

Em todos os sistemas de segurança, inclusive no sistema biométrico, existem dois momentos distintos, que se pode chamar um de momento de Registro e outro momento de Verificação. Pois o tipo de operação que se deseja efetuar em determinada circunstância pode afetar a integridade da segurança do sistema.

Defina-se momento de registro como sendo o momento onde o sistema está pronto para receber um novo registro, um novo modelo de característica biométrica que deverá ser armazenado. Este momento é crítico, pois não pode ser vinculado indevidamente um modelo de característica a um usuário que não seja o verdadeiro titular da característica. Neste instante tem de se tomar o maior cuidado para não gerar registro incorreto que pode facilitar futuras fraudes e inconsistências.

No momento de verificação o sistema aguarda um novo exemplar para comparação, não permitindo alteração no banco de dados utilizado no sistema.

Os sistemas de biometria aplicados na segurança têm que ter um gerenciado rígido destes dois momentos para eliminar possíveis fraudes e com isto falta de credibilidade do mesmo.

1.4 Requisitos do sistema biométrico

De acordo com Pinheiro (2008), estes sistemas se baseiam em características intrínsecas do ser humano, e podem ser empregados como métodos de autenticação rápida e com alto nível de precisão, tendo como principais vantagens o fato de serem intransferíveis e não podendo ser perdidos ou roubados. Existem três requisitos básicos para que o sistema de identificação biométrico seja considerado seguro:

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

Qualquer característica, física ou comportamental pode ser utilizada na identificação, desde que satisfaça os seguintes requerimentos:

- **Universalidade** – todos devem possuir a característica a ser utilizada como medida;
- **Singularidade** – a medida da característica não pode ser igual em indivíduos diferentes, ou que a possibilidade seja considerada mínima ou nula;
- **Permanência** – a característica não deve variar com o tempo, alterar com envelhecimento;
- **Mensurabilidade** – poder ser medida quantitativamente, com base num modelo selecionado;

Um sistema de reconhecimento biométrico tem três características importantes quanto ao seu funcionamento:

- **Precisão e Desempenho** – a precisão do sistema deve ser aceitável, mesmo que implique num menor desempenho;
- **Aceitabilidade** – tem que ter aceitação por parte de seus usuários;
- **Proteção** – dificultar que o usuário consiga burlar o sistema;

1.5 Componentes do sistema biométrico

De acordo com Pinheiro (2008), a arquitetura de um sistema biométrico básico pode ser divida em quatro componentes principais:

- **Subsistema Interface de usuário** – conjunto de elementos que contém o dispositivo que capta a amostra biométrica do indivíduo. O desempenho de todo o sistema é afetado pela qualidade da amostra adquirida pelo dispositivo de coleta e varia de acordo com a tecnologia biométrica aplicada;
- **Subsistema Estação de Controle** – responsável pelas funções de controle dos dispositivos e por receber as amostras biométricas fornecidas pela interface de usuário. Neste subsistema também é realizado o processo de análise da qualidade da amostra, assim como de filtrar e remover ruídos e imperfeições que possam afetar o processo de comparação;

- **Subsistema Comparador** – esta etapa faz a comparação da amostra biométrica apresentada com o *template* da base de dados. Este subsistema tem a função de decidir se a amostra é válida ou não, de acordo com valores de semelhança pré-estabelecidos, e comunicar os demais subsistemas sobre os resultados obtidos;
- **Subsistema de Armazenamento** – este subsistema armazena os *templates* dos usuários cadastrado no sistema, permitindo sempre que necessário a atualização desta base de dados. Dependendo da finalidade e do tamanho dos *templates*, estes podem ser armazenados em diferentes dispositivos de armazenagem como cartões magnéticos, *Smart Cards, tokens*, HD, etc.

O tamanho do modelo numérico criado pelo sistema biométrico depende da precisão exigida para a segurança, pois quanto maior a precisão maior será o tamanho da chave. Mas é possível criar sistemas biométricos com chaves muito pequenas. Um padrão de retina pode ser armazenado em 35 bytes, face em 84 bytes e a impressão digital e íris ocupam de 256 a 512 bytes, enquanto a geometria da mão ocupa 9 bytes (Pinheiro, 2008).

Neste primeiro capítulo foi apresentado o conceito e um breve histórico da biometria. Também se descrevem as características e componentes básicos dos sistemas biométricos. O objetivo é de demonstrar que ao contrário de que muitos pensam a biometria não é algo novo e sim a continuidade de estudos de nossos ancestrais.

No próximo capítulo serão detalhados os tipos de sistema biométricos mais conhecidos.

2 TIPOS DE SISTEMAS BIOMÉTRICOS

As características biométricas do indivíduo possibilitam as mais diversas técnicas de identificação, pois o ser humano tem características físicas e comportamentais passíveis de medição. Os sistemas biométricos se dividem de acordo com os tipos de características escolhidas para medição. Os tipos normalmente utilizados para identificação de seres humanos são (VIGLIAZZI, 2006):

- **Impressão digital** – é uma das formas de identificação mais usadas, que consiste na captura da formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa;
- **Veias da palma da mão** – é baseado no desenho formado pelas veias da mão;
- **Reconhecimento facial** – é o sistema mais utilizado para os seres humanos se reconhecerem entre si;
- **Íris** – é baseada na leitura dos anéis coloridos existentes em torno da pupila;
- **Retina** – identificação através dos vasos da retina. É uma forma muito segura, pois são únicas em cada olho e com uma dificuldade muito grande de modificação e duplicação;
- **Geometria das mãos e dedos** – é baseado nas medidas das mãos, como forma, tamanho da palma, comprimento e largura dos dedos;
- **Reconhecimento de voz** – é a combinação de biometrias comportamental e fisiológica. Pois as características se baseiam nas formas e tamanho das cordas vocais, da boca, dos lábios, da cavidade nasal, ou seja, nos órgãos usados na síntese do som;
- **Dinâmica de digitação** – é a medida da velocidade de digitação;

- **Assinatura** – é a forma de assinar de um indivíduo revela sua identidade e vem sendo muito bem aceita nas transações legais e comerciais;
- **DNA** – possui característica biométrica única para cada indivíduo, por isto é muito utilizado em aplicações forenses;
- **Termogramas de face, mãos e veias da mão** – esta técnica de identificação utiliza o calor emitido pelo corpo, contudo, a captura de termogramas em ambientes não controlados é muito complexa.

Muitos são os tipos de biometrias existentes, pois tudo que for mensurável em termos de vida é passível de se tornar uma técnica viável de sistema biométrico. Mas o objetivo deste trabalho é apresentar os métodos aplicáveis na segurança das transações bancárias. Dentro deste contesto, não serão apresentados os estudos sobre as técnicas de reconhecimento por DNA e por Termogramas. O DNA por ter baixa aceitação e ter sua principal aplicação na área forense, e o termograma por não ser recomendado para ambientes não controlados.

Nas próximas seções serão apresentadas as outras técnicas que demonstram mais aptidão para serem aplicadas na solução que será apresentada por este trabalho.

2.1 Reconhecimento da impressão digital

A impressão digital é a representação da epiderme do dedo, formada por um conjunto de linhas que fluem frequentemente paralelas e produzem singularidades locais. Estas linhas possuem micro-singularidades que são chamadas de minúcias, que são determinadas essencialmente pela terminação ou pela bifurcação das linhas do cume. As minúcias que combinam, constituem a base da maioria dos algoritmos para comparação da impressão digital (VIGLIAZZI, 2006).

2.1.1 Características da impressão digital

A impressão digital é o desenho formado por vales e cristas na ponta dos dedos. Sendo formada ainda no feto, muda muito pouco com a idade e não é a mesma nem para gêmeos. Este desenho formado pela impressão digital possui pontos característicos que permitem a sua identificação (CANEDO, 2003).

Vigliazzi (2006) cita as características típicas da impressão digital:

- **Linhas de Cume**: a linha da impressão digital que é comparada com uma montanha;
- **Vale**: é o espaço entre os cumes;
- **Ponto de União**: o ponto onde dois cumes se unem;
- **Núcleo Superior**: o lugar onde a dobra do cume ascendente é maior;
- **Bifurcação**: o ponto aonde um cume divide-se;
- **Núcleo Inferior**: o lugar onde a dobra do cume é maior, o fluxo do cume gira em torno do centro completamente;
- **Delta**: o ponto onde o fluxo do cume divide-se em três direções;

2.1.2 Método de captura de impressão digital

Os dois métodos para se capturar uma impressão digital: o de tinta no papel (*ink in paper*) e por leitores de IDs. O primeiro método o dedo é colocado em tinta e depois pressionado e rolado em um papel para que seja posteriormente escaneado (TESDECO, 2003). Este método não oferece uma boa qualidade de imagem, por este motivo está sendo muito pouco utilizado, e não é passível de utilização na proposta deste trabalho.

A ilustração (figura 2.1) mostra a diferença entre uma ID adquirida pelo método tinta no papel e pelo leitor. A diferença da qualidade do exemplar adquirido compromete a eficácia do método de captura através de tinta no papel.

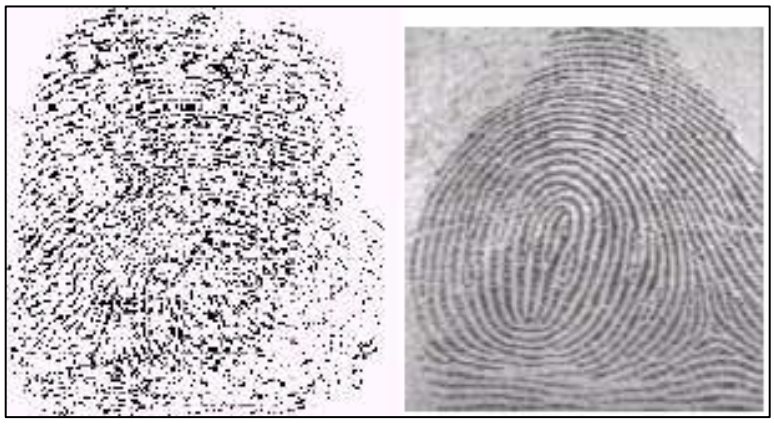

Figura 2.1: Impressão tinta no papel (esq.) e a impressão adquirida em um leitor (dir.).
Fonte: Tedesco, 2003 p. 3

O segundo método, por leitores de IDs (figura 2.2), utiliza um sistema eletrônico de geração de dados, e por esta razão é muito mais eficiente. O leitor biométrico captura a imagem dos os aspectos físicos extraídos da impressão digital, ser processado pelo algoritmo.

Figura 2.2: Leitor ótico de impressão digital.
Fonte: Siemens, 2009

Existem diferentes tipos de leitores de ID, Canedo (2003) em seu trabalho apresenta alguns destes tipos e como eles funcionam:

- **Leitor Ótico:** o dedo é colocado sobre uma das faces de um prisma a luz e projetada de outra face e na terceira face uma câmera capta a imagem, as partes do dedo em contato com o vidro causam uma alta diferença de contraste que é detectada pela câmera. Um sistema de lentes para correção de imagem é necessário;
- **Leitor Emissor de luz:** as papilas do dedo entram em contato com uma pequena camada de um material especial que com o contato emite uma pequena quantidade de fótons que são detectados por um sensor CMOS localizado logo a baixo;
- **Leitor Térmico:** possui sensores térmicos que detectam o contato das papilas;
- **Leitor eletroluminescente:** possui fina camada de material eletroluminescente que é excitado com o contato das papilas, a camada de sensores detecta esta luz;
- **Leitor Capacitivo:** é formado de pequenos capacitores que são descarregados e seu nível de carga são medidos pelos circuitos lógicos e enviado para um conversor Analógico para Digital que transforma essa informação em nível de cinza.

Para que o processo de comparação de IDs seja considerado confiável, normalmente se faz necessária a execução de etapas preliminares para o tratamento das IDs. Estas etapas iniciais podem envolver técnicas como binarização, afinamento, remoção de ruídos, filtros, detecção de bordas, entre outros métodos existentes.

O processo de binarização significa transformar imagens em tons de cinza em imagens binárias e o afinamento é algoritmo que remove todos os *pixels* redundantes das imagens de IDs produzindo uma nova imagem simplificada com largura de um único *pixel*, formando um esqueleto do ID (figura 2.3).

Figura 2.3: Impressão Digital: à esquerda sem o afinamento e à direita com o afinamento.
Fonte: Tesdeco, 2003 p. 7

Identificando-se as minúcias características da ID então é formado o grafo representando em uma lista de adjacência onde o centróide é ligado as n minúcias mais próximas (figura 2.4).

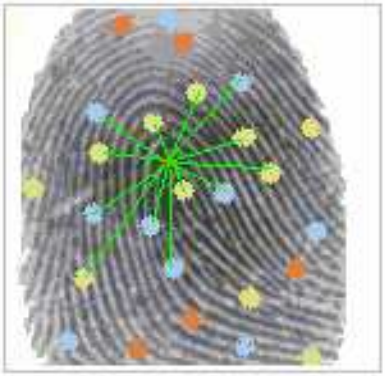

Figura 2.4: As minúcias e o centróide sobreposto à imagem da Impressão Digital.
Fonte: Tedesco, 2003 p. 8

Este tratamento é o processo de extração descrito por Tedesco (2003), que tem o objetivo de gera um grafo (perfil) a ser armazenado, ou o atributo a ser comparado com o perfil já armazenado no banco de dados. A finalidade é melhorar o desempenho da identificação através de ID quando apresentados com algum grau de rotação.

Existem diferentes tipos de algoritmos de reconhecimento de ID, que apresentam desempenhos variados, o importante é que o tipo de equipamento e software escolhido demonstre a resposta esperada para solução do problema.

2.1.3 Sistema automatizado de identificação de impressões digitais (AFIS)

De acordo com Pinheiro (2008) o sistema automatizado de identificação de impressões digitais (*Automated Fingerprint Identification System* - AFIS) é um sistema que visa garantir a unicidade da identificação de um indivíduo, trazendo agilidade ao processo de identificação através do mapeamento de impressões digitais. Esta tecnologia é capaz de identificar um único indivíduo a partir de um banco de dados contendo milhões de indivíduos que usam de uma até dez impressões digitais.

> A AFIS pode ser considerado um tipo diferenciado de tecnologia biométrica pela impressão digital. Trata-se de uma tecnologia muito madura e de eficiência comprovada, que opera em ambientes estritamente definidos. Entretanto, enquanto a maioria dos sistemas biométricos provê verificação e identificação em segundos, os sistemas AFIS podem levar minutos, horas, até mesmos dias para efetivar uma comparação, dependendo do tamanho do banco de dados biométrico consultado (Pinheiro, 2008 p.157).

Os sistemas seguem o princípio biométrico básico, o qual envolve o processamento da característica adquirida pelo leitor, geração do modelo e comparação com banco de dados, o desafio é assegurar que todos os registros adquiridos pelo sistema sejam robustos para permitir a comparação contra milhões de indivíduos cadastrados.

2.2 Reconhecimento através das veias da palma da mão

As veias da palma da mão permitem uma forma extremamente segura de autenticação da identidade do indivíduo, pois como trata de uma técnica baseada em uma característica interna do corpo dificulta a falsificação (VIGLIAZZI, 2006).

Pode-se afirmar que é um sistema biométrico muito higiênico, pois não há necessidade de contato direto com dispositivo de captura, o que facilita a sua utilização em locais públicos.

2.2.1 Características das veias da palma da mão

Os padrões das veias da palma da mão são muito consistentes para a identificação. Cada mão possui um padrão único e não se alteram com a idade nem com trabalho pesado.

As características originadas das veias da palma são únicas, segundo o fabricante Fujitsu (2005). Pois como se observa na figura 2.5, a imagem capturada das veias apresenta diversas minúcias que serão utilizadas para definição do perfil da característica do usuário.

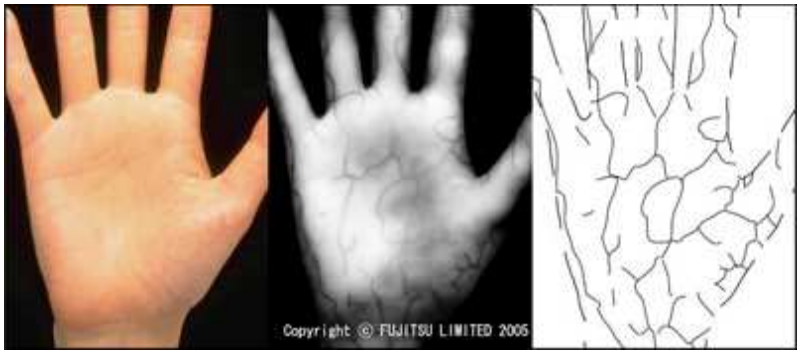

Figura 2.5: Tecnologia da autenticação da veia da palma da Fujitsu.
Fonte: Fujitsu, 2009

Como vantagem da utilização destes padrões vasculares da mão, pode-se citar as seguintes características (VIGLIAZZI, 2006):

- **Singularidade –** mesmo em gêmeos as mãos direita e esquerda são diferentes;
- **Estabilidade –** não ocorrem mudanças por longos períodos;
- **Independência de contaminações e cicatrizes ou outros fatores externos –** não há alteração das características ocasionada por pequenas lesões.

2.2.2 Método de captura das veias da palma da mão

No método de captura das características biométricas das veias é utilizado um pequeno leitor (figura 2.6) fácil e rápido de usar. Coloca-se a mão a poucos centímetros do mesmo para que este faça a leitura do padrão. Não é necessário contato com o mesmo e em

menos de meio segundo está feita à captura do exemplar para registro ou comparação. O sistema minimiza desse modo à resistência psicológica quanto a sua utilização por falta de higiene, fato que ocorre quando vários indivíduos tocam no mesmo dispositivo. A autenticação da veia da palma é segura, já que somente uma quantidade mínima de luz infravermelha utilizada para ler padrão de característica das veias (FUJITSU, 2009).

Figura 2.6: Imagem do leitor de veias da palma da mão da Fujitsu - Palm Secure.
Fonte: Fujitsu, 2008

A Sony diz que seu leitor para autenticação através das veias é uma tecnologia superior a outras soluções biométricas, na medida em que produz resultados mais precisos e rápidos do que métodos como a leitura de impressões digitais ou da retina. Segundo a empresa, a falsa rejeição do sistema é inferior a 0,1 por cento, e o tempo de processamento para a autenticação produzir efeito é de apenas 0,015 segundos usando um computador (PORTAL DA SEGURANÇA, 2009). Esta velocidade e desempenho deste sistema, o torna uma ferramenta muito interessante na aplicação de identificação de indivíduos.

