UNICEUB – CENTRO UNIVERSITÁRIO DE BRASÍLIA
FAET – FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGICAS
CURSO DE ENGENHARIA DA COMPUTAÇÃO

ESTUDO DO USO DE BIOMETRIA PARA AUTENTICAÇÃO EM TERMINAIS DE AUTO-ATENDIMENTO

KLECIUS VINICIUS ASSIS CUSTÓDIO

BRASÍLIA – DF 2007

KLECIUS VINICIUS ASSIS CUSTÓDIO

ESTUDO DO USO DE BIOMETRIA PARA AUTENTICAÇÃO EM TERMINAIS DE AUTO-ATENDIMENTO

Trabalho apresentado à banca examinadora
da Faculdade de Ciências Exatas e
Tecnológicas, para conclusão do curso de
Engenharia da Computação.

Prof. Orientador: M.Sc. Marco Antônio Araújo

BRASÍLIA - DF

KLECIUS VINICIUS ASSIS CUSTÓDIO

ESTUDO DO USO DE BIOMETRIA PARA AUTENTICAÇÃO EM TERMINAIS DE AUTO-ATENDIMENTO

COMISSÃO EXAMINADORA

_____
M.Sc. Marco Antônio Araújo

_____
Maria Marony Sousa Farias Nascimento

_____
Fabiano Mariath D'Oliveira

BRASÍLIA, 28 DE JUNHO DE 2007.

Aos meus pais, irmãs e meus amigos.

Agradecimentos

Primeiramente a Deus, ao meu pai Manoel Custódio, minha mãe Juraci Maria de Assis Custódio e minhas irmãs Karina Assis Custódio e Amanda Assis Custódio.

A minha namorada Eliza C. Ferreira por sua compreensão, por me incentivar nos momentos mais difíceis e principalmente pelo seu apoio incondicional ao logo de minha vida acadêmica e profissional.

Aos meus amigos que sempre estiveram comigo nessa longa caminhada.

Ao meu colega Renato Fróes, pelo auxílio no desenvolvimento do sistema em Java.

Ao meu professor orientador M.Sc. Marco Antônio Araújo, pelo apoio e incentivo desde o “estado da arte” até a conclusão desse trabalho.

“Só existem dois dias no ano em que você não pode fazer nada pela sua vida: Ontem e Amanhã”

(Dalai Lama)

Sumário

Resumo

Neste trabalho será demonstrado como funcionam os terminais de auto-atendimento, as vulnerabilidades que os clientes/usuários deste serviço estão sujeitos. Será apresentado o que é a biometria e seus tipos de autenticações e após essa análise, visando agregar mais segurança na autenticação dos clientes, será proposto um método de autenticação, baseado no uso de biometria de impressão digital.

Este método poderá substituir os atuais cartões magnéticos utilizados pelos usuários de caixas eletrônicos por uma solução capaz de validar o cliente utilizando sua impressão digital. Com essa solução será possível aumentar o nível de segurança dos clientes que utilizam esse serviço, além de reduzir o volume de fraudes que as instituições financeiras têm nesse canal de atendimento.

A impressão digital é uma das tecnologias mais seguras para autenticação. É pouco provável que existam duas pessoas com o mesmo padrão da impressão digital ou que essa impressão seja clonada, como os cartões magnéticos.

Palavras-chave: Biometria, impressão digital, Auto-atendimento, Autenticação.

Lista de Tabelas

Lista de Figuras

Glossário

ACH - Automated Clearing House

AFIS - Automated Fingerprint Identification Systems

ATM - Automatic Teller Machine

DOC - Documento Eletrônico de Transferência

DSV - Verificação Dinâmica de Assinatura

PIN - Personal intentification number

TED - Transferência Eletrônica Disponível

1. Introdução

Com o aumento de produtos e serviços oferecidos pelas instituições financeiras tais como *internet banking* e caixas eletrônicos, surge a necessidade de agregar maior nível de segurança ao processo de autenticação nesses canais de atendimento devido ao crescente número de fraudes aplicadas nesses serviços.

As instituições financeiras estão pesquisando outros métodos de autenticação em caixas eletrônicos para substituir os atuais cartões magnéticos e o uso de um número pessoal de identificação – PIN que atualmente é o que está disponível para seus clientes.

Uma das técnicas pesquisadas é o uso da biometria que utiliza características biológicas e comportamentais que são únicas a cada indivíduo para autenticar uma pessoa baseado em suas características como voz, íris veias das mãos e a impressão digital.