2.3 Reconhecimento facial

O reconhecimento facial, de acordo com Vigliazzi (2006), é fácil se as imagens apresentadas estiverem processadas e tratadas especialmente, de forma que a face ocupe a imagem inteira, sem ser obstruída por outros objetos e sem nenhuma desordem adicional do fundo que possa confundir o algoritmo de reconhecimento. Entretanto, sob a maioria das circunstâncias, tais condições não se aplicam.

As imagens capturadas em câmeras normalmente são mais amplas que os rostos a serem reconhecidos. Para que seja possível reconhecer a face primeiramente o sistema deve eliminar todos os objetos adicionais e assim obter a imagem isolada da face.

Para reconhecer o rosto de uma pessoa, os programas mapeiam a geometria e as proporções da face. Através de registros de vários pontos delimitadores na face, os quais permitem estabelecer proporções, distâncias e formas de cada elemento do rosto, o software com base nesses dados pode iniciar as comparações.

2.3.1 Características do reconhecimento facial

A técnica de reconhecimento facial tem como pontos principais: os olhos, nariz, queixo, maçãs do rosto, orelhas, lábios, etc. Com o objetivo de diminuir margens de erro devem ser utilizadas as medidas do rosto que nunca se alteram, mesmo após cirurgias plásticas. Estas medidas básicas são (figura 2.7):

- Distância entre os olhos;
- Distância entre boca, nariz e os olhos;
- Distância entre olhos, queixo, boca e linha dos cabelos.

Vigliazzi (2006) relata que a tecnologia de reconhecimento facial está bastante acessível e tem uma grande variedade de aplicações. Atribui como vantagem deste sistema a necessidade da maioria dos usuários de precisar comprar apenas o Software que executa o reconhecimento, sem ter que adquirir novos equipamentos.

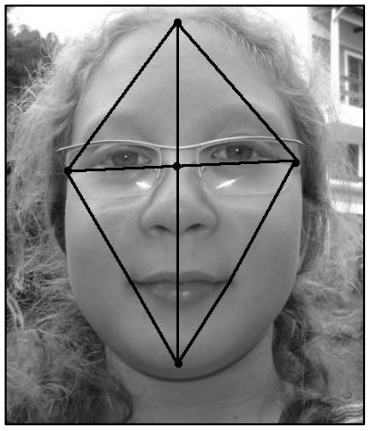

Figura 2.7: Imagem face capturada.
Fonte: Ribeiro, 2008 p. 40

2.3.2 Método de captura das faces

Os sistemas de reconhecimento facial, conforme descreve Pinheiro (2008), funcionam a partir da captura da imagem da face do indivíduo através de uma câmera ou máquina fotográfica.

Segundo Vigliazzi (2006) a captura da imagem pode ser colorida ou monocromática, pois para um reconhecimento eficiente ela é convertida para monocromática, todo o brilho é removido e então iniciado o processo de centralização dos pontos do rosto.

Quando pronta à centralização, o sistema identifica os pontos e marca os elementos da face. A partir destes elementos é criado o *template* para armazenamento ou para comparação com o banco de dados.

2.4 Reconhecimento de íris

De acordo com o livro de Pinheiro (2008), a íris é a parte colorida do olho, em torno da pupila, e permite 249 pontos de diferenciação que podem ser utilizados no processo de reconhecimento. As características da íris não se alteram com envelhecimento do indivíduo, portanto pode ser considerada uma identificação biométrica estável. A probabilidade de danos à íris é mínima, pois a mesma está protegida pela córnea.

2.4.1 Características do reconhecimento de íris

Conforme Vigliazzi (2006) descreve em seu livro, a íris tem muitas características que podem ser usadas para distinguir os indivíduos. Uma dessas características é o tecido que parece dividir a íris em uma forma radial. Estas características são estabelecidas de forma permanente no oitavo mês da gestação. Devido à inexistência de influência genética até mesmo os gêmeos idênticos tem íris diferentes.

A íris do olho humano possui uma imagem muito complexa e por esse motivo é, teoricamente, única (VIGLIAZZI, 2006). Alguns autores afirmam que esta tecnologia é uma das mais seguras que existe.

O processo de reconhecimento da íris tem um excelente desempenho, pois a codificação, comparação e tomada de decisão são processadas digitalmente, diminuindo o

tempo de resposta da identificação. Mas este grau de precisão traz uma desvantagem, como explica Pinheiro (2008. p. 69), a íris não é um alvo fácil.

> Portanto, exige a colaboração do usuário para a sua coleta. Embora seja uma boa técnica para identificação, o desenvolvimento em larga escala é impedido por falta de base instalada.

2.4.2 Método de captura da íris

A captura da imagem da íris é feita através da uma câmera (figura 2.8), usando a luz visível e infravermelha. Para que seja possível a captura da característica da íris, o indivíduo deve estar dentro do campo de visão da câmera.

Figura 2.8: Câmera de alta resolução.
Fonte: LG, 2009

Conforme Pinheiro (2008) o processo de reconhecimento da íris pode ser dividido em três etapas. A primeira etapa é a aquisição da imagem da íris na imagem capturada; a segunda é aplicação do algoritmo de extração que isola o padrão da íris da pupila (figura 2.9); a terceira é o processo de extração das características para gerar o *Iriscode* (figura 2.10).

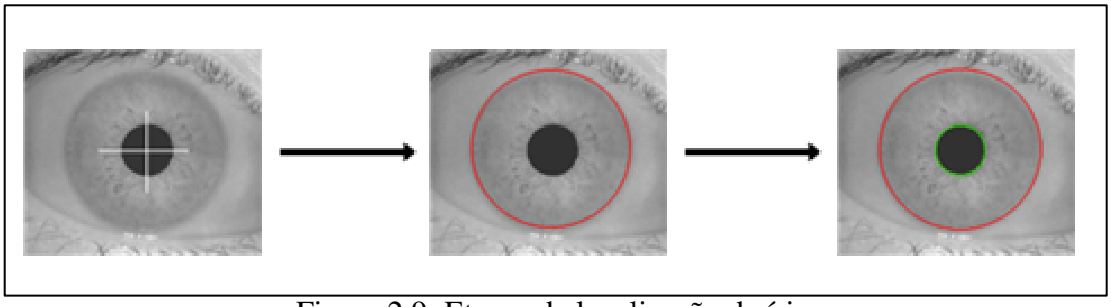

Figura 2.9: Etapas da localização da íris.
Fonte: Íris 1.0, 2007

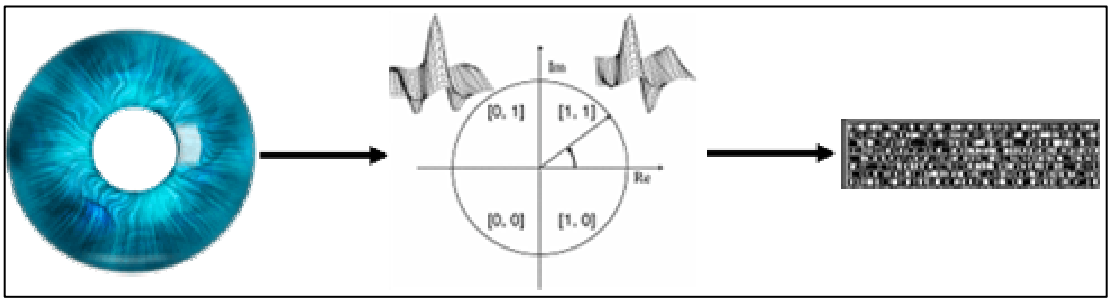

Figura 2.10: Etapas da extração de características.
Fonte: Íris 1.0, 2007

O *iriscode* é o registro a ser armazenado no banco de dados ou o exemplar a ser comparado com o registro do banco de dados.

2.5 Reconhecimento da retina

O reconhecimento da retina é um processo que utiliza as características dos vasos sanguíneos encontrados na retina do olho, ou seja, na membrana mais interna do globo ocular. Os vasos desta membrana formam padrões únicos o que possibilita uma identificação precisa do indivíduo (PINHEIRO, 2008).

2.5.1 Características do reconhecimento da retina

Inúmeras pesquisas têm comprovado que o padrão de vasos da retina (figura 2.11) é a característica com maior garantia de singularidade que um indivíduo pode possuir (VIGLIAZZI, 2006).

O alto grau de precisão deste método o torna uma das mais seguras técnicas de identificação biométrica. As desvantagens deste método são: como sugere Pinheiro (2008), a dificuldade da captura dessa imagem, pois o processo exige que se olhe fixamente para um ponto de luz de infravermelho até que a câmera focalize os padrões e os capture; outro o alto custo de implementação.

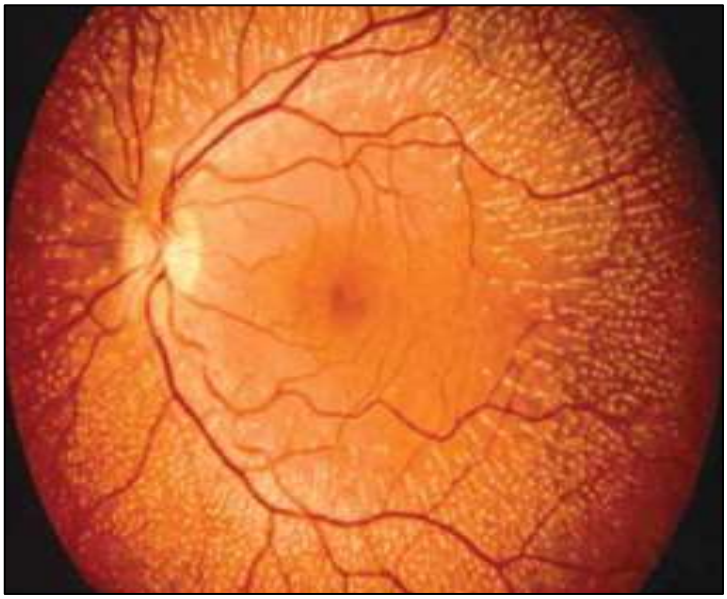

Figura 2.11: Retina do olho.
Fonte: Ribeiro, 2008 p. 55

2.5.2 Método de captura da retina

O processo de captura da imagem da retina (figura 2.11) é efetuado por um *scanner* de retina (figura 2.12) o qual utiliza um laser de baixa intensidade para medir os padrões dos vasos sanguíneos da retina. Inicialmente delimitando a região central do olho, a pupila, definindo quais são os pontos importantes para a identificação.

Figura 2.12: Analisador de retina.
Fonte: Ribeiro, 2008 p. 55

Após definir o tamanho do anel que limita o comprimento padrão para medição dos vasos, o sistema faz o mapeamento completo das características e a área da retina é delineada o que permitirá gerar um exemplar único para identificação do indivíduo.

2.6 Reconhecimento da geometria da mão

A autenticação da identidade do indivíduo neste método é feita através da forma geométrica de sua mão. Para efetuar este reconhecimento são utilizadas características físicas da mão.

2.6.1 Características do reconhecimento da geometria da mão

Dentre as mais de 90 medições que esta tecnologia leva em conta no processo de identificação (VIGLIAZZI, 2006). As principais características são (COSTA, 2007):

- Comprimento;
- Largura;
- Espessura;
- Curvatura;
- Localização relativa destas características.

Este sistema apresenta baixo custo de implementação e o *template* adquirido após a aplicação do algoritmo fica reduzido a apenas 9 bytes, possibilitando o armazenamento do padrão biométrico em qualquer tipo de cartão disponível. Entretanto, esta tecnologia é menos confiável devido às características não serem suficientemente descritivas para precisa identificação do indivíduo (PINEIRO, 2008).

2.6.2 Método de captura da geometria da mão

O sistema de captura da imagem para reconhecimento da geometria da mão é composto por uma fonte clara, uma câmera, um único espelho e uma superfície com cinco pinos. Estes cinco pinos servem como pontos de controle para colocação apropriada da mão direita do usuário (COSTA, 2007).

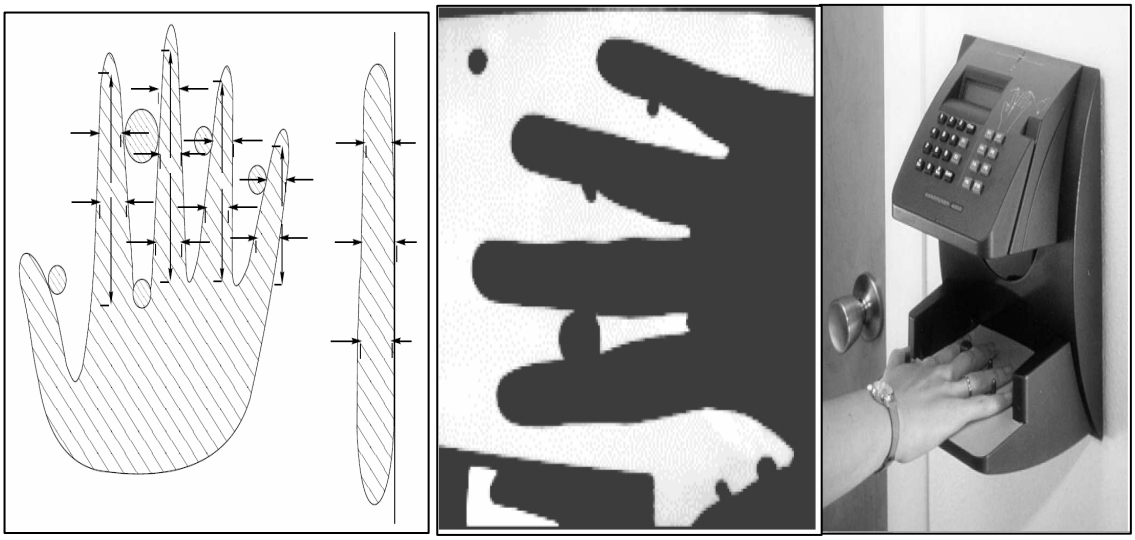

Figura 2.13: Modelo esquemático (esq.), a imagem real (centro), dispositivo (dir.).
Fonte: Ribeiro, 2008 p. 49

Com a colocação da mão no leitor, começa o processo de captura da imagem. O algoritmo usa a imagem capturada para efetuar a extração das medidas das larguras e dos comprimentos dos dedos em várias posições, assim definindo o vetor de características da mão do indivíduo (VIGLIAZZI, 2006). O sistema calcula e registra as proporções destas medidas as quais são decisivas na identificação da pessoa, gerando o *template* a ser armazenado ou comparado com o banco de dados.

2.7 Reconhecimento da voz

O reconhecimento de voz, conforme descreve Pinheiro (2008), é uma tecnologia que analisa os padrões harmônicos e não apenas reproduções de seqüências predefinidas de voz. Segundo Vigliazzi (2006. p. 39), a técnica de identificação por voz é atrativa porque prevalece na comunicação humana.

> Nós esperamos, ao atender o telefone, ser capazes de reconhecer alguém pela voz após ouvir algumas palavras, pois o cérebro humano é muito bom para explorar o contexto e verificar as possibilidades.

Esta técnica de reconhecimento é vulnerável, pois a interferência de ruídos e o estado emocional do indivíduo podem impedir sua precisão. Por este motivo deve ser observado o tipo de ambiente onde será utilizada esta ferramenta, a fim de evitar problemas com seu desempenho e eficácia.

2.7.1 Características do reconhecimento da voz

Os sistemas de reconhecimento de voz podem ser divididos em classes, conforme o protocolo estabelecido:

- **Texto fixo –** o indivíduo pronuncia uma palavra ou frase preestabelecida, gravada durante a fase de registro;
- **Dependente do texto –** o sistema solicita ao indivíduo que pronuncie algo específico, dentre as diversas opções previamente registradas;
- **Independente do texto –** o indivíduo pronuncia qualquer frase que desejar;
- **Conversacional –** o indivíduo é interrogado pelo sistema, tornando-se um protocolo misto de conhecimento de códigos e biometria, pois as frases têm certo grau de segredo.

Conforme Vigliazzi (2006), a fala tem características específicas devido às diferenças em aspectos físicos e comportamentais do sistema de produção da fala nos seres humanos. O principal aspecto físico deste sistema é a forma do intervalo vocal, este intervalo modifica o índice espectral de uma onda acústica enquanto passa através dele, produzindo a fala. Nos sistemas de verificação de voz é comum a utilização das características derivadas somente do intervalo vocal.

2.7.2 Método de captura da voz

O método necessita de um dispositivo como microfone ou telefone para aquisição da característica biométrica do usuário. Para realizar esta aquisição o usuário deve pronunciar uma palavra ou frase para iniciar o processo de reconhecimento.

O sistema baseado nesta captura e no processamento digital do áudio falado, então utiliza um algoritmo que segmenta este áudio em pequenos pedaços conhecidos com fonemas. A partir destas informações adquiridas o sistema gera o padrão biométrico que será armazenado ou comparado com banco de dados.

2.8 Reconhecimento da dinâmica de digitação

A técnica biométrica da dinâmica da digitação é baseada no comportamento do ser humano ao digitar um texto em um teclado. Apesar de ser uma técnica de baixo custo, pois não necessita de um equipamento especial, e parecer um método inseguro, é adotada por muitas redes corporativas de forma natural por ser transparente para o usuário (VIGLIAZZI, 2006).

2.8.1 Características do reconhecimento da dinâmica de digitação

Existem várias maneiras de medir a dinâmica da digitação quando os usuários digitam em um teclado de computador:

- **O intervalo** de tempo entre o pressionamento de teclas consecutivas;
- **O tempo** que uma tecla fica pressionada; o tempo total da digitação;
- **A freqüência** da digitação de teclas erradas;
- **O hábito** de usar teclas diferentes do teclado.

Alguns estudos indicam esta técnica para autenticação de usuários em aplicações da internet, pois suas características e o baixo custo demonstram a possibilidade de criar um segurança adicional nas operações efetuadas pela rede.

2.8.2 Método de captura da dinâmica de digitação

O processo de captura desta técnica é simples, pois é baseada na operação mais básica do usuário em um computador, a digitação. Normalmente o padrão é capturado no momento de digitação da identificação do usuário no sistema, pois conforme cita Pinheiro (2008), o sistema autentica o acesso segundo uma análise da forma como a pessoa digita seu nome e senha.

2.9 Reconhecimento da assinatura manuscrita

A técnica de reconhecimento da assinatura manuscrita é a forma mais utilizada para confirmar a identidade de uma pessoa em documentos, pois para validar estes documentos

basta assiná-los. A sociedade aceita a assinatura pessoal como forma de identificação e autorização de um indivíduo (Pinheiro, 2008).

2.9.1 Características do reconhecimento da assinatura manuscrita

O reconhecimento da assinatura é um método de autenticação baseado em uma biometria comportamental, devido ao fato de que assinar é uma ação de reflexo, não influenciada pelo controle muscular deliberado. Por este motivo ao analisar a maneira como o indivíduo faz a sua assinatura pode-se confirmar sua identidade (Pinheiro, 2008).

A assinatura manuscrita apresenta características que permite a identificação como exemplo:

- Velocidade da escrita;
- Pontos de Pressão;
- Inclinação das letras;
- Espaçamento entre as letras;
- Ritmo;
- Toques sucessivos na superfície do papel;
- Aceleração.

O sucesso deste método de identificação depende de encontrar as características na assinatura que sejam mais constantes, isto é, que variem pouco durante o processo de cadastramento e autenticação.

2.9.2 Método de captura da assinatura manuscrita

Segundo Pinheiro (2008), os sistemas atuais estão baseados em dois tipos: Sistemas Dinâmicos e Sistemas Estáticos. Estes tipos se diferenciam pela forma de captura da característica biométrica.

No sistema dinâmico a assinatura é efetuada num dispositivo eletrônico (figura 2.14) preparado para sua captura, que apresenta alto grau de resolução, assim as características

dinâmicas temporais da assinatura, como a trajetória da caneta, a pressão, direção e elevação do traço, podem ser observadas.

Figura 2.14: Exemplo de um dispositivo para captura dinâmica.
Fonte: Lago, 2005 p. 7

No sistema estático a assinatura é impostada em documentos de papel, escrita por meio convencional e posteriormente adquirida por meio de uma câmera ou scanner. Após a captura da imagem é efetuado o processo de extração das características da assinatura.

Para melhor desempenho do sistema estático é necessário o pré-processamento da imagem adquirida. Este pré-processamento consiste nos métodos de solarização, realce de imagens e limiarização.

A solarização é aplicada para tentar eliminar o ruído incutido no fundo da imagem da assinatura, tentando, juntamente com o realce, destacar somente o traço da assinatura (LAGO, 2005). Este algoritmo aplica um nível de luminosidade a cada *pixel* da imagem. Assim, apenas o traço da assinatura, que é o predominante na imagem, resta, como pode ser observado (figura 2.15).

Figura 2.15: Imagem obtida e sua correspondente solarizada.
Fonte: Lago, 2005 p. 8

Segundo Lago (2005), o realce da imagem é um processo subseqüente ao de solarização e visa restaurar o traço após a eliminação do ruído pela técnica de solarização (figura 2.16).

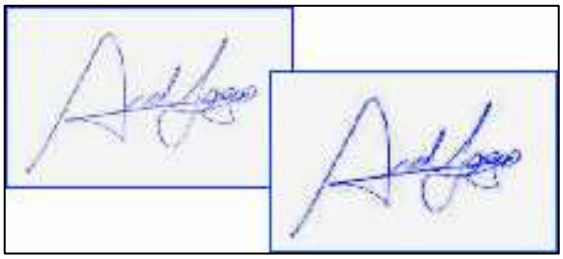

Figura 2.16: Imagem solarizada e sua correspondente, depois da técnica de realce.
Fonte: Lago, 2005 p. 9

Observe que a imagem final na figura 2.16 (direita), parece pior se comparada com a imagem na figura 2.15 (esquerda), mas isto está correto, porque a finalidade do processo é justamente valorizar as características relevantes da assinatura.

O método de limiarização, também conhecido como alargamento de contraste, consiste na aplicação de uma função que clareia os valores acima de um valor padrão e escurece valores abaixo deste. Somente após a aplicação deste algoritmo é que se podem extrair os dados da imagem para armazenamento ou comparação (LAGO, 2005).

Este segundo capítulo apresenta os diversos tipos de sistemas biométricos, com objetivo de demonstrar as características de cada técnica e os métodos que estas utilizam para extrair os dados biométricos dos usuários.

O estudo dos diversos tipos de técnicas é necessário para correta escolha do sistema biométrico, que deverá aumentar a segurança nas transações bancárias. Continuando nesta busca, o próximo capítulo mostra as ferramentas de segurança existentes.

3 SEGURANÇA NO SISTEMA BANCÁRIO

A segurança pode ser definida como a condição de estar protegido de perigo ou perda. A sensação de estar seguro é fundamental para se estabelecer uma relação de confiança. Pode-se definir que dar crédito é confiar em alguém.

O mundo dos negócios só funciona porque existe o crédito, as troca de mercadorias e as transações financeiras só ocorrem porque foi estabelecida uma relação de confiança entre as partes envolvidas.

No sistema financeiro um dos maiores valores que uma organização pode ter é a credibilidade, pois para que uma empresa se consolide neste mercado ela precisa transmitir muita confiança aos seus clientes. Os bancos precisam demonstrar que estão continuamente aperfeiçoando seus produtos e sistemas, com a finalidade de assegurar os negócios de seus clientes.

Nos momentos de crise, como a que se apresentou em meados de 2008, há necessidade das instituições financeiras de reafirmar seus valores se amplia, pois a aversão ao risco de qualquer natureza aumenta. A busca por informações precisas e decisões corretas passa a ser de fundamental importância para superação destes momentos de adversidade. Por este motivo a segurança da informação torna-se fator crítico.

3.1 Segurança da informação

A segurança da informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas

computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados.

A segurança da informação para Pinheiro (2008, p. 7),

> Trata-se do processo de proteger a informação de uma corporação dos diversos tipos de ameaças externas e internas, visando garantir a continuidade dos negócios, minimizar os prejuízos que podem advir, maximizar o retorno do investimento e aumentar as oportunidades de novos negócios.

Para os bancos as informações armazenadas em seus bancos de dados são um dos principais patrimônios que as empresas desde ramo podem ter, pois a dependência desta base de dados é tão grande, ao ponto de afirmar que a perda destas informações causaria o fim de suas atividades.

Com o objetivo de evitar qualquer dano a este patrimônio, os bancos investem anualmente verdadeiras fortunas em tecnologia da informação. Parte deste investimento é direcionado para pesquisa de soluções inovadoras as quais colocam os bancos na vanguarda tecnológica do mundo. Para atingir este objetivo deve-se estabelecer uma política de segurança da informação, a qual será a tradução das expectativas da empresa em relação à segurança.

Conforme Pinheiro (2008, p. 9) escreve em seu livro,

> a política de segurança da informação é um conjunto de diretrizes, normas, procedimentos e instruções, destinadas respectivamente aos níveis estratégico, tático e operacional, com o objetivo de estabelecer, padronizar e normatizar a segurança tanto no escopo humano como no tecnológico.

3.2 Tipos de atendimento ao cliente bancário

O cliente bancário conta com varias tipos de canais de atendimento, de acordo com serviços ou produto demandado, ele pode escolher entre os canais o que melhor lhe atende para solução de sua necessidade. O direito do consumidor bancário garante a livre escolha, o cliente pode e deve escolher o sistema de atendimento que lhe convier.

3.2.1 Atendimento pessoal

O atendimento presencial no caixa é o método mais antigo utilizado para efetivar transações financeiras num banco. Por ser um atendimento pessoal, o funcionário atendente

tem a responsabilidade pela identificação do usuário. Neste processo são utilizadas técnicas de identificação básicas como: documentos de identidade, o cartão bancário, verificação de assinatura e senhas. Após o atendente ter confirmado a identificação do cliente ele realizará as transações solicitadas pelo mesmo. Quanto maior a quantidade de verificações efetuadas pelo funcionário, menor será o risco de ocorrência de fraude.

3.2.2 Atendimento no terminal de auto-atendimento

No auto-atendimento não existe o envolvimento de um atendente no processo de operacionalização da transação financeira. Por este motivo o terminal tem que ter condições de verificar a identificação do indivíduo que está utilizando o sistema naquele momento. Com o objetivo de dar essas condições ao terminal são desenvolvidas ferramentas que funcionam como uma espécie de chave, um cartão bancário e senha. Estes terminais estão normalmente equipados com leitor de cartão e teclado numérico.

3.2.3 Atendimento por telefone

O atendimento por telefone frequentemente é efetuado utilizando o conjunto de senhas, informações pessoais e dependendo do tipo de transação é direcionado para o atendimento de um operador da central de atendimento telefônico. Neste atendimento os números são peças chave, pois como o teclado do telefone é limitado, as trocas de informações automatizadas serão efetuadas através de números. Utilizando por exemplos: número de conta, número do cartão, data nascimento, número de algum documento pessoal, entre outros.

3.2.4 Atendimento pelo internet banking

A internet possibilitou o atendimento bancário nas instalações do próprio cliente, permitindo que ele interaja remotamente com o banco e realize transações sem a necessidade de sair de sua casa ou escritório. O internet banking em relação à segurança tem uma fragilidade, que é a dependência das atitudes do usuário para a prevenção contra tentativas de fraude eletrônicas. O usuário é orientado a proteger seu computador de possíveis ataque por vírus, sobre as ferramentas de segurança do internet banking e a forma de utilização do site.

3.3 Técnicas comuns de autenticação e identificação

Os bancos desenvolveram diversas técnicas de autenticação, com o objetivo de elevar a segurança das transações realizadas pelos clientes. A base destas técnicas de autenticação e identificação é o que se tem e o que se sabe.

3.3.1 Autenticação por senhas

As senhas são baseadas em dados secretos os quais somente o usuário conhece, normalmente ele próprio define a combinação que será utilizada para sua autenticação.

> Define-se senha como "um dado secreto, usualmente composto por uma seqüência de caracteres, que é usado como informação para autenticar um usuário ou pessoa" (Pinheiro, 2008. p. 17).

Nos bancos a senha é utilizada em conjunto com um identificador (*login*) que normalmente é formando pelos números da agência e da conta do cliente.

De acordo com tipo de atendimento a formação de senha pode variar, por motivo de limitação de recursos do equipamento. Como observado nos terminais de auto-atendimento, terminais de caixa e no telefone, ambos tem apenas um teclado numérico, isto determina a padronização de senhas numéricas para autenticação do cliente.

Hoje em dia, outros formatos de senha estão sendo utilizados, pois os tipos de atendimento através da internet possibilitam o uso de senhas alfanuméricas (figura 3.1), que os bancos aplicam junto com outras técnicas para dificultar a fraude.

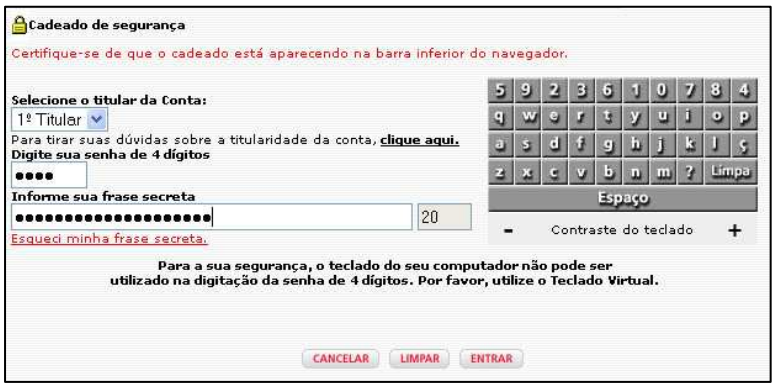

Figura 3.1: Imagem teclado virtual e frase secreta.
Fonte: Banco Bradesco, 2009

3.3.2 Autenticação por posse

Segundo Pinheiro (2008), este método de autenticação é baseado no dispositivo que o usuário possui. Nos bancos este método é observado na aplicação do cartão bancário, principalmente no auto-atendimento, pois o uso do cartão na maioria das transações é obrigatório.

Observa-se que na maioria das transações bancárias que envolvem valores, além da posse do dispositivo é obrigatória uma segunda autenticação que normalmente se faz pela solicitação da senha do usuário.

Na análise em relação à segurança, a soma dos dois métodos os quais se baseiam, no conhecer e possuir, elevam o nível de confiabilidade do sistema. Mas como se pode observar não elimina a possibilidade de fraude, pois o conhecer e possuir são transferíveis, ou seja, uma outra pessoa de posse do dispositivo e conhecendo a senha poderá ter sucesso ao efetuar uma transação no sistema.

3.4 Técnicas de proteção contra cópia das senhas

Para proteção contra a cópia das senhas, os bancos disponibilizam diferentes ferramentas com objetivo de dificultar a captura destas. Assim, combatendo possíveis fraudes.

3.4.1 Teclado virtual

O teclado virtual (figura 3.2) é uma ferramenta que aumenta a segurança, pois se utiliza o mouse para informar a senha. Como os números não têm posição fixa, a cada acesso mudam de lugar, dificulta a captura de informação por alguns tipos de vírus. O fato de não se digitar a senha via teclado também aumenta a segurança do internet banking.

> Com o teclado virtual algumas funções importantes de segurança deixam de depender do seu navegador, como a limpeza do campo onde a senha é digitada. Diminuem-se, também, os riscos decorrentes do armazenamento da senha, pois, com o teclado virtual, ela não ficará em disco ou memória.
>
> Além disso, o teclado virtual incrementa a proteção contra alguns tipos de "cavalos de tróia" ou *trojans* que monitoram a digitação no teclado, os campos de digitação em páginas Web e as informações, antes de serem criptografadas pelo browser (Banco do Brasil, 2009).

Figura 3.2: Imagem teclado virtual.
Fonte: Banco do Brasil, 2009

3.4.2 Digitação indireta de senha

O método de digitação indireta da senha, assim como o teclado virtual, tem a intenção de dificultar a captura da senha através da memorização das teclas pressionadas durante a digitação da senha nos terminais de auto-atendimento. Este método consiste em desvincular a posição da tecla a ser digitada do valor indicado na tela do terminal.

Os bancos com a intenção de aumentar a segurança das transações efetuadas no auto-atendimento, acrescentaram há pouco tempo atrás uma outra senha, adicional a comumente utilizada senha numérica. Independente do nome que foi adotado, código de acesso, código de letras, entre outros, o conceito da funcionalidade é a mesma. Cada instituição implementou esta ferramenta de acordo com seu planejamento estratégico.

O funcionamento desta técnica é baseado no conhecimento do código, que normalmente é formado por letras, estas letras são apresentadas na tela do terminal junto com outras, que formam uma pequena lista de opções. O cliente visualiza os caracteres que representam seu código, e indica apenas sua localização através das teclas auxiliares ou numéricas correspondentes. Como as letras ou caracteres ficam misturados num grupo montado momentaneamente pelo sistema, mesmo que se observe qual foi à tecla pressionada pelo usuário, não se consegue identificar qual foi à resposta selecionada.

3.4.3 Senha segmentada

A segmentação das senhas é a divisão das senhas de acordo com o tipo de atendimento realizado. Consiste basicamente em ter várias senhas para utilização do cliente, ou seja, a senha de internet é diferente da senha do auto-atendimento, que por sua vez é

diferente da senha do atendimento telefônico. O sistema não deve aceitar senhas iguais em diferentes tipos de atendimento, pois o objetivo é impedir que uma senha utilizada para verificar o saldo através do terminal de auto-atendimento, permita o acesso ao sistema pela internet, por exemplo.

Verifica-se que alguns bancos, de acordo com tipo de atendimento e da transação a ser efetuada, agrupam duas ou mais senhas, com a finalidade aumentar a segurança e segmentar também por tipo ou valor da transação.

3.5 Ferramentas de segurança

As ferramentas de segurança têm o objetivo de proteger, tanto o banco quanto o cliente, pois as diversas ferramentas aplicadas garantem uma exposição mínima a risco de fraude.

3.5.1 Cartão bancário

O cartão bancário é a ferramenta de identificação mais comum utilizada pelos bancos. Pode-se afirmar que é a chave básica de acesso ao sistema. Inicialmente o cartão tinha apenas uma tarja magnética, o chamado cartão magnético. Mas com o crescimento das clonagens desta tarja, foi acrescentado junto ao cartão um chip o qual vem dificultando a continuidade destas fraudes.

O cartão sempre é utilizado juntamente com a senha do cliente, assim se tornando um meio bastante seguro para realização de transações financeiras. Em alguns bancos é comum o cartão ter múltiplas funções, a função bancária, a função de crédito e função de débito, e este fato o transformou um dos meios de pagamento mais utilizado no país.

3.5.2 Cadastramento de computadores

O cadastramento de computadores é uma solução que torna mais seguras as transações realizadas no atendimento pela Internet. A partir da adesão ao cadastramento de computadores os limites para transações financeiras pela Internet serão maiores. O computador passa a ser reconhecido pelo sistema do Banco, evitando que pessoas não autorizadas possam movimentar a conta a partir de outros computadores.

3.5.3 Certificado digital

O Certificado Digital funciona como um documento eletrônico que visa atestar a identidade do seu titular (pessoa ou organização) no mundo virtual. Com esse documento é possível a realização, em canais virtuais, de serviços eletrônicos como operações bancárias.

Os certificados, como o tipo A3, utilizam como mídia de armazenamento e portabilidade um hardware criptográfico, que pode ser um cartão inteligente (*smart card*) ou um *token* (USB). Nos chips desses dispositivos são armazenadas as informações referentes ao certificado do usuário. O acesso a essas informações é feito por meio de uma senha pessoal, determinada pelo usuário.

3.5.4 Cartão chave de segurança

O processo de utilização do cartão chave de segurança (figura 3.3) agrega mais segurança nos acessos realizados por meio do internet banking e do auto-atendimento, em razão de utilizar uma chave de segurança que somente o cliente de posse do cartão saberá. Como não existem cartões iguais, cada cartão contém um conjunto de chaves exclusivo para cada cliente.