Esta técnica apresenta a vantagem de usar as características do indivíduo sem necessidade de possuir objetos ou memorizar algo. O indivíduo é autenticado por aquilo que é.

1.1 Objetivos

O objetivo geral desta monografia é apresentar uma nova forma de acesso a serviços de caixa eletrônico baseado na utilização de leitura biométrica da impressão digital por clientes de instituições financeiras. Com isso pretende-se mostrar a utilização da biometria como alternativa ou complemento à tecnologia de cartões magnéticos e senhas atualmente adotada pelos bancos.

Para atingir os objetivos gerais os seguintes objetivos específicos devem ser alcançados:

- Apresentar o funcionamento e a forma de autenticação utilizada atualmente em ATM;

- Apresentar as vulnerabilidades nos ATM para os usuários desse serviço;

- Apresentar o estado da arte sobre biometria e os tipos de autenticação biométrica;

- Implementar uma solução que simule o acesso ao serviço de caixa eletrônico de um banco qualquer com a utilização de biometria, no caso a impressão digital.

1.2 Motivação

Atualmente os bancos contam com vários canais para transações, além das agências físicas. Porém, o mais procurado são os terminais de auto-atendimento, que processaram no ano passado de 2006, 12 bilhões de operações, muito acima dos volumes registrados pelo call center, Internet Banking e correspondentes bancários [FEBRABAN, 2007].

Com aumento desses canais, está caindo o número de correntistas que vão às agências físicas dos bancos. Em 2000, elas respondiam por 22,1% das transações financeiras e no ano passado a participação das agências ficou em 10,4% [FEBRABAN, 2007].

O número fraudes bancárias e eletrônicas cresceu vertiginosamente em todo o Brasil no segundo trimestre de 2006. De acordo com dados do Grupo de Resposta a Incidentes para a Internet Brasileira, mantido pelo Comitê Gestor da Internet, o crescimento foi de 259% em relação ao trimestre anterior, passando de 2.213 para 7.942 notificações de fraudes. Na comparação com o mesmo período do ano anterior, o aumento chegou a 1313% [FEBRABAN, 2007].

O prejuízo provocado pelo uso de mecanismos conhecidos como "chupacabras", que clona cartões e roubam dados, é milionário. De acordo com Jair Scalco, diretor setorial da área de Cartões e Negócios Eletrônicos da Federação Brasileira de Bancos (Febraban), somente neste ano, os bancos brasileiros tiveram um prejuízo de R$ 300 milhões com estes tipos de crime.

2. Terminais de Auto-Atendimento

Uma maquina de automação de caixa (ATM – *Automatic Teller Machine*) ou terminal de Auto-Atendimento é um dispositivo eletrônico computadorizado que permite aos clientes de instituições financeiras tem acesso a serviços bancários como retirada de dinheiro, extratos de conta e outros, sem a necessidade de ir à um caixa humano em uma agencia. Muitos ATMs também permitem que os clientes realizem depósitos em dinheiro ou cheques, transferências entre contas correntes pagamentos e até empréstimos [IESNA, 1997].

2.1 Histórico

O ATM foi de desenvolvido e construído por Luther George Simjian e instalado em 1939 em Nova York pelo banco de Nova York, mas foi removido após 6 meses devido a falta de aceitação dos clientes [IESNA, 1997].

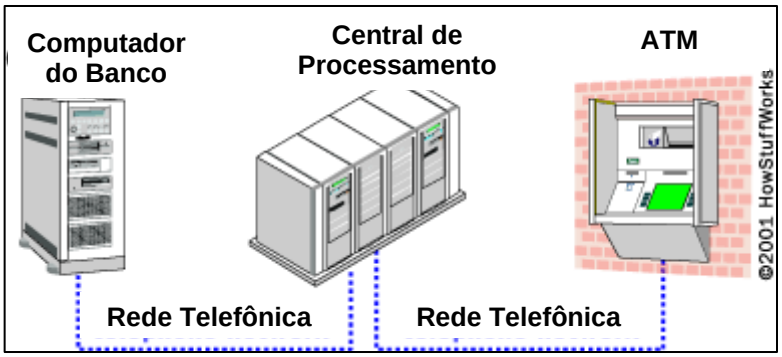
Depois disso, a história dos ATMs parou por 25 anos, até que De La Rue desenvolveu o primeiro ATM eletrônico, que foi primeiramente instalado na cidade de Enfield em Londres em 1967 pelo banco *Barclays Bank* [IESNA, 1997].