Figura 3.3: Imagem cartão chave de segurança.
Fonte: Banco Bradesco, 2009

3.5.5 Dispositivo de chave de segurança eletrônica

O dispositivo gerador da chave de segurança (figura 3.4), semelhante ao cartão chave de segurança, agrega mais segurança nos acessos realizados por meio do internet banking, em razão de utilizar uma chave de segurança que somente o cliente de posse do dispositivo saberá no momento de sua utilização. Como não existem dispositivos com números de séries iguais, cada um gerará um conjunto de chaves exclusivo para cada cliente.

Figura 3.4: Imagem dos geradores de chave de segurança eletrônica.
Fonte: Banco Bradesco, 2009

O modelo GO3 é utilizado pelos clientes pessoas físicas do Banco Bradesco. Ao aderir à solução de segurança, o banco fornece o dispositivo que é vinculado ao cliente pelo seu número de série, então possibilitando a validação da identificação no usuário.

Para pessoa jurídica o banco disponibiliza o modelo BR001. Neste caso, o dispositivo, além do número de série que o vincula ao cliente, é equipado com sensor para leitura da transação que está sendo realizada. Assim, este dispositivo gera chave específica para cada transação efetuada na internet pelo cliente, validando o mesmo pelo conjunto de informações adquiridas pelo sistema (BANCO BRADESCO, 2009).

No terceiro capítulo tratou-se do assunto segurança, onde foi abordada a importância da proteção de informação. Os tipos de atendimento ao cliente e qual a técnicas e ferramentas utilizadas atualmente para ter segurança nas transações realizadas junto aos bancos.

O capítulo quatro apresenta estudos de casos que optaram pela biometria como ferramenta de elevação do nível de segurança de operações financeiras.

4 ESTUDOS DE CASOS

4.1 Banco Bradesco

O Banco Bradesco, um dos maiores bancos do país, iniciou a instalação de terminais de auto-atendimento com sensores que lêem as veias da mão de seu cliente. Após análise dos diversos métodos de identificação, a instituição decidiu pela utilização de técnicas biométricas para combater as fraudes nas transações realizadas através deste canal de atendimento.

O uso de biometria pelo banco foca, principalmente, o aumento na segurança. O banco iniciou seu projeto piloto com a instalação de 40 terminais (figura 4.1) em São Paulo e 10 no Rio de Janeiro, utilizando o "PalmSecure", um *scanner* desenvolvido pela empresa japonesa Fujitsu que captura uma imagem do padrão vascular da palma da mão. Hoje em dia, o banco já tem instalado mais de 8.200 terminais de auto-atendimento com leitor biométrico (BANCO BRADESCO, 2009).

Figura 4.1: Imagem do terminal com leitor PalmSecure.
Fonte: Banco Bradesco, 2009

Através deste sistema, o correntista ganha uma "camada extra" de segurança, tendo a leitura do padrão das veias das mãos como uma "chave humana" para acesso à conta.

Além da exigência de senhas alfanuméricas, chips, chaves de segurança e frases secretas, o correntista passa a usar as veias da própria mão para comprovar sua identidade. A introdução da biometria em caixas eletrônicos (figuras 4.2, 4.3 e 4.4) coloca finalmente o que já foi instrumento de ficção científica no dia-a-dia do brasileiro.

Segundo o vice-presidente executivo do Bradesco, Laércio Albino Cezar, em 2006 o banco investiu R$ 1,5 bilhão em tecnologia de segurança, sendo grande parte desse montante destinado à biometria. Ele diz que os gastos com biometria não serão transferidos aos clientes.

No caso do Bradesco, não é necessário trocar o caixa eletrônico para introduzir a biometria. O cartão e a senha ainda são necessários. Os painéis biométricos hoje custam cerca de US$ 700. O banco espera tê-los por até US$ 100 quando for trocar sua "frota". Sua implantação sai por US$ 300 (FOLHA ONLINE, 2007).

Figura 4.2: Imagem frontal do terminal com leitor biométrico.
Fonte: Do Autor

Figura 4.3: Imagem do leitor de cartão, teclado e leitor biométrico.
Fonte: Do autor

Figura 4.4: Imagem do leitor biométrico das veias da mão.
Fonte: Do autor

A proposta é que nos caixas com biometria, o cliente pode utilizar o serviço apenas com o cartão sem digitar a senha numérica. Basta encostar a palma da mão no leitor biométrico e o sistema reconhece o cliente, se ele estiver previamente cadastrado.

Todas as agências que já contarem com o serviço nos ATMs também terão o sistema biométrico na mesa dos gerentes, para registro no processo de abertura das contas. O Bradesco está estudando um leitor biométrico para uso do internet banking. “Dessa forma, o cliente estará protegido contra a clonagem.” (Informaniaco, 2009).

Conforme explicações de um funcionário do banco, o processo de cadastramento é simples. Ele é efetuado no próprio terminal, o funcionário habilita a operação através de seu cartão e senha funcional. O cliente insere seu cartão e digita sua senha, o sistema solicita a colocação da mão no leitor para captura da característica, em seguida, orienta a retirar e colocar novamente a mão no leitor. A segunda leitura é para verificar se a captura foi bem sucedida, assim, concluindo o cadastramento da característica da mão. O sistema ainda pergunta se o cliente deseja cadastrar a outra mão, se optar pela não captura da outra mão, o terminal conclui o cadastramento.

Para o banco, caso não haja rejeição por parte dos clientes, a previsão é configurar os 24 mil terminais no Brasil com leitor biométrico até o final de 2010.

Conforme apresentado na figura a seguir (figura 4.5), o site do Banco Bradesco S/A, divulga a nova tecnologia com a frase “Segurança Bradesco na palma de sua mão”, explicando como se cadastrar e suas principais características.

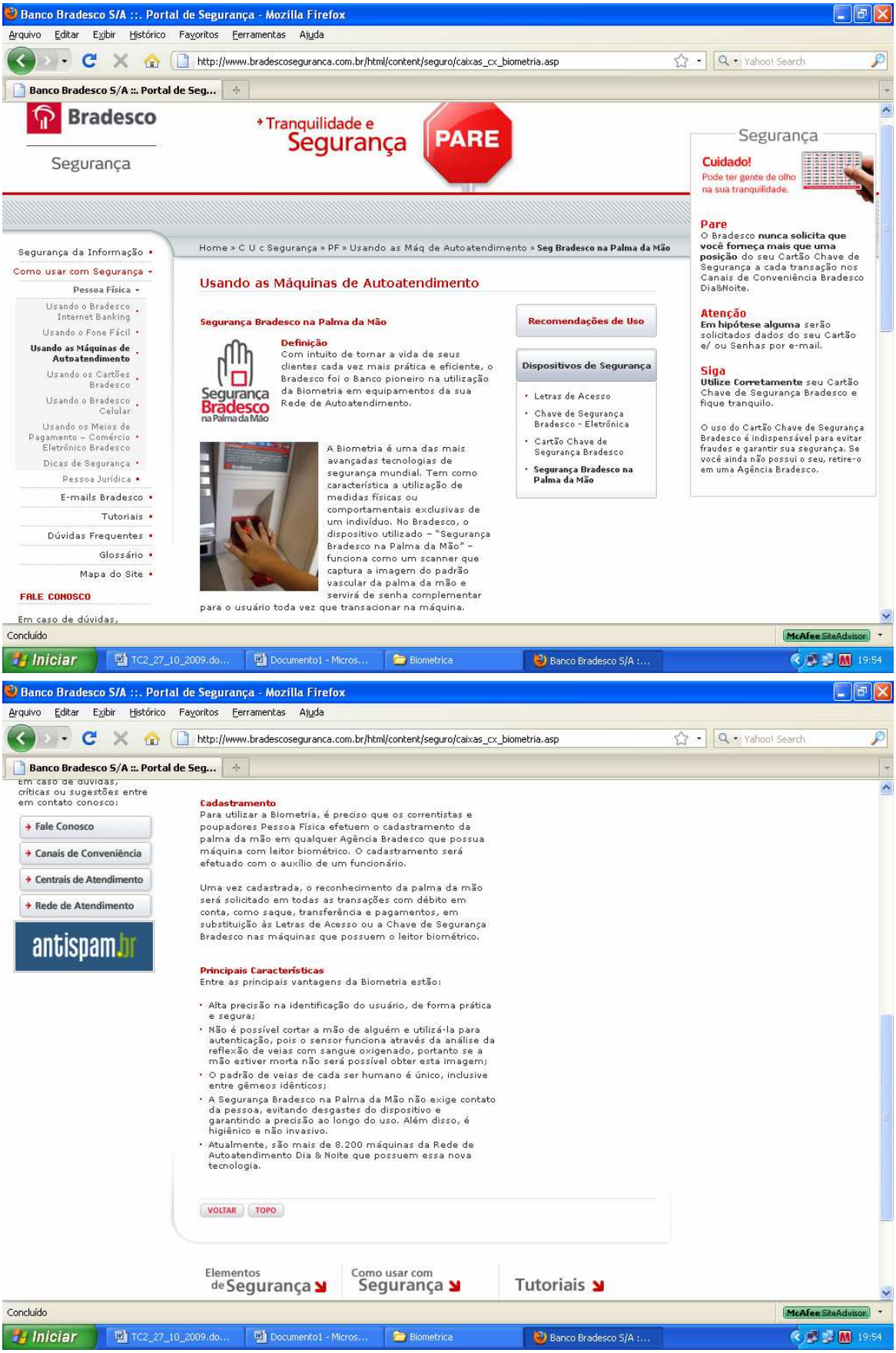

Figura 4.5: Site do Bradesco – Segurança Bradesco na palma da sua mão.
Fonte: Banco Bradesco, 2009

4.2 Impressão digital vai substituir cartão de crédito no Japão

Os japoneses estão dispostos a jogar fora seus cartões de crédito, carteiras e senhas: em breve, poderão fazer suas compras com uma simples impressão digital, graças à tecnologia biométrica. Os funcionários do grupo japonês Hitachi vão colocar à prova um novo sistema em que já não são mais necessários os cartões de crédito, cédulas ou cheques. O novo método conta com a colaboração de várias lojas e da financeira JCB.

No caixa, os funcionários vão especificar que desejam pagar através de sua conta JCB e, com isso, devem passar o dedo sobre um leitor que captará a imagem do sistema vascular através de um raio luminoso direto (FOLHA ONLINE, 2007).

Segundo a Hitachi, como a estrutura dos vasos capilares do dedo é única e não se modifica com o tempo, é impossível reproduzi-la artificialmente. Os dados biométricos do comprador serão comparados no ato com o registro da JCB e as referências bancárias do cliente. Assim como uma compra normal paga com cartão de crédito, o valor será automaticamente descontado ao final do mês da conta corrente. No caso de a impressão digital não corresponder aos dados da entidade, a transação não poderá ser feita.

A experiência feita com os funcionários da Hitachi tem como objetivo elaborar um modelo técnico e econômico viável antes do lançamento comercial do sistema. A biometria já é um sistema muito utilizado no Japão, em particular nas empresas e hospitais que usam a tecnologia para controlar o acesso e as conexões em rede dos seus funcionários. Muitos bancos japoneses já começaram a usar instrumentos biométricos para identificar seus clientes que realizam operações de pagamentos ou transferências de dinheiro nos caixas automáticos.

4.3 Pagamento por impressões digitais

Em Xangai cerca de mil lojas e restaurantes do principal reduto financeiro e comercial da China, começaram a utilizar um novo sistema de pagamento que substitui o cartão de crédito pelas impressões digitais dos clientes (FOLHA ONLINE, 2007).

O sistema biométrico foi lançado apenas para os clientes do Banco Agrícola da China, do distrito de Changning. Para poder pagar suas compras, o cliente coloca o dedo sobre um terminal de pagamento tátil (figura 4.6), o sistema o identifica através de sua

impressão digital, e o dinheiro é retirado diretamente da conta bancária para pagar a conta correspondente.

A empresa responsável pelo sistema, a *Live By Touch Holdings*, assegura que o pagamento por meio das impressões digitais é mais "seguro" que o dos cartões bancários, já que é praticamente impossível imitar as digitais, o que evita possíveis fraudes.

Nos Estados Unidos, quem mora na cidade de Chicago, já pode optar por pagar com o dedo em 10 postos da rede Shell. Eles estão trabalhando em parceria com a empresa "*Pay by Touch*" (Pague por toque), que já tem o sistema funcionando em vários outros negócios e lojas. O cliente faz um cadastro da primeira vez e depois basta utilizar o seu dedo para pagar por sua gasolina (VIDIG, 2007).

Figura 4.6: Imagem terminal *Pay by Touch*.
Fonte: Vigid, 2007

No quarto capítulo apresenta estudos de casos que aplicaram a biometria como ferramenta de autenticação e identificação de clientes. Mostra a viabilidade dos sistemas biométricos aplicados na área financeira.

O capítulo cinco pretende demonstrar a importância da seleção correta do tipo de biometria escolhida para uma determinada aplicação.

5 SELEÇÃO DO SISTEMA BIOMÉTRICO

A seleção do sistema biométrico adequado para cada tipo de aplicação é um processo complexo que envolve diversos fatores. Segundo Pinheiro (2008), de um modo geral os parâmetros de seleção são extraídos dos requisitos da aplicação, sendo determinantes para escolha da tecnologia mais adequada.

5.1 Parâmetros de seleção

A tecnologia escolhida deve prever as diversas variáveis que possam influenciar nas características biométricas obtidas. Assim, minimizando rejeições e validações incorretas.

De acordo com Pinheiro (2008) uma primeira análise pode ser baseada nos pontos fortes e fracos de cada técnica. Para auxiliar no processo de seleção, pode ser utilizada uma matriz de comparação baseada em pesos de atributos. A combinação entre requisitos e atributos resulta em valores de avaliação para cada tecnologia. A interpretação dos pesos, segundo Pinheiro (2008), pode ser ajustada arbitrariamente. A tecnologia de identificação biométrica pode ser avaliada através de alguns parâmetros importantes: desempenho, grau de confiabilidade, nível de conforto, nível de aceitação, custo de implementação e velocidade.

5.1.1 Desempenho

A avaliação do desempenho do sistema biométrico depende de sua capacidade de resposta em termos de velocidade de identificação e da taxa de precisão ou de erro que ele apresenta. Estes fatores são determinantes para mensurar a qualidade e a aceitação da técnica escolhida.

Para analisar o desempenho pode-se utilizar a medida da taxa de falsa aceitação e da taxa de falsa rejeição, pois estas demonstram as margens de erros de identificação dos indivíduos.

5.1.1.1 Taxa de falsa aceitação

Segundo Pinheiro (2008), a primeira métrica que dever ser observada em um sistema biométrico é a taxa de falsa aceitação (FAR ou FMR), pois esta determina o risco de uma permissão de acesso indevida, ou seja, autoriza um impostor a utilizar o sistema se passando por outro indivíduo.

A complexidade da comparação dos exemplares biométricos analisados no processo de identificação é elevada pela diversidade de circunstâncias que possibilitam a perfeita captura da característica a ser válida pelo sistema. As possíveis semelhanças entre as características de dois indivíduos podem causar falsas validações.

As taxas de falsa aceitação podem ser reduzidas com o ajuste do nível de tolerância, exigindo o máximo de igualdade possível entre o exemplar capturado e a característica armazenada no banco de dados o que resultará em um maior nível de segurança, porém se este nível for muito elevado, a taxa de falsa rejeição aumenta proporcionalmente. Pode-se dizer que a taxa de falsa aceitação é inversamente proporcional a taxa de falsa rejeição.

De acordo com Pinheiro (2008), a taxa de falsa aceitação representa a percentagem de usuários não autorizados que são incorretamente identificados como usuários válidos e pode ser calculada como:

$$FAR = NFA / NIIA$$

Onde, NFA é o número de falsas aceitações e NIIA é o número de tentativas de identificação do impostor.

Na prática, se a taxa de falsa aceitação for zero ou nula, pode causar uma alta taxa de falsa rejeição, que tornaria o sistema biométrico inviável. Conclui-se que nenhum impostor teria sucesso na sua validação, mas os indivíduos credenciados teriam uma grande dificuldade em validar seu acesso, a ponto de causar muitos transtornos e ineficiência do sistema biométrico.

5.1.1.2 Taxa de falsa rejeição

A taxa de falsa rejeição é a probabilidade da comparação incorreta entre os exemplares biométricos, negando a autenticação do usuário válido aos recursos do sistema ao qual ele está habilitado.

Esta situação ocorre porque não existe uma correlação suficientemente forte entre a característica biométrica apresentada e a armazenada no banco de dados. Pode-se atribuir aos seguintes fatores:

- Mudanças nos dados biométricos;
- Mudança na forma como o usuário apresenta os dados;
- Mudanças no ambiente do sistema, no qual os dados são apresentados.

Pode-se reduzir o impacto da falsa rejeição com adequada parametrização do sistema. Mas é importante ressaltar que com o aumento da utilização, os sistemas biométricos tendem a apresentar problemas de falsa rejeição.

A taxa de falsa rejeição sendo muito alta pode causar conseqüências negativas, pois resulta em lentidão, perda de produtividade, usuários frustrados, entre outros. Por este motivo tem peso muito grande no processo de aceitação do sistema biométrico a ser implementado.

Conforme Pinheiro (2008) resume em seu livro, a taxa de falsa rejeição representa a percentagem de usuários autorizados que são indevidamente rejeitados pelo sistema e pode ser calculada da seguinte forma:

$$FRR = NFR / NEIA$$

Sendo, NRF o número de falsas rejeições e NEIA o número de tentativas de identificação de usuários legítimos.

Em seu livro Pinheiro (2008), lembra que a taxa de falsa aceitação (FAR) e o taxa de falsa rejeição (FRR) são mutuamente dependentes, ou seja, diminuir FAR significa aumentar FRR e vice-versa. Na tabela 5.1 são apresentadas às taxas de desempenho FRR e FAR de alguns sistemas biométricos utilizados.

Tabela 5.1 – Taxas de desempenho em sistemas biométricos.

TIPO DE SISTEMA	FRR	FAR	TEMPO
Impressão Digital	9,4 %	0,0 %	7,0 segundos
Retina	1,5 %	1,5 %	7,0 segundos
Palma da Mão	0,0 %	0,00025 %	3,0 segundos
Geometria da Mão	0,1 %	0,1 %	3,0 segundos
Voz	8,2 %	0,4 %	3,0 segundos

Fonte: Pinheiro, 2008 p.106

5.1.2 Grau de confiabilidade

De acordo com Pinheiro (2008), o grau de confiabilidade de um sistema biométrico pode ser aferido segundo os índices de falsa aceitação e de falsa rejeição. Mas como estas variáveis são dependentes, não é possível minimizar ambas. Pode-se calibrar o sistema através de ajustes do limiar, mas eleva-se a margem de erros de identificação.

Como já foi dito anteriormente, a falsa aceitação deixa brechas para admissão de usuários não-autorizados, porém a falsa rejeição causa problemas de conveniência, negando acesso aos usuários legítimos.

Na avaliação de confiabilidade e qualidade do sistema biométrico é necessário encontrar o ponto de equilíbrio, onde as taxas FAR e FRR são iguais. Este ponto é chamado de CER (*Crossover Error Rate*), também denominado ponto de operação EE (*Equal Error*), ao qual está associada uma taxa EER (*Equal Error Rate*). Depois de identificado este ponto de equilíbrio deve-se calibrar o sistema para operar nas faixas de maior conveniência ou de maior segurança, que por conseqüência estabelece um grau de confiabilidade do sistema.

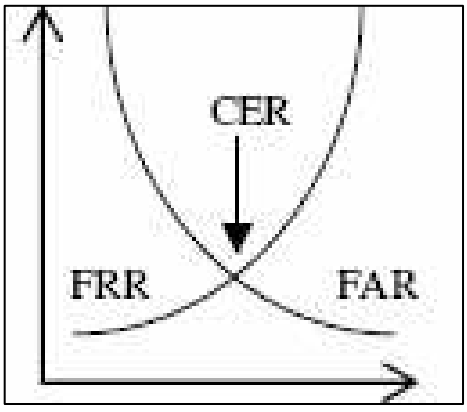

Figura 5.1: Relação entre FRR, FAR e CER.
Fonte: Pinheiro, 2008 p. 108

5.1.2.1 Taxa de falha de registro

Segundo Pinheiro (2008), a taxa de falha de registro representa a probabilidade de um determinado usuário não poder se registrar no sistema biométrico, isto ocorre quando o mesmo apresenta amostras insuficientes da característica biométrica.

Pode-se afirmar que a taxa de falha de registro (FTE – *Failure-To-Enroll Rate*), é na prática a medição de quantas tentativas de captura da característica biométrica são necessárias para que o sistema adquira com sucesso o exemplar a ser armazenado no banco de dados. Essa taxa difere significativamente de tecnologia para tecnologia e de dispositivo para dispositivo. Deve-se considerar não apenas o tipo de característica biométrica, mas também a ergonomia dos dispositivos de aquisição.

Para melhor entendimento, por exemplo, um dispositivo de leitura de impressão digital colocado sobre uma mesa sem a devida orientação de posicionamento do dedo para correta coleta da característica. Desta forma, a digital capturada poderia ser lida com ângulo de 90º graus em relação à posição correta. Isto certamente causaria dificuldade na validação do exemplar. Por este motivo os dispositivos e o devido treinamento dos usuários do sistema biométrico são fatores fundamentais para redução da taxa de falha de registro.

Busca-se minimizar esta taxa através da escolha correta do tipo de biometria e dos dispositivos mais adequados para implantação do sistema.

5.1.3 Conforto e aceitação

Este parâmetro é determinante para o sucesso do sistema biométrico, pois conforto e aceitação são padrões subjetivos do usuário. De um modo geral, o sistema é mais aceito quanto menos intrusivo ele for.

5.1.4 Custos de implementação

Como em qualquer projeto ou negócios a ser iniciado, um dos fatores mais importantes para análise de sua viabilidade é o custo. Pois para aceitação de um novo sistema, a visão empresarial sempre se baseia no custo/benefício da solução apresentada. Pode-se elaborar um sistema muito seguro, praticamente inviolável e com baixíssima probabilidade de falhas, mas se o custo for impraticável, será considerado inadequado.

5.1.5 Velocidade de operação

A velocidade de operação deve ser avaliada na escolha do sistema biométrico. Apesar do tempo de resposta ter influência direta do usuário, pois o processo de captura depende da colaboração do mesmo, a velocidade também depende do método de comparação que o sistema irá utilizar. Se a comparação for direta, com apenas um exemplar específico no banco de dados (1:1), o tempo de resposta será menor. Mas se for utilizado um padrão de comparação de um com todos os exemplares existentes (1:N), isto tornará o tempo de resposta maior, comprometendo a velocidade de operação. No caso de um banco, por exemplo, ficaria inviável comparar uma característica biométrica capturada com todo o banco de dados, pois além de elevar as margens de identificação errada, teria sua velocidade operacional comprometida.

5.2 Metodologias da avaliação

Em seu livro, Pinheiro (2008) explica que um sistema biométrico pode ser complexo, produzir definições duvidosas de precisão e desempenho, além de demandar fortes investimentos em infra-estrutura, hardware, software, treinamento, entre outros. Por este motivo faz-se necessário uma avaliação mais consistente, pois é desejável a existência de métricas precisas e de testes bem definidos. Nesta finalidade, destacam-se as metodologias de avaliação de tecnologia, de cenário e operacional.

5.2.1 Avaliação de tecnologia

Conforme, Costa (2007), o objetivo da avaliação de tecnologia é a comparação dos algoritmos biométricos competidores de uma tecnologia única. Os testes são realizados sobre um banco de dados padronizado de perfis biométricos. Neste tipo de avaliação, é concedido aos competidores um período de tempo para treinar seus algoritmos de verificação. Um banco de dados de perfis biométricos é disponibilizado para esta função, baseado em dados previamente construídos. Os módulos de comparação dos competidores recebem estes dados e têm direito a um certo tempo para o treinamento de seus algoritmos. Após esta fase de treinamento, inicia-se a fase de teste, onde são definidas as maneiras de obtenção das estatísticas de desempenho. Pode-se dizer que a avaliação consiste em duas fases, fase de treinamento e fase de competição.

A avaliação de tecnologia permite obter estimativas das taxas de erro dos comparadores. O ponto fraco desta avaliação é que os módulos de comparação são aplicados sobre os bancos de dados já existentes, sem controle do ambiente de registro.

5.2.2 Avaliação de cenário

Segundo Costa (2007), o objetivo da avaliação de cenário é determinar o desempenho geral do sistema numa aplicação em testes que simulam o ambiente real. É fornecida uma mesma coleção de dados biométricos para os sistemas participantes da avaliação. Este tipo de avaliação ocorre em uma instalação especial, onde são instalados os dispositivos biométricos de verificação (1:1) usados nos testes. Um grupo de voluntários utiliza os sistemas durante um período de tempo, enquanto as estatísticas são coletadas. Pode-se comparar diferentes fabricantes ou até mesmo diferentes tecnologias ao mesmo tempo. Esta avaliação cria como subproduto um banco de dados de perfis biométricos que pode ser utilizado posteriormente para avaliações operacionais. Nestes testes são obtidas estimativas de FAR e FRR. O ponto fraco desta avaliação é que os dispositivos não são realmente atacados, o que resulta em valores irreais de FAR.

5.2.3 Avaliação operacional

Costa (2007) diz que o objetivo da avaliação operacional é determinar o desempenho do sistema biométrico como um todo, inserido num ambiente específico de aplicação, atuando sobre um público selecionado. Os resultados geralmente não são passíveis de repetição, já que dependem de características às vezes desconhecidas ou não documentadas do ambiente de aplicação. Este tipo de avaliação é realizado sob circunstâncias reais, ou seja, no ambiente organizacional. Mesmo sendo a avaliação mais realista, não pode medir a verdadeira FAR, já que os eventos de falsa aceitação serão de conhecimento exclusivo dos fraudadores. No entanto, ainda há a possibilidade de estimativa da verdadeira FAR, complementando esta avaliação por meio da utilização de algo parecido com a utilização de testes de invasão, a exemplo do que é feito com segurança de redes de computadores.

5.3 Extração de características

Como Pinheiro (2008) explica em seu livro, uma questão fundamental nos sistemas de processamento de imagens é o esforço computacional necessário para realizar a tarefa de extração das características biométricas do indivíduo. Sabe-se que é grande a probabilidade da existência de dados redundantes e irrelevantes. Isto torna o processo de classificação demorado e assim elevando o custo e prejudicando a eficiência do sistema.

As técnicas de extração devem ter como objetivo focar apenas as características relevantes do padrão a ser verificado, assim reduzindo o tempo gasto no processo de identificação. A eficiência da extração é fator importante para seleção do sistema biométrico.

5.4 Falha nos sistemas biométricos

Para correta escolha do sistema biométrico a ser utilizado, deve-se levar em consideração que como qualquer tipo de sistema existe a possibilidade de falha. Pois cada tipo de sistema biométrico apresenta vantagens e desvantagens em relação o grau de certeza ou probabilidade de erro, facilidade de aplicação, custos, rapidez de resposta e outros parâmetros.

> Os sistemas biométricos não são totalmente imunes contra falhas de segurança e todos os sistemas de reconhecimento biométrico, em princípio, estão sujeitos a ataques e fraudes em maior ou menor grau. (Pinheiro, 2008. p. 118)

Apesar dos sistemas biométricos serem considerados os menos vulneráveis num processo de identificação, existe a possibilidade de enganar o sistema de reconhecimento apresentando amostras artificiais, tais como uma impressão digital falsificada, uma íris artificial ou uma máscara facial.

Mas para elaborar com precisão o falsificador deve conseguir uma representação da característica biométrica original. Observa-se que a possibilidade de sucesso pode ocorrer em determinadas condições:

- O tipo biométrico falsificado é conseguido com a cooperação voluntária ou involuntária do proprietário original da característica;
- A característica biométrica falsificada é elaborada a partir da característica original obtida anteriormente;

- A característica biométrica falsificada é montada a partir da imagem reconstituída do modelo (*template*) fornecido ao sistema pelo proprietário verdadeiro daquela característica e armazenada no banco de dados.

Embora seja relativamente simples obter uma característica biométrica falsificada, produzir uma cópia com qualidade suficiente para enganar um sistema de reconhecimento é muito difícil.

A tabela 5.2 apresenta informações importantes a serem analisadas no comparativo entre as tecnologias biométricas, apresentando critérios de: padrão codificado, taxa de falhas na identificação, nível de segurança e aplicabilidade.

Tabela 5.2 – Comparativo entre as tecnologias biométricas por critério.

Característica Biométrica	**Padrão Codificado**	**Taxa de falhas na identificação**	**Nível de segurança**	**Aplicabilidade**
Reconhecimento da íris	Padrões da íris	1 em 1200000	Alto	Instalações de alta segurança
Impressão digital	Impressão digital	1 em 1000	Médio	Autenticação, controle de acesso, etc.
Forma da mão	Tamanho, comprimento, largura.	1 em 700	Baixo	Instalações de baixa segurança
Reconhecimento facial	Perfil, distribuição dos pontos nodais.	1 em 100	Baixo	Instalações de baixa segurança
Assinatura	Forma das letras, modo de escrita, pressão sobre a superfície.	1 em 100	Baixo	Instalações de baixa segurança
Reconhecimento da voz	Características da voz	1 em 30	Baixo	Serviço de telefonia

Fonte: Pinheiro, 2008 p.123

5.5 Performance das propriedades por tipo de biometria

De acordo com Sá (2006), para uma biometria ser útil em situações práticas, ela deve ter precisão no reconhecimento e velocidade com o uso de equipamentos de boa performance e baixo custo, ser aceita pela população atendida e ser suficientemente robusta contra fraudes. Na Tabela 5.3 as propriedades de vários tipos de biometrias são comparadas:

• Universal: indica se a biometria é encontrada em todos os indivíduos;

• Distinção: indica o quanto uma biometria distingue um indivíduo do outro;

• Permanência: indica se a biometria mantém-se inalterada no envelhecimento;

• Coleta: indica a facilidade de adquirir os atributos da biometria para comparação;

• Desempenho: indica a precisão, a velocidade e a robustez do sistema;

• Aceitação: indica o grau de aprovação do uso da biometria em seu cotidiano;

• Fraude: indica a dificuldade de se enganar o sistema.

As propriedades estão categorizadas como: alta (A), média (M) ou baixa (B). Uma classificação alta indica uma performance boa da biometria no critério avaliado, enquanto que uma classificação baixa indica um performance ruim. A tabela 5.3 apresenta uma atualização da tabela original apresentada por Sá em 2006. Tal atualização se fez necessária pela grande evolução destas tecnologias.

Tabela 5.3 – Comparação das biometrias.

Identificador Biométrico	**Universal**	**Distinção**	**Permanência**	**Coleta**	**Desempenho**	**Aceitação**	**Fraude**
Assinatura	**B**	**B**	**B**	**A**	**B**	**A**	**B**
Caminhada	**M**	**B**	**B**	**A**	**B**	**A**	**M**
Dinâmica de Digitação	**B**	**B**	**B**	**M**	**B**	**M**	**M**
DNA	**A**	**A**	**A**	**B**	**A**	**B**	**B**
Face	**A**	**B**	**M**	**A**	**B**	**A**	**B**
Geometria da Mão	**M**	**M**	**M**	**A**	**M**	**M**	**M**
Impressão Digital	**A**	**A**	**A**	**A**	**A**	**M**	**A**
Íris	**A**	**A**	**A**	**M**	**A**	**B**	**A**
Odor	**A**	**A**	**A**	**B**	**B**	**M**	**A**
Orelha	**M**	**M**	**A**	**M**	**M**	**A**	**M**
Retina	**A**	**A**	**M**	**B**	**A**	**B**	**A**
Termograma Facial	**A**	**A**	**B**	**A**	**M**	**A**	**A**
Veias da Mão	**A**	**A**	**A**	**A**	**A**	**M**	**A**
Voz	**M**	**B**	**B**	**M**	**B**	**A**	**B**

5.6 Mercado dos sistemas biométricos

De acordo com CFSEC *Security Architects*, a Biometria vem sendo uma tecnologia de segurança de adoção mais acelerada nos últimos anos. Seu custo começou a cair a partir do momento que o mercado deixou de ser só as agências governamentais e passou a contar com o mundo corporativo privado.

5.6.1 Expectativa de faturamento com os sistemas biométricos

A empresa independente de pesquisa do Reino Unido, *International Biometric Group* (IBG), publica relatórios sobre as tendências do mercado de Biometria a nível global. Os gráficos 5.1 e 5.2 apresentam as projeções deste crescimento, pré-crise e pós-crise.

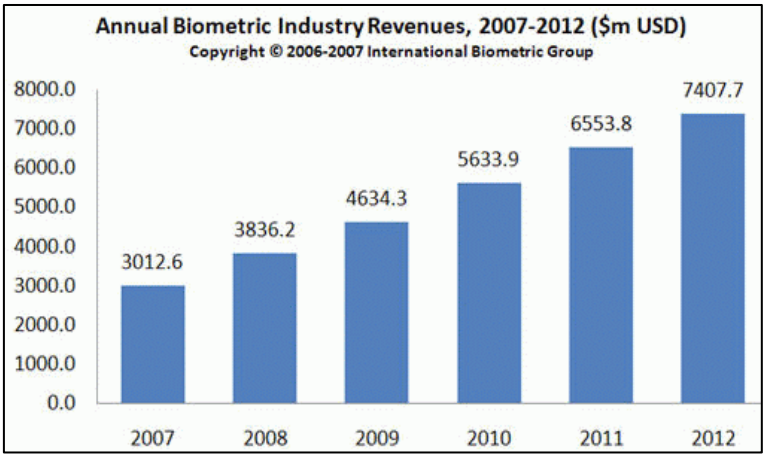

Gráfico 5.1: Faturamento projetado da Biometria 2007-2012, Pré-crise.
Fonte: International Biometric Group, 2007

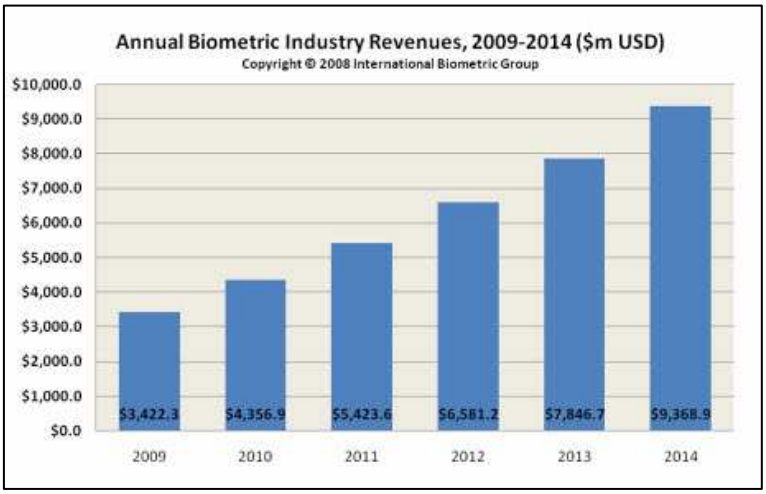

Gráfico 5.2: Faturamento projetado da Biometria 2009-2014, Pós-crise.
Fonte: International Biometric Group, 2008

Comparando as informações apresentadas nos gráficos 5.1 e 5.2, verifica-se que apesar da crise econômica mundial ocorrida no ano de 2008, este mercado continua com projeções muito favoráveis, que confirmam seu grande potencial de mercado.

Observa-se no gráfico 5.2 que o faturamento global está projetado para crescer de 3,42 bilhões de dólares em 2009, para 9,37 bilhões de dólares em 2014.

Ainda segundo o relatório do IBG, espera-se que a biometria de impressão digital fique com 45,9% do mercado, excluindo-se as soluções de AFIS. Apesar da forte evolução, o mercado de íris só deve chegar em 500 milhões de dólares em 2012, basicamente equipando forças armadas ou organizações governamentais.

Cabe salientar que mesmo tendo nascido fora dos Estados Unidos ou Europa, o mercado reconhecimento de veias, que encontra sua maior força no Japão, deve chegar a ter 10% do total, exceto AFIS, até 2014.

5.6.2 Análise de participação dos diferentes tipos de biometria no mercado

O mercado de sistemas biométricos, conforme resultado apurado pelo IBG, vem apresentando a impressão digital com uma das técnicas mais utilizadas e mais comercializadas a nível mundial.

A grande participação da impressão digital justifica-se pelas vantagens desta técnica em relação as outras existentes. O alto grau de aceitação, somado ao bom desempenho e o baixo custo, projetam que esta técnica pode representar cinqüenta por cento do mercado.