Os primeiros caixas eletrônicos aceitavam apenas uma ficha ou cupom de uso único, que era retida pelo caixa. Essas trabalhavam em vários princípios como radiação e magnetismo de baixa coercitividade[1] que era retirado pelo leitor de cartão para tornar fraudes mais difíceis [IESNA, 1997].

A idéia de um número de identificação pessoal (PIN) armazenado no cartão em si ao invés de ser digitado quando se queria retirar o dinheiro foi desenvolvido pelo engenheiro britânico James Goodfellow em 1965, que ainda possui patentes internacionais cobrindo esta tecnologia [IESNA, 1997].

[1] A intensidade do campo magnético externo que deve ser imposta a uma substância ferromagnética para lhe anular a magnetização; força coerciva – Dicionário Aurélio.

Um ATM é simplesmente um terminal de dados com dois dispositivos de entrada e quatro de saída. Como a maioria dos outros terminal de dados, o ATM tem que se conectar, e se comunicar, através de uma central de processamento. Uma central de processamento é análogo a um Provedor de Serviços de Internet (ISP) no sentido em que ele é um portal através do qual todas as várias redes do ATM se tornam disponíveis ao usuário (a pessoa que está esperando pelo dinheiro).



Fonte: HowStufWorks

Figura 1 – Topologia de funcionamento de um ATM.

A maioria das centrais de processamento podem suportar tanto *leased-line* (linhas alugadas) quanto dial-up (linhas discadas). Máquinas *leased-line* se conectam diretamente a central de processamento por meio de uma linha de telefone dedicada, ponto a ponto, de quatro fios. ATMs Dial-up se conectam a central de processamento por meio de uma linha telefônica normal utilizando um modem ou através de um servidor de Internet usando um número de acesso local discado por um modem [16].

ATMs *leased-line* são preferidos por causa de sua capacidade *throughput* , e ATMs dial-up são preferidos onde o custo tem maior impacto do que o *throughput*. O custo inicial de uma máquina *dial-up* é menos que a metade de uma máquina *leased-line*. Os custos mensais de operação de um terminal *dial-up* são apenas uma fração dos custos de um *leased-line* [16].

Uma central de processamento pode ser adquirida por um banco ou instituição financeira, ou pode ser adquirido por um provedor de serviços independente. Os processadores bancários normalmente suportam apenas

máquinas bancárias, assim como processadores independentes suportam máquinas comerciais [16].

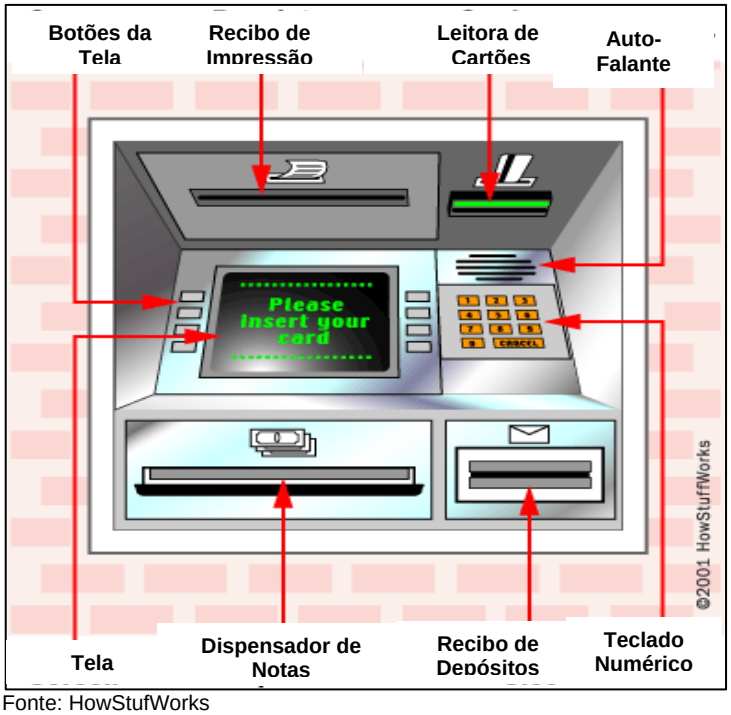
Há dois tipos principais de ATMs, são eles:

- Dispositivo Mono-função, que permite apenas um tipo de transação, por exemplo, consulta somente saques, ou somente extratos. [IESNA, 1997]

- Dispositivos Multi-função, que realizam múltiplos serviços como, depósitos, imprimir extratos, realizar saques. Sendo todos executados numa mesma máquina. [IESNA, 1997]

2.2 Partes de um ATM

Atualmente um ATM possui dois dispositivos de entrada que são a leitora de cartão e o teclado que pode ser numérico ou alfa-numérico e quatro dispositivos de saída que são o auto-falante, o monitor, a impressora e dispensador de notas. Abaixo segue a descrição de cada dispositivo em um ATM [16].