Observa-se uma forte tendência do mercado pela utilização de impressão digital, mas isto faz parte do processo natural da quebra de paradigmas, pois é baseada em um método de identificação já aplicado e conceituado junto a órgãos oficiais por todo mundo. Esta característica facilita a aceitação da tecnologia por parte do usuário.

Como é de costume em todo segmento de mercado, a primeira onda tecnológica aceita, concentra os investimentos pesados dos fabricantes com objetivo de manter sua participação neste novo conceito. Após expansão do volume de sistemas biométricos instalados e com a popularização desta ferramenta, inicia-se outra etapa que é o processo de

diversificação de métodos baseado na biometria, assim novas técnicas são desenvolvidas e aperfeiçoadas aumentando a competitividade dos diferentes tipos de sistemas.

Analisando os gráficos, verifica-se expansão de técnicas baseadas na impressão digital, a *Fingerprint* (Impressão Digital) e a AFIS/*Live-Scan* (*Automated Fingerprint Identification System* - Sistema de identificação de impressão digital automatizada), na comparação entre os gráficos de faturamento por tipo de biometria, apresentados pelo IBG, as vendas destas técnicas juntas em 2007 (gráfico 5.3) totalizavam 58,95% do total, já em 2009 (gráfico 5.4) projeta-se que as mesmas totalizarão 66,4% do total de faturamento do mercado da biometria. Isto comprova o crescimento do uso impressão digital no mundo (CFSEC, 2009).

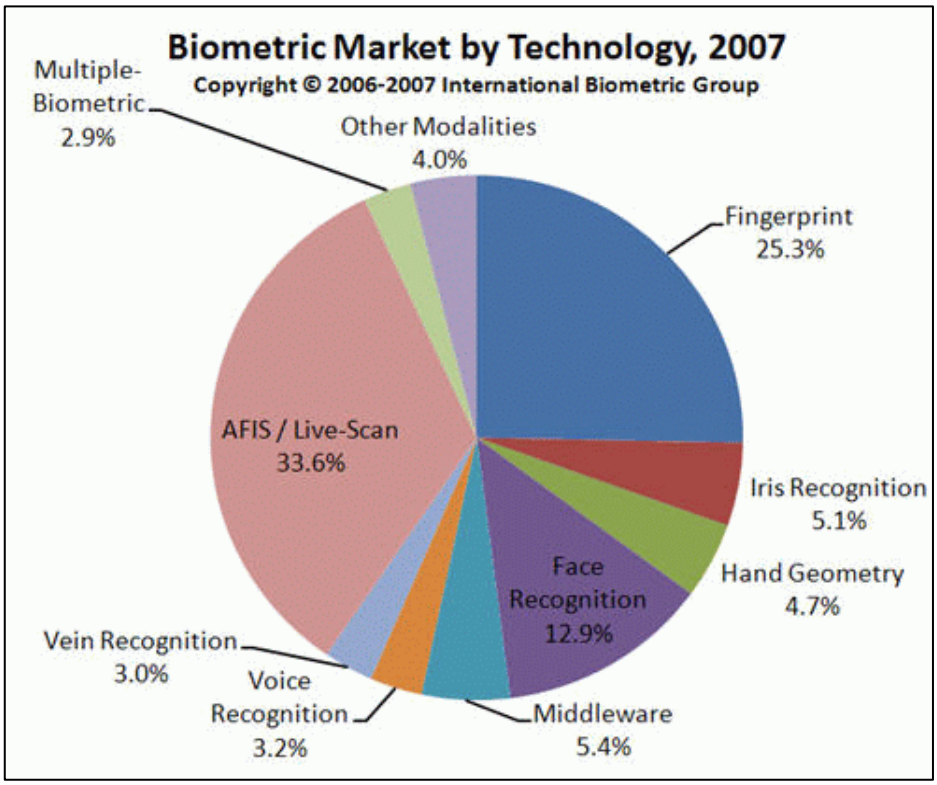

Gráfico 5.3: Faturamento pelo tipo de Biometria 2007.
Fonte: International Biometric Group, 2007

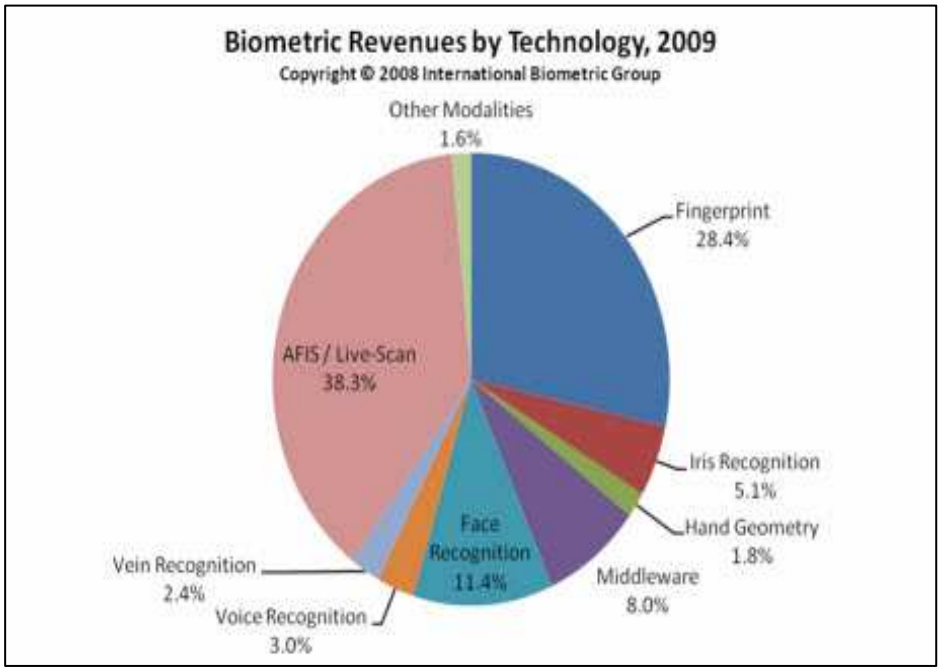

Gráfico 5.4: Faturamento pelo tipo de Biometria 2009.
Fonte: International Biometric Group, 2009

A busca por maior segurança faz o mercado se alterar, observa-se o aumento das vendas das tecnologias que apresentam o melhor desempenho no combate a fraudes. Por exemplo, a redução da participação do método de geometria das mãos, verifica-se uma redução de sua participação para 1,8% das vendas em 2009 com relação ao porcentual de 4,7% apurado em 2007. O estudo dos gráficos 5.3 e 5.4 demonstra que as técnicas biométricas que apresentam o melhor desempenho no quesito combate à fraude (fraude = A na tabela 5.3) somado ao baixo custo de implantação, estão aumentando seus índices de participação no faturamento a nível global.

Estima-se neste cenário de mercado o crescimento dos sistemas biométricos baseados nas veias, tanto da mão quanto do dedo. Este método apresenta performance semelhante a da impressão digital, nos quesitos aceitação e fraude (tabela 5.3), por isto o IBG projeta um aumento de faturamento deste tipo de sistema. No Brasil o sistema de reconhecimento pelas veias da palma da mão deu um importante avanço em termos de mercado, pois esta é a tecnologia escolhida por um dos maiores bancos brasileiros, Banco Bradesco S/A, o qual já instalou o leitor (figura 4.4) em milhares de terminais de auto-atendimento (figura 4.2) por todo país.

5.7 Análise sobre seleção dos sistemas biométricos

Os estudos realizados neste trabalho demonstram a importância da correta seleção dos tipos de sistemas que serão propostos para utilização da biometria na segurança das transações bancárias.

No processo de escolha, além do desempenho do sistema escolhido, é necessária uma profunda análise do ambiente onde os mesmos serão inseridos. Observa-se que no estudo da proposta muitos obstáculos são identificados no ambiente que dificultam a implementação da solução.

Para exemplificar como o ambiente pode mudar a escolha do método, relata-se que no início deste trabalho, antes do devido conhecimento dos métodos de captura das características biométricas do indivíduo e o impacto que o ambiente poderia causar sobre a perfeita aquisição destas características, idealizava-se a possibilidade de implantação do reconhecimento de voz na autenticação do usuário nos terminais de auto-atendimento. Após os estudos sobre o método, apesar de apresentar baixo custo de implementação, o mesmo demonstrou que não seria a solução adequada para o ambiente de uma sala de auto-atendimento, pois a interferência de ruídos gerados pelas pessoas que utilização o local causaria altos nível de falsa rejeição. Conclui-se que o reconhecimento de voz não é o sistema adequado nestas condições, não se descartando o uso desta técnica para o atendimento telefônico.

Dentro as técnicas de identificação biométricas comportamentais, como voz, assinatura e dinâmica de digitação, observa-se a baixa performance em relação ao combate a fraude, o que diminui o interesse pela aplicação destas técnicas. Mas não se deve descartar a futura aplicação de nenhuma delas, pois em termos de aumento da segurança, todos os tipos de biometria têm dado sua colaboração.

Os sistemas biométricos que ganham forte aderência são os baseados em características físicas, pois os mesmos apresentam em média melhor desempenho no combate a fraude e falhas de identificação.

Entre as características físicas, destaca-se pelo alto grau de confiabilidade e baixíssimo risco de fraude estão o reconhecimento da íris e da retina. Estas técnicas estão sendo utilizadas em lugares que necessitam de acesso restrito com alto nível de segurança,

onde normalmente é fornecido aos usuários treinamento para utilização dos leitores, pois muitos destes equipamentos precisam de um olhar fixo por alguns segundos para efetuar a correta captura da característica. Para finalidade desta proposta, o interesse por esta técnica diminui baseado no alto custo do sistema e principalmente no baixo nível de aceitação dos usuários.

O reconhecimento de face apresenta melhor desempenho em termos de aceitação, muito dos terminais de auto-atendimento já possuem câmera que captura imagem do usuário para armazenagem desta junto à transação. Porém para o uso desta técnica teria que ser realizada toda uma reestruturação do ambiente, principalmente em termos de luminosidade, pois a falta de padrão atual causa muita interferência na captura da imagem. Esta técnica, assim como a de reconhecimento de voz, está muito sucessível a interferências do ambiente, causando um baixo desempenho. Além disso, apresenta uma baixa avaliação no requisito de combate à fraude. Assim, chega-se a conclusão que não é a tecnologia adequada para solução do problema proposto neste trabalho.

Outra técnica estudada é do reconhecimento pela geometria da mão. Apesar de apresentar um desempenho razoável, esta tecnologia vem diminuindo sua participação no mercado. Como o seu custo está muito próximo ao de outras técnicas que demonstram melhor avaliação, principalmente no requisito de combate à fraude, esta técnica vem sendo mais utilizada por sistemas que não requerem um nível muito alto de confiabilidade. Avalia-se que o desempenho deste método de identificação está abaixo do nível esperado para solução proposta por este trabalho e a diminuição de suas vendas no mercado mundial induz a acreditar que está caindo em desuso.

Neste momento encontra-se a grande disputa, pois eliminada momentaneamente a utilização de outros sistemas biométricos, tem-se pela frente a decisão de apresentar dentre as duas tecnologias de grande potencial para solução da proposta de trabalho, que são: o reconhecimento de impressão digital e o reconhecimento pelas veias da palma da mão.

Nos estudos realizados, as tecnologias apresentaram excelente desempenho no combate à fraude, o principal objetivo da proposta. No conceito de aceitação, ambas empatam, com nível razoável de performance neste item. Na análise comparativa da tabela 5.3, observa-se que as duas tecnologias demonstram um melhor desempenho na visão geral, em comparação com as demais técnicas apresentadas neste trabalho.

De acordo, com informações disponíveis no site da Fujitsu, em 14.07.2009 o seu sistema de identificação biométrica baseado no reconhecimento de veias da palma da mão, chamado PalmSecure, é a primeira solução de reconhecimento vascular a ganhar uma certificação internacional, isto posiciona o PalmSecure como uma das soluções biométricas mais seguras da indústria de identificação.

Com base nas informações do fabricante, Fujitsu, e confirmadas pelo comprador, Banco Bradesco S/A, o que justifica optar pela técnica de reconhecimento pelas veias da palma da mão, mesmo com o maior custo de investimento inicial em relação à impressão digital é a diferença entre os leitores biométricos. Existe uma vantagem do leitor de veias o qual não exige contato direto da palma da mão, a captura é efetuada a uma distancia de aproximadamente três centímetros, aumentando a higiene e diminuindo o custo de manutenção e limpeza do dispositivo.

Defini-se, considerando todas as informações até o momento obtidas, somada a busca por soluções padronizadas para este segmento de mercado, que a principal tecnologia biometria a ser proposta na utilização para segurança das transações bancárias é o de reconhecimento das veias da palma da mão.

No quinto capítulo apresenta-se o processo de seleção do sistema biométrico que deverá ser indicado para solução da proposta deste trabalho, demonstrando a importância dos estudos necessários para correta escolha da tecnologia.

O capítulo seis pretende apresentar a proposta deste trabalho para a utilização do sistema biométrico na segurança das transações bancárias.

6 PROPOSTA DE UTILIZAÇÃO DA BIOMETRIA

A utilização da biometria nas transações bancárias é, sem dúvida, a solução para minimizar os riscos de fraudes, pois as ferramentas de segurança aplicadas na maioria das transações estão baseadas no que se possui e no que se conhece (PINHEIRO, 2008). Esta tecnologia inclui um novo conceito, que é do "ser", onde a característica autentica que o indivíduo é quem diz ser. Isto gera um novo cenário em termos de segurança, que restringe a exposição dos bancos a possíveis perdas financeiras e ganho com aumento da credibilidade.

Além do combate a fraude, os bancos se tornaram referência em relação às inovações tecnológicas, isto gera comparações por parte do mercado que cria expectativas sobre a evolução do sistema bancário. "A indústria bancária costuma ser reconhecida como um dos setores que mais se destacam no uso de tecnologia de informação" (BARBIERI, 2008 p. 45).

Apesar da pressão por soluções inovadoras. O processo de implantação da biometria deve ser realizado de forma gradual, priorizando os usuários que demonstram maior aceitação. Deve-se primeiro divulgar as vantagens da utilização da técnica. Assim, se terá maior sucesso na implantação desta nova tecnologia.

Nesta proposta, o sistema biométrico terá a função autenticação do cliente, ou seja, primeiro o mesmo de identifica e só então o sistema valida sua autenticidade (1:1).

6.1 Estratégia de marketing

A instituição financeira deve efetuar uma ação de marketing, focada na adesão por parte dos clientes à nova ferramenta. A elaboração de frase de impacto, como fez o Bradesco com a frase: "Segurança Bradesco na palma de sua mão", causam efeito positivo na divulgação da nova tecnologia.

Com a realização de uma ampla divulgação das vantagens em relação à segurança e os benefícios que a adesão pela biometria poderá proporcionar ao cliente. Pode-se estabelecer um programa de benefícios aos clientes que aderirem à técnica, como por exemplo:

- Desconto em tarifas bancárias;
- Pontuação extra em programas de relacionamento;
- Desconto na anuidade de cartões de crédito;
- Maior segurança para cliente.

Uma estratégia de marketing bem desenvolvida acelera o processo de adesão à solução, ocasionando o retorno do investimento no menor prazo possível.

6.2 Proposta de sistemas biométricos - terminais auto-atendimento

Inicia-se a implantação da utilização dos sistemas biométricos pelos terminais de auto-atendimento, pela importância estratégica destes equipamentos para os bancos e por ser um dos canais de atendimento mais sucessível a fraude.

O sistema biométrico de autenticação pelas veias da palma da mão é a tecnologia escolhida para utilização nos terminais de auto-atendimento. A técnica apresenta vantagens em relação aos demais métodos biométricos. Principalmente em relação ao leitor biométrico, que não necessita do contato direto com o mesmo para realizar a captura do exemplar. Isto evita danos e aumenta a vida útil do equipamento reduzindo custo de manutenção. Esta característica do leitor é vantajosa para instalação num terminal de auto-atendimento, pois o leitor fica exposto num ambiente sem controle rígido, onde o usuário tem total acesso ao mesmo. Outra vantagem é o fato do método ser pouco intrusivo não gerando desconforto ao cliente durante o processo de utilização do leitor.

6.2.1 Implantação

Inicia-se com a aquisição e instalação dos leitores nos terminais de auto-atendimento, e/ou com a aquisição de novos terminais já com equipamento instalado. Para diminuir o impacto inicial, recomenda-se que cada ambiente de auto-atendimento tenha pelo menos um terminal com o leitor. Com a evolução do uso da técnica o objetivo é que todos os terminais instalados tenham o dispositivo.

6.2.2 Estimativa de custo e prazo

Segundo estudos efetuados sobre a estimativa de custo de implantação do sistema biométrico de reconhecimento pelas veias da palma da mão, tendo como fornecedores a Fujitsu e a Perto e comprador um banco de grande porte, como Bradesco, Itaú e Banco do Brasil, o custo médio do leitor instalado e funcionando por terminal seria:

- Terminal de auto-atendimento novo - custo adicional do leitor R$ 900,00;
- Terminal de auto-atendimento instalado - custo instalação do leitor R$ 2.000,00.

O prazo para instalação de no mínimo um terminal por ponto de atendimento é estimado em 2 anos. Para a instalação em todos os terminais de auto-atendimento projeta-se que seriam necessários 6 anos. Mas estes prazos dependem muito do interesse estratégico do banco que vai estabelecer um grau de prioridade ao projeto.

6.2.3 Agrupamento dos clientes para cadastramento

A partir da instalação do primeiro terminal com leitor biométrico na agência ou posto de atendimento bancário, todos os novos clientes terão sua característica biométrica cadastrada. Os atuais clientes do banco serão convidados a aderir à nova tecnologia de forma gradual, estabelecendo grupos de acordo com o perfil do cliente, como por exemplo:

- Idade do cliente;
- Freqüência de utilização do auto-atendimento;
- Nível de relacionamento;
- Tempo de atualização cadastral;
- Entre outros tipos de seleções possíveis de agrupamento.

A finalidade deste agrupamento é evitar uma demanda elevada, que possa gerar um fluxo de cadastramento acima das expectativas e da capacidade de atendimento por parte do banco. Assim, evita-se uma imagem negativa por possíveis transtornos neste processo. Deve-se considerar que um grande banco possui mais de dez milhões de clientes e se não for adotada uma estratégia adequada para este novo projeto, as conseqüências podem prejudicar a imagem do sistema e da instituição como um todo.