Fonte: HowStufWorks

Figura 2 - Dispositivos de um ATM.

Um ATM tem dois dispositivos de entradas:

Leitora de Cartões: A leitora de cartões captura as informações da conta armazenadas na tarja magnética que estão na parte de trás dos cartões de débito ou de crédito. A central de processamento usa esta informação para direcionar a transação ao banco do usuário [16].

Teclado numérico – O teclado numérico permite que o usuário indique ao banco que tipo de transação ele quer realizar (retirada de dinheiro, conferência de extrato, etc.) e qual quantia. Além disso, o banco pede seu número pessoal de identificação (PIN – senha) para verificação [16].

Um ATM possui quatro dispositivos de saída:

Alto-falante – O auto-falante proporciona ao usuário uma resposta quando uma tecla é pressionada.

Tela de exibição – A tela de exibição exibe ao usuário cada passo do processamento da transação. Máquinas *leased-line* comumente usam um monitor CRT (Tubo de raios catódicos) monocromático ou colorido. Máquinas dial-up usam comumente um LCD monocromático ou colorido.

Recibo de Impressão – O recipiente de impressão provê o usuário com um papel contendo a transação.

Dispensador de Notas: O coração de um ATM é o armazenamento de dinheiro e o mecanismo de dispensa de notas. O fundo da maioria dos pequenos ATM é formada pelo recipiente que contém o dinheiro.

Sensor de Notas

O mecanismo de dispensa de notas possui um olho elétrico que conta cada nota que existe no dispensador. A contagem de notas e todas as informações pertinentes a uma transação particular são gravadas em um recibo. A informação do recibo é impressa periodicamente e uma cópia das transações é mantida no disco rígido pelo proprietário da máquina por dois anos. Sempre que o usuário tem dúvidas sobre uma transação, ele (a) pode

pedir um extrato com o demonstrativo da transação, e então pode contatar a central de processamento. Se não for possível imprimir o extrato, o usuário precisa notificar o banco ou instituição que forneceu o cartão e preencher um formulário que será enviado por fax à central de processamento. É responsabilidade da central de processamento resolver a questão [16].

Além do olho elétrico que conta cada nota, o mecanismo de dispensa de notas também possui um sensor que avalia a espessura de cada nota. Se duas notas são selecionadas juntas, em vez de serem dispensadas ao usuário elas são direcionadas a uma bandeja de rejeição. A mesma coisa acontece com uma nota que é excessivamente gasta, rasgada ou dobrada [16].

Fonte: HowStufWorks

Figura 3 – Dispensor de notas.

O número de notas rejeitadas também é gravado, assim o proprietário da máquina pode estar atento à qualidade das notas que são colocadas dentro da máquina. Uma alta taxa de rejeição pode indicar um problema com as notas ou com o mecanismo de dispensa [16].

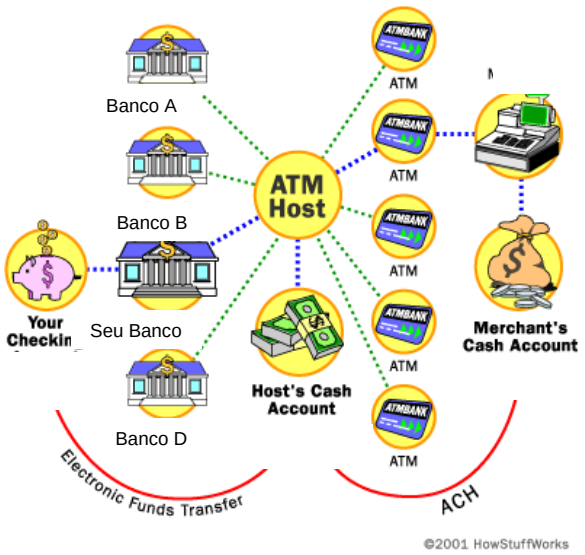
ATMs para o Deficiente Visual

Existem ATMs que são acessíveis para cegos e para pessoas deficientes visuais. Essas máquinas são localizadas em quiosques. E os teclados numéricos nos ATMs são equipados com braile [16].