6.2.4 Nível do cadastro biométrico do cliente

Um nível de cadastro biométrico pode ser estrategicamente estabelecido pelo banco. Para fins de implantação e minimização de riscos, o banco estabelece diferentes níveis em relação ao cadastramento da característica biométrica do cliente. Exemplo:

- **Nível 1** - característica biométrica cadastrada pelo cliente sem validação de um funcionário do banco;
- **Nível 2** - característica biométrica cadastrada pelo cliente com validação de um funcionário do banco;
- **Nível 3 -** característica biométrica cadastrada pelo cliente com validação e confirmação de um funcionário do banco.

O objetivo destes níveis é ter a possibilidade de gerenciar os tipos de transações que o cliente poderá realizar com a característica cadastrada. Pode-se observar que o nível 1 é sucessível a fraude de cadastramento, pois o processo é efetuado sem presença do funcionário. Desta forma, nada impede que seja cadastrada uma característica biométrica diferente da verdadeira característica do cliente. É importante o entendimento que o nível de cadastro biométrico, visa facilitar a implantação do sistema. A possível fragilidade no nível 1 é a mesma apresentada nas atuais técnicas de combate a fraude. O verdadeiro aumento da segurança se estabelece a partir do nível 2 e atingindo sua plenitude no nível 3, como será detalhado nas próximas seções.

6.2.5 Captura da identificação biométrica do cliente

Inicialmente esta captura será efetuada no próprio terminal de auto-atendimento, onde o próprio cliente utilizando seu cartão bancário e sua senha fará a captura da característica biométrica de suas veias da palma da mão. Este cadastro é efetuado sem a participação de funcionário do banco, então é atribuído o nível 1 de segurança.

6.2.6 Alteração do nível de cadastramento biométrica do cliente

A alteração do nível será efetuada de forma gradual, ou seja, o banco deve estabelecer de acordo com andamento da adesão pela tecnologia. Não sendo necessariamente

obrigatória, mas recomendada para que se atinja o grau máximo em termos de segurança, que pode ser atribuído a esta tecnologia.

Para efetuar a alteração é necessário que um funcionário valide o cadastro da característica do cliente, através de um comando no sistema, onde o cliente se identifica, apresentando seus documentos (documento de identidade válido pela legislação brasileira) e digita sua senha. Assim, o funcionário utiliza sua senha funcional para a validação do cliente, alterando para o nível 2.

O nível 3 será atribuído através de processo semelhante ao do nível 2, acrescentando que será necessário a confirmação da característica biométrica cadastrada no sistema. Isto será efetuado com a identificação do cliente, com a digitação de sua senha e com a captura de sua característica biométrica pelo devido dispositivo, que poderá ser no terminal de auto-atendimento ou na própria mesa de atendimento, se esta já estiver equipada com o leitor biométrico. Assim, o funcionário vai utilizar sua senha funcional para validar e confirmar a característica biométrica do cliente.

6.2.7 Nível de segurança da transação

O nível de segurança da transação é a ferramenta de gestão do banco para controle dos riscos relacionados ao tipo de transação e valores envolvidos na mesma. Como já foi visto anteriormente, é comum que os bancos utilizem senha por tipos de canal de atendimento e a solicitação de mais de uma senha para realização de determinada transação.

Para melhor entendimento, a tabela 6.1 apresenta um exemplo de agrupamento de transações por níveis de segurança.

Tabela 6.1 – Nível de segurança no terminal de auto-atendimento.

Nível	Limite saque	Limite transferência	Limite pagamento	Outras transações
A	200,00	200,00	200,00	Saldo e extrato de conta
B	600,00	1.000,00	1.000,00	Investimento e empréstimos
C	1.000,00	5.000,00	5.000,00	Talão de cheque
D	3.000,00	20.000,00	20.000,00	Demais transações disponíveis

A tabela 6.1 apresenta uma sugestão de limites e transações disponíveis em cada nível, sendo recomendado que o banco ajuste a mesma de acordo com sua estratégia. O banco pode adotar tabelas diferentes, conforme o perfil de relacionamento ou personalização dos limites para cada cliente, como já praticado no cenário atual.

A aplicação prática do nível de segurança da transação consiste na soma de pré-requisitos que são analisados para atingir determinado nível. Os pré-requisitos devem ser estabelecidos de acordo com grau de risco envolvido na transação.

Para melhor entendimento, a tabela 6.2 apresenta um exemplo de aplicação destes pré-requisitos relacionando com os níveis de segurança resultantes.

Tabela 6.2 – Nível do cadastro aplicado no nível de segurança do auto-atendimento.

Nível	**A**	**B**	**C**	**D**
1	(Cartão + senha) ou (Cartão + Biometria)	(Cartão + 2 senhas) ou (Cartão + senha + Biometria)	Não atinge.	Não atinge.
2	(Cartão + senha) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + 2 senhas) ou (Cartão + Biometria)	(Cartão + senha + Biometria)	Não atinge.
3	(Cartão + senha) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + 2 senhas) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + Biometria)	(Cartão + senha + Biometria)

Analisando a tabela 6.2 observa-se o sistema biométrico acrescentando maior segurança nas transações bancárias. A proposta da tabela objetiva a implantação gradual do sistema, pois como pode ser visto, o cliente poderá efetuar transações até no nível B de segurança sem a adesão da nova tecnologia. A partir do nível C é obrigatória a adesão à solução, sendo justificada pelos valores mais elevados dos limites e tipos de transações.

Verifica-se que a partir do cadastro biométrico nível 2, há a possibilidade de realizar transações bancárias sem a utilização do cartão, situação que ocorre por problemas no cartão ou por falta do mesmo, devido a circunstâncias alheias a vontade do cliente. Nesta situação o

sistema biométrico demonstra mais uma funcionalidade que é um diferencial da adesão pela tecnologia.

Cabe salientar que com a evolução da adesão e utilização da solução e depois de todo parque tecnológico do banco estar apto a efetiva utilização da biometria, esta tabela (6.2) de acordo com decisão estratégica do banco poderá ser alterada e até mesmo extinta, pois o objetivo final é que todo o cadastro biométrico do cliente atinja o nível 3.

6.2.8 Operacionalização do terminal de auto-atendimento

A operação do terminal com leitor é simples. Ao inserir o cartão no leitor, o cliente que não aderiu à solução será convidado a cadastrar-se. Aceitando a adesão, o sistema inicia o processo de cadastramento da característica biométrica pedindo que o cliente posicione a mão no leitor, então é feita a captura das características das veias da palma da mão. Com duas leituras o dispositivo estabelece o exemplar e ser armazenado. Após a captura, o cliente à valida com sua senha pessoal, e então é concluído o cadastramento da característica biométrica.

O cliente já cadastrado, ao inserir o cartão no leitor, efetuará sua transação normalmente, e de acordo com o nível de segurança necessário para sua realização. O sistema irá solicitar a colocação na mão para leitura das veias, como os demais pré-requisitos para atingir o nível de segurança solicitado. Se atingido o nível, a transação é autorizada. Caso não atenda estes pré-requisitos, o sistema orientará o cliente de como deve proceder.

A transação sem o cartão inicia-se a pedido do cliente com o toque no botão indicado. Ele digita as informações solicitadas, agência e conta, indica a transação e se autentica pela leitura das veias de palma da mão. Se o nível de segurança foi atingido será autorizada a transação, caso contrário será orientado pelo sistema como deve proceder.

6.3 Proposta de sistemas biométricos - atendimento pessoal

A implantação da utilização dos sistemas biométricos no atendimento pessoal deve ser preferencialmente implementado em conjunto com auto-atendimento, mas no caso que não seja possível, deverá ser o próximo passo do projeto. Assim, viabilizará todo o potencial que a solução pode oferecer.

Como definido no auto-atendimento, o sistema biométrico de autenticação pelas veias da palma da mão é a tecnologia escolhida para utilização no atendimento pessoal, tanto nos guichês de caixas quanto nas mesas de atendimento.

6.3.1 Implantação

Inicia-se com aquisição e instalação dos leitores nas estações de trabalho dos guichês de caixas e das mesas de atendimento. Para diminuir o impacto inicial, recomenda-se que cada ambiente de atendimento tenha pelo menos uma estação com o leitor instalado. Com a evolução do uso da técnica, o objetivo é que todas as estações de trabalho tenham o dispositivo.

6.3.2 Estimativa de custo e prazo

Segundo estudos efetuados sobre a estimativa de custo de implantação do sistema biométrico de reconhecimento pelas veias da palma da mão, tendo como fornecedor a Fujitsu e comprador um banco de grande porte, como Bradesco, Itaú e Banco do Brasil o custo médio do leitor instalado e funcionando por estação de trabalho seria:

- Estação de trabalho – compra e instalação do leitor R$ 600,00.

O prazo para instalação de no mínimo um leitor por agência é estimado em 1 ano. Para a instalação em todas as estações de trabalho do atendimento e caixa, projeta-se que seriam necessário 3 anos. Mas estes prazos dependem muito do interesse estratégico do banco, que vai estabelecer um grau de prioridade para esta etapa do projeto. A tendência é que as instalações dos leitores no atendimento pessoal, fiquem em segundo plano em relação ao sistema de auto-atendimento.

6.3.3 Agrupamento dos clientes para cadastramento

A partir da instalação do leitor biométrico na agência ou posto de atendimento bancário, todos os clientes que forem atendidos terão sua característica biométrica cadastrada.

Os atuais clientes do banco serão convidados a aderir à nova tecnologia de forma gradual. A abordagem deve ser baseada no diferencial da tecnologia e as vantagens que ela apresenta.

A finalidade deste agrupamento é evitar uma demanda elevada, que possa gerar um fluxo de cadastramento acima das expectativas e da capacidade de atendimento por parte do banco, como foi descrito na seção 6.2.3 deste trabalho. Neste caso, o agrupamento será focado em ações não só para adesão a tecnologia, mas também para atualização do cadastro biométrico do cliente para nível 3.

De acordo com agrupamento, serão enviadas mensagens para os clientes pelos mais diversos meios, como por exemplo:

- Mala direta;
- Oferta ativa nos terminais de auto-atendimento;
- Mensagem via celular;
- Contato telefônico;
- Internet banking;
- Entre outros meios de comunicação.

O objetivo é alcançar o maior número de clientes possíveis com adesão à técnica e com nível mais alto de cadastro biométrico (nível 3).

6.3.4 Nível do cadastro biométrico do cliente

O nível de cadastro biométrico no atendimento pessoal é o mesmo descrito na seção 6.2.4. A diferença é que neste tipo de atendimento não será gerado nenhum cadastro biométrico de nível 1. Pois este nível só é possível quando efetuado pelo próprio cliente no auto-atendimento.

A partir da instalação do leitor biométrico nas estações de trabalho, todos os atendimentos irão gerar apenas o nível 3 de cadastro biométrico.

6.3.5 Captura da identificação biométrica do cliente

A captura será efetuada no leitor biométrico instalado na estação de trabalho, onde após a devida identificação do cliente que apresenta sua documentação legal. O funcionário inicia processo de captura digitando os dados da conta do cliente através do aplicativo especifico, o dispositivo efetua a leitura da característica biométrica do cliente, e então este

utilizando sua senha pessoal assina eletronicamente esta operação. No mesmo processo o funcionário valida e confirma a captura com sua senha funcional, assumindo a responsabilidade pelo correto cadastramento da identificação biométrica do cliente. Este cadastro é efetuado com a participação de funcionário do banco, então é atribuído o nível 3 ao cadastro do cliente.

6.3.6 Alteração do nível de cadastramento biométrica do cliente

A alteração do nível será efetuada conforme descrito na seção 6.2.6, ou seja, somente será necessária para os clientes que ainda não tenha atingido o nível 3 do cadastro biométrico.

A operação de alteração será efetuada com a devida identificação do cliente, através de sua documentação, digitação de sua senha e captura de sua característica biométrica a qual será validada e confirmada pela senha funcional do atendente.

Outras situações que poderão ocorrer são o caso de um registro indevido onde foi identificado que a característica biométrica não pertence ao cliente cadastrado no sistema. Também deve ser previsto a possibilidade de alguma lesão física alterar a característica das veias da palma da mão do cliente. Então, por decisão administrativa, dois funcionários com cargo gerencial poderão alterar o nível ou excluir o cadastro biométrico do cliente. Assim, iniciando um novo processo de captura.

6.3.7 Nível de segurança da transação

O nível de segurança da transação é a ferramenta de gestão do banco para controle dos riscos relacionados ao tipo de transação e valores envolvidos na mesma. No atendimento pessoal existe o envolvimento de um funcionário que faz a identificação do cliente através de sua documentação, isto se soma as demais ferramentas de autenticação já apresentadas no auto-atendimento possibilitando as elevações dos limites estabelecidos para este canal.

Para melhor entendimento, a tabela 6.3 apresenta um exemplo de agrupamento de transações por níveis de segurança.

Tabela 6.3 – Nível de segurança no atendimento pessoal.

Nível	Limite saque no caixa	Limite transferência no caixa	Limite pagamento no caixa	Outras transações Atendimento Pessoal
A	1.000,00	1.000,00	1.000,00	Saldo e extrato de conta
B	5.000,00	10.000,00	10.000,00	Investimento e Talão de cheque
C	30.000,00	50.000,00	50.000,00	Demais transações disponíveis
D	100.000,00	100.000,00	100.000,00	Demais transações disponíveis

A tabela 6.3 apresenta sugestão de limites e transações disponível em cada nível, sendo recomendado que o banco ajuste a mesma de acordo com sua estratégia.

A aplicação prática do nível de segurança da transação no caixa consiste na soma de pré-requisitos que são analisados para atingir determinado nível. No caso dos pré-requisitos não serem atingidos, existe a possibilidade de um funcionário com cargo gerencial e devidamente habilitado, utilizar sua senha funcional para autorizar a transação.

A tabela 6.4 apresenta um exemplo de aplicação destes pré-requisitos relacionando com os níveis de segurança resultantes.

Tabela 6.4 – Nível do cadastro aplicado no nível de segurança no caixa.

Nível	**A**	**B**	**C**	**D**
1	(Cartão + senha) ou (Cartão + Biometria)	(Cartão + senhas + senha Gerente) ou (Cartão + senha + Biometria)	(Cartão + senha + Biometria + senha Gerente)	Não atinge
2	(Cartão + senha) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + senhas + senha Gerente) ou (Cartão + Biometria)	(Cartão + senha + Biometria + senha Gerente)	(Cartão + senha + Biometria + senha Gerente)
3	(Cartão + senha) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + senhas + senha Gerente) ou (Cartão + Biometria) ou (Digitação Agência e Conta + Biometria)	(Cartão + Biometria)	(Cartão + senha + Biometria + senha Gerente)

Analisando a tabela 6.4 observa-se o sistema biométrico acrescentando maior segurança nas transações bancárias. A proposta da tabela objetiva a implantação gradual do sistema, pois como pode ser visto, o cliente poderá efetuar transações até no nível A de segurança sem a adesão a nova tecnologia. No nível B, as transações que não tiverem a autenticação biométrica serão obrigatoriamente autorizadas por senha de funcionário habilitado, que antes de autorizar deve propor ao cliente a adesão na nova tecnologia. Caso o cliente não aceite a proposta, o gerente decide se autoriza ou não a transação. A partir do nível C é obrigatória a adesão à solução, sendo justificada pelos valores mais elevados dos limites e os tipos de transações.

Verifica-se que a partir do cadastro biométrico nível 2 a possibilidade do realizar transações bancárias no caixa sem a utilização do cartão, assim como ocorre no auto-atendimento. Isto demonstra a credibilidade do banco na tecnologia.

Deve-se informar que está tabela (6.4) apresenta parâmetros para as transações chamadas “eletrônicas”, ou seja, o cliente não assina nenhum documento para realização da operação. É importante o esclarecimento que as transações não previstas ou que estejam fora da tabela serão efetuadas dentro da regra estabelecidas nas normas do banco. Assim, o entendimento é que todos os valores acima do nível D serão efetuados através de documentos específicos assinados pelo cliente e devidamente autorizados pelo gerente, como exemplo: cheques e recibo de saques, entre outros.

6.3.8 Operacionalização do atendimento pessoal

A operação da estação de trabalho com leitor biométrico é simples. O funcionário ao identificar que o cliente não aderiu à solução, deverá ofertar o cadastramento. Aceitando a adesão, o funcionário inicia o processo de cadastramento da característica biométrica pedindo que o cliente posicione a mão no leitor, então é feita a captura das características das veias da palma da mão. Com duas leituras o dispositivo estabelece o exemplar e ser armazenado. Após a captura o cliente à valida com sua senha pessoal, e então é concluído o cadastramento da característica biométrica.

O cliente já cadastrado é identificado pelo funcionário que efetuará sua transação normalmente, e de acordo com o nível de segurança necessário para sua realização. O sistema solicitará que o cliente posicione a mão no leitor. Assim, como os demais pré-requisitos para

atingir o nível de segurança solicitado. Se atingido o nível a transação é autorizada, caso não atenda estes pré-requisitos, o sistema solicitará autorização gerencial.

A transação sem o cartão inicia-se com a identificação do cliente pelo funcionário, através dos documentos legais. Ele seleciona a transação que o cliente deseja efetuar, digita as informações da agência e conta do cliente. Solicita ao cliente que posicione a mão para captura da característica das veias de palma da mão, se o nível de segurança foi atingido será autorizada à transação. Caso contrário, o sistema solicitará autorização gerencial.

6.4 Proposta de sistemas biométricos - internet banking

A utilização dos sistemas biométricos no Internet Banking é uma proposta diferente em relação às soluções apresentadas para os terminais de auto-atendimento e o atendimento pessoal, pois nestas duas situações o ambiente e os equipamentos envolvidos são de propriedade do banco. A internet é um novo desafio, pois o ambiente de sua utilização pode ser a casa, a empresa ou outros ambientes escolhidos pelos clientes.