Fonte: HowStufWorks

Figura 4 – Teclado numérico com braile.

Quando um usuário quer fazer uma transação num terminal de auto-atendimento, ele provê a informação necessária por meio do leitor de cartão e do teclado numérico. O ATM encaminha esta informação a central de processamento, que encaminha a transação requerida ao banco do usuário ou instituição que forneceu o cartão. Se o usuário está solicitando dinheiro, a central de processamento realiza uma transferência eletrônica de fundos para tirá-lo da conta bancária do cliente e passá-la à conta bancária da central de processamento. Uma vez os fundos transferidos à conta bancária da central de processamento, é enviado um código de aprovação ao ATM autorizando a máquina a dispensar o dinheiro. Desta forma, o comerciante é reembolsado de todos os fundos dispensados pelo ATM [16].



Fonte: HowStufWorks

Figura 5 - Um ATM independente pode acessar qualquer banco.

Então, quando você solicita dinheiro, o dinheiro se move eletronicamente da conta do usuário para a conta do comerciante.

Transferências ACH

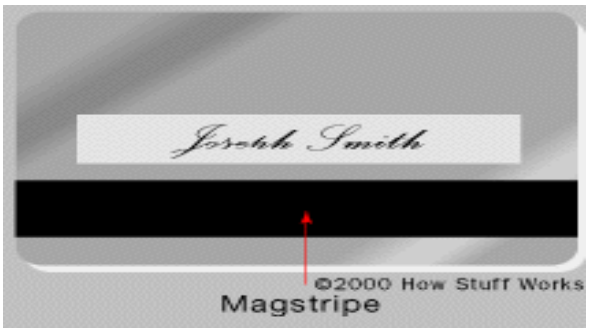
"ACH" é a sigla para "limpeza automática da casa". Esta terminologia bancária significa que uma pessoa ou empresa está autorizando outra pessoa ou empresa a fazer retirada de uma conta. É comum para academias e outros negócios ACH (debitar) uma taxa de associação mensal da conta de seus membros, e muitos pequenos negócios usam ACH (débitos) para o depósito direto de pagamentos [16].

Como funciona a tarja magnética da parte de trás dos cartões

A tarja na parte de trás de um cartão de crédito é uma tarja magnética, frequentemente chamada de *magstripe*. A tarja magnética é feita por finas partículas magnéticas a base de ferro em uma espécie de filme plástico. Cada partícula é na verdade uma fina barra magnética com comprimento a cerca de 20 milionésimos de polegada [16].

Fonte: HowStufWorks

Figura 6 – Números do Cartão.



Fonte: HowStufWorks

Figura 7 – Tarja magnética de um cartão e local para assinatura.

A tarja magnética pode ser “escrita” porque as finas barras magnéticas podem ser magnetizadas tanto na direção do pólo norte quanto do sul. A tarja magnética na parte de trás dos cartões é muito parecida com uma parte de fita cassete colada na parte de trás do cartão [16].

Funcionamento

Em vez do motor que move a fita para que ela seja lida, sua mão exerce o movimento quando você “passa” um cartão de crédito através do leitor ou o insere o cartão na leitora de cartões [16].

Existem três trilhas na tarja magnética. O comprimento de cada trilha é 0,110 polegadas. A norma ISO/IEC 7811, que é utilizada pelos bancos. Um cartão de crédito tipicamente usa apenas as trilhas um e dois. A trilha três é uma trilha de leitura/gravação (que inclui uma senha criptografada, código do país, unidade local, quantidade autorizada), mas este uso não é padronizado entre os bancos [16].

Depois que se desliza o cartão de crédito no leitor, o software de Captura Eletrônica de Dados (CED) no terminal do ponto de venda (POS) disca um número de telefone armazenado, via modem, para chamar uma autenticadora. Uma autenticadora é uma organização que coleta autenticações de crédito solicitadas por comerciantes e provê uma garantia de pagamento ao comerciante [16].

Quando a companhia de autenticação obtém a solicitação de autenticação de cartão de crédito, ela checa a transação para validação e a grava na tarja magnética por:

* ID do comerciante
* Número válido do cartão
* Data de expiração
* Limite do cartão de crédito
* Uso do cartão

Transações *dial-up* são