O sistema biométrico de autenticação pelas veias da palma da mão é a tecnologia escolhida para utilização nos terminais de auto-atendimento e no atendimento pessoal, como visto anteriormente. A mesma técnica é viável de aplicação no internet banking, em termos tecnológicos não se teria problemas, a solução pode ser implantada. Mas aqui está o desafio, o computador que o cliente utiliza está em sua casa, então precisará ter seu próprio leitor biométrico. Neste momento aparece a dificuldade da aplicação de uma única solução para todos os tipos de atendimento oferecidos ao cliente bancário.

O problema é o custo, nos pontos de atendimento do banco o custo é diluído entre os milhares de clientes que usufruirão do sistema, mas na internet não existe esta divisão. O custo do leitor fica individualizado, o que, no momento, torna inviável sua aplicação neste canal de atendimento. Todavia, não pode ser eliminada a utilização desta técnica no atendimento ao segmento corporativo, onde os clientes são as grandes empresas que efetuam transações de grandes valores, este segmento tem interesse de ambas as partes por soluções segurança e inovadoras.

Na busca por um sistema biométrico viável para implantação no internet banking, os estudos demonstraram a existência de dispositivo biométrico com leitor de impressão digital

que somado a certificação digital se torna uma ferramenta de segurança aplicável para o canal de atendimento em questão.

6.4.1 Implantação

Inicia-se com a aquisição do certificado digital tipo A-3, junto a Certisign e do *token* com leitor de impressão digital compatível com certificado. Após a devida habilitação do certificado na autoridade certificadora e instalação do certificado no *token*, o cliente deve cadastrar no site do banco. As ferramentas já existem, cabe ao banco incentivar a utilização da técnica. Apresentando ao cliente a solução e negociando com os fornecedores parceiros uma redução do custo de aquisição do certificado e do dispositivo.

6.4.2 Estimativa de custo e prazo

O custo atual de implantação pode ser reduzido com uma maior divulgação da tecnologia, cabe ao banco procurar parceiros para viabilizar a adesão:

- Custo atual - certificado validade por 3 anos R$ 165,00, dispositivo R$ 250,00, total R$ 415,00;
- Custo estimado após negociação - certificado valido por 3 anos R$ 90,00, dispositivo R$ 150,00, total R$ 250,00.

O prazo estimado para instalação é de 15 a 60 dias, devido ao tempo para habilitação da certificação que tem que ser agendado com a autoridade certificadora.

6.4.3 Agrupamento dos clientes para cadastramento

O agrupamento dos clientes, neste caso, é uma ferramenta de gestão focada na oferta desta solução. A partir da negociação com os fornecedores, o banco deve utilizar em sua estratégia o perfil dos grupos para divulgação e adesão a nova tecnologia.

Os clientes do banco serão convidados a aderir à nova tecnologia de forma gradual, estabelecendo grupos de acordo com o perfil do cliente, como por exemplo:

- Freqüência de utilização do internet banking;
- Idade do cliente;

- Nível de relacionamento;
- Entre outros tipos de seleções possíveis de agrupamento.

A finalidade deste agrupamento é atuação focada do banco para atingir o maior número de adesões possível, com o objetivo de tornar o atendimento via internet cada vez mais utilizado e mais seguro. Para o banco, o combate à fraude neste canal de atendimento é estratégico, pois além da melhora da imagem do banco, haverá uma redução de seus custos operacionais e das perdas financeiras causadas pelas fraudes realizadas pela internet.

6.4.4 Nível do cadastro biométrico do cliente

Assim, como auto-atendimento e no atendimento pessoal, um nível de cadastro biométrico pode ser estabelecido para esta tecnologia. Para fins de gestão e minimização de riscos, o banco estabelece diferentes níveis de adesão à tecnologia. Exemplo:

- **Nível 1** - adesão pelo cliente sem validação de um funcionário do banco;
- **Nível 2** - adesão pelo cliente com validação de um funcionário do banco.

O objetivo destes níveis é ter a possibilidade de gerenciar os tipos de transações que o cliente poderá realizar com o certificado cadastrado. Como o certificado é validado por autoridade certificadora, as possibilidades de fraudes são mínimas. A criação de dois níveis é para melhor gestão de risco por parte do banco, pois a principal diferença entre eles são limites de valores das transações e a obrigatoriedade no nível 2 para transações efetuadas por administradores de grandes empresas.

6.4.5 Captura da identificação biométrica do cliente

A captura será efetuada pelo próprio cliente utilizando seu computador e o *token* e sua senha, ele fará a captura da característica biométrica da impressão digital. Este cadastro é efetuado sem a participação de funcionário do banco, então é atribuído o nível 1 de cadastro biométrico.

6.4.6 Alteração do nível de cadastramento biométrica do cliente

A alteração do nível será efetuada quando demandada pelo cliente ou quando tratar-se de administrador de grande empresa cliente do banco que tenha aderido à tecnologia, neste caso, a validação é obrigatória.

Para a alteração é necessário que um funcionário valide o cadastro da característica do cliente, através de um comando no sistema, onde o cliente se identifica, apresentando seus documentos (documento de identidade válido pela legislação brasileira) e digita sua senha. Assim, o funcionário utiliza sua senha funcional para a validação do cliente, alterando para o nível 2.

No caso de administrador de empresa, cliente do banco, a solicitação da validação e, conseqüentemente, elevação do nível, poderá ser através de documento gerado pelo próprio site do banco, devidamente assinado pelos administradores da empresa. Então dois funcionários com cargos gerenciais e habilitados validarão o certificado utilizando suas senhas funcionais.

6.4.7 Nível de segurança da transação

O nível de segurança da transação é a ferramenta de gestão do banco para controle dos riscos relacionados ao tipo de transação e valores envolvidos na mesma. Como já foi visto anteriormente, é importante que os bancos utilizem estes tipos ferramenta para minimizar riscos operacionais.

Para melhor entendimento, a tabela 6.5 apresenta um exemplo de agrupamento de transações por níveis de segurança.

Tabela 6.5 – Nível de segurança no internet banking.

Nível	Limite transferência	Limite pagamento	Outras transações
A	200,00	200,00	Saldo e Extrato da Conta e Simulações
B	30.000,00	30.000,00	Todas as transações
C	50.000,00	50.000,00	Todas as transações
D	10.000.000,00	10.000.000,00	Todas as transações

A tabela 6.5 apresenta uma sugestão de limites e transações disponível em cada nível, sendo recomendado que o banco ajuste a mesma de acordo com sua estratégia. O banco pode adotar tabelas diferentes, conforme o perfil de relacionamento ou personalização dos limites para cada cliente, como já praticado no cenário atual.

A aplicação do nível de segurança consiste na soma de senha e ferramentas que tornam o acesso ao internet banking mais seguro. O certificado eleva muito esta segurança e, somado a biometria, se transforma numa ferramenta poderosa de combate as fraudes neste canal.

A tabela 6.6 apresenta um exemplo de aplicação destes pré-requisitos relacionando com os níveis de segurança resultantes.

Tabela 6.6 – Nível do cadastro aplicado no nível de segurança do internet banking.

Nível	**A**	**B**	**C**	**D**
1	(Digitação agência e conta + senha)	(Digitação agencia e conta + senhas + *token* com leitor biométrico e certificação)	Não atinge.	Não atinge.
2	(Digitação agência e conta + senha)	(Digitação agencia e conta + senhas + *token* com leitor biométrico e certificação)	(Digitação agencia e conta + senhas + *token* com leitor biométrico e certificação)	Igual ao nível C, mas só aplicado para empresas.

Na tabela 6.6 observa-se o sistema biométrico acrescentando maior segurança nas transações bancárias realizadas na internet. Verifica-se que o cliente poderá efetuar transações até no nível B sem a validação da adesão à nova tecnologia. A partir do nível C, é obrigatória a validação da adesão à solução, sendo justificada pelos valores mais elevados dos limites e tipos de transações.

Deve-se salientar que o nível D é aplicado somente para o segmento de empresas, onde normalmente as transações são autorizadas por mais de um administrador. Os valores apresentado tabela (6.5) são os limites máximos para as transações efetuadas por este canal de atendimento, este valor deve ser personalizado conforme acordo documentado entre o banco e a cliente (empresa) que estabelecerá os limites em função de suas necessidades.

6.4.8 Operacionalização do internet banking

A operação do internet banking é realizada pelo cliente que não aderiu à solução. Normalmente, neste momento o sistema verifica se é publico alvo para adesão, se for o caso, o mesmo será convidado a aderir à nova solução, sendo informado como proceder para adesão.

O cliente já cadastrado inicia sua navegação normalmente, e de acordo com o nível de segurança necessário para sua realização, o sistema pedirá o uso do certificado digital do cliente. Com a colocação do *token* e a leitura da impressão digital do cliente, o sistema verifica os pré-requisitos para atingir o nível de segurança solicitado. Se atingido o nível a transação é autorizada, caso não atenda estes pré-requisitos, o sistema orientará o cliente de como deve proceder.

Neste capítulo foi apresentada a proposta de aplicação dos sistemas biométricos nas transações bancárias. Pode-se observar que esta tecnologia acrescenta um elevado nível de segurança nas transações realizadas pelos clientes nos diferentes canais de atendimento.

CONCLUSÃO

Pode-se afirmar que os estudos realizados demonstram a possibilidade de implementação de sistemas biométricos para as mais diversas áreas, as quais necessitem de procedimento de identificação ou autenticação de indivíduos. Os vários tipos de métodos de identificações biometrias abrem inúmeras oportunidades de utilização. De acordo com o nível desejado de segurança, pode-se garantir um excelente desempenho em termos de confiabilidade. Baseado em suas características e com a escolha correta do tipo de sistema a ser utilizado, a biometria torna-se uma ferramenta importante no combate às fraudes em transações financeiras.

A biometria aplicada nas transações bancárias acrescenta em termos de segurança um novo conceito, que é a possibilidade de verificação se o indivíduo realmente é quem diz ser. Este conceito, agregado as ferramentas já utilizadas pelos bancos, reduzirão os riscos relativos a perdas em fraudes bem sucedidas. O impacto da adesão dos bancos e clientes a esta tecnologia aumentará a credibilidade de todos os tipos de atendimento ao cliente bancário. Somente com a implantação dos leitores biométricos nos terminais de auto-atendimento, já se terá uma diminuição dos crimes praticados, tanto nos terminais quanto pela internet, pois as fraudes eletrônicas normalmente sempre terminam no saque em dinheiro nestes terminais, através de uso de cartões e senhas, que são roubados e utilizados pelos criminosos. As fraudes identificadas antes destes saques, na sua maioria são passiveis de recuperação, através de devolução destes dos valores, sem prejuízo para as partes envolvidas, cliente e banco.

Entende-se que os sistemas biométricos apresentados neste trabalho demonstram-se viáveis e compatíveis com as atuais ferramentas de TI já utilizadas pelos bancos. Por este motivo o custo de implantação ficará dentro da capacidade de investimento dos principais bancos do país. O retorno deste investimento se dará pelo crescimento da utilização dos

sistemas, principalmente de auto-atendimento, com aumento da segurança e da facilidade de utilização.

A facilidade de utilização é um dos argumentos para a adesão a esta solução. Observa-se que ainda nos dias de hoje muitos clientes pedem ajuda para realização de um simples saque de seu beneficio. Isto ocorre principalmente pela necessidade de várias interações com o terminal, seleção da operação e digitação da senha. O sistema proposto simplificará esta transação, pois o cliente que recebe sua aposentadoria pelo banco, fará apenas três ações, que serão inserir o cartão, colocar a palma da mão no leitor e pegar o dinheiro no dispensador de cédulas do terminal. O processo simples e ágil da transação aumenta a aceitação e a utilização dos terminais de auto-atendimento, reduzindo as filas nos bancos.

O processo de seleção da tecnologia a ser aplicada, sem dúvida, foi um dos maiores desafios deste trabalho, pois cada tipo de sistema biométrico apresenta suas vantagens e desvantagens de acordo com ambiente, público e finalidade. Os diversos tipos de técnicas e dispositivos de captura das características biométricas tornam esta seleção muito complexa. Além disto, a evolução dos dispositivos e dos softwares aplicados nos variados sistemas biométricos acrescenta um maior nível de dificuldade na escolha, pois o que hoje é a melhor solução, amanhã já não é mais. Mas isto faz parte da área de TI, sendo a motivação de quem optou por esta área, pois estão sempre buscando soluções inovadoras.

Observa-se o crescimento da aplicação dos sistemas biométricos nas mais diversas áreas. Grandes bancos utilizando a identificação pelas veias da palma da mão, a justiça eleitoral utilizando a impressão digital para identificar o eleitor, até pequenos postos de gasolina usando ponto eletrônico com leitor biométrico. Esta percepção confirma a tendência de utilização dos sistemas biométricos que em pouco tempo estarão no dia a dia de todos.

Afirma-se que as expectativas em relação à proposta apresentada neste trabalho são positivas, pois as leituras realizadas durante a confecção deste trabalho, demonstram o imenso potencial da biometria, e assim, com a aplicação desta tecnologia poderá aumentar a segurança das transações bancárias.

Como trabalhos futuros podem ser citados a aplicação dos sistemas biométricos nas transações com cartão de débito e de crédito, realizando estudos para proposta de aplicação de umas das técnicas viáveis para implantação junto as dispositivos instalados nos

estabelecimentos que aceitam o cartão com meio de pagamento. Este é um caso de estudo que apresenta uma complexidade maior, porque não é decisão de uma única instituição e sim de um acordo entre as administradoras de cartões e as operadoras dos sistemas de cartões.

REFERÊNCIAS BIBLIOGRÁFICAS

BANCO BRADESCO S/A. Disponível em: <http://www.bradesco.com.br>. Acesso em: 12 junho 2009.

BANCO DO BRASIL S/A. Disponível em: <http://www.bb.com.br>. Acesso em: 12 junho 2009.

BARBIERI, Jose Carlos; SIMANTOB, Moysés. **Organizações Inovadoras do Setor Financeiro: Teoria e Casos de Sucesso**. Rio de Janeiro: Saraiva, 2008.

CANEDO, José Alberto Fernandes. **Terminal de Controle de Ponto e Acesso Usando Biometria e Integrado a WEB**. Goiânia: Trabalho de Conclusão. UFG, 2003.

CFSEC Security Architects. **Expectativas positivas para o mercado de biometria.** 2009. Disponível em: <http://cfsec.com.br/artigos/>. Acesso em: 31 outubro 2009.

COSTA, Luciano. **Um Modelo de Autenticação Biométrica para WEB Banking**. Florianópolis: Dissertação de Mestrado, Universidade Federal de Santa Catarina, 2007.

EL-ERIAN, Mohamed A. **Mercados em Colisão**. Rio de Janeiro: Ediouro, 2008.

FOLHA ONLINE. **Caixa eletrônico começa a exigir leitura da mão para evitar fraudes**. 2007.Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u21495.shtml.>. Acesso em 26 setembro 2009.

FOLHA ONLINE. **Impressão digital vai substituir cartão de crédito no Japão**. 2007. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u318994.shtml>. Acesso em 25 setembro 2009.

FOLHA ONLINE. **Pagamento por impressões digitais**. 2007. Disponível em: <http://www1.folha.uol.com.br/ folha/informática/ult124u336763.shtml>. Acesso em 25 setembro 2009.

FORTUNA, Eduardo. **Mercado Financeiro: Produtos e Serviços**. Rio de Janeiro: Qualitymark, 1997.

FUJITSU. **Fujitsu Wins Contract for World's First Library System Using Palm Vein Authentication Technology**. Disponível em: <http://www.fujitsu.com/global/news/pr/ archives/month/2005/20051222-01.html>. Acesso em: 07 novembro 2009.

GREENSPAN, Alan. **Epílogo Sobre a Crise Financeira**. Rio de Janeiro: Elsevier, 2008.

INFOMANIACO. **Bradesco coloca leitor biométrico em mais de 1800 agências.** Disponível em: <http://www.infomaniaco.com.br/noticias/bradesco-coloca-leitor-biomtrico-em-mais-de-1800-agncias/>. Acesso em 24 setembro 2009.

ÍRIS 1.0. **Iris Recognition & Identification System**. 2007. Disponível em: < http://pwp.net.ipl.pt/alunos.isel/24685/post1.html> . Acesso em 24 abril 2009.

KRUGMAN, Paul R. **A Crise de 2008 e o Retorno da Depressão Econômica**. Rio de Janeiro: Campus, 2009.

LAGO, André Eder da Rocha. **SIRA - Sistema de Reconhecimento de Assinaturas**. Uruguaiana: Trabalho de Conclusão. PUC RS, 2005.

PACHECO, César A. R. dos Anjos. **Autenticação com Impressão Digital**. Lisboa: Projeto Final de Graduação. ISEL, 2003.

PINHEIRO, José Mauricio. **Biometria nos Sistemas Computacionais – Você é a Senha**. Rio de Janeiro: Ciência Moderna, 2008.

PORTAL DA SEGURANÇA. **Biometria com veias**. Disponível em: <http://www.portaldeseguranca.com.br/artigos.asp?id=5831>. Acesso em 24 setembro 2009.

PRODANOV, Cleber. **Manual de Metodologia Científica**. 3ª ed. Novo Hamburgo: FEEVALE, 2003. 79p.

RIBEIRO, Sérgio Santiago. **Tecnologias de controle de acesso e sua aplicação no sistema de segurança aeroportuário**. Brasília: Monografia. Universidade de Brasília, 2008.

SÁ, Gustavo Ferreira Cardoso de. **Melhorias no Reconhecimento de Impressões Digitais Baseado no Método FingerCode**. Campinas: Dissertação de Mestrado. UNICAMP, 2006.

SANTOS, Arnaldo F. dos. **Fraudes: Prevenção a Fraudes e Golpes**. Florianópolis: Insular. 2006.

TEDESCO, Cláudia; COUTO, Daniel Lucena. **Desenvolvimento de Algoritmos para Análise de Imagens de IDS Rotacionadas Utilizando Grafos**. Salvador: Artigo. Faculdade Ruy Barbosa, 2003.

VIDIG.COM.BR. **Vai pagar com dinheiro, cartão ou DEDO?**!. 2007. Disponível em: <http://vidig.blogspot.com/2007/11/vai-pagar-com-dinheiro-carto-ou-dedo.html>. Acesso em 24 setembro 2009.

VIGLIAZZI, Douglas. **Biometria: Medidas de Segurança**. Florianópolis: Visual Books, 2006.

WOLF, Martin. **Reconstrução do Sistema Financeiro Global**. Rio de Janeiro: Campus, 2008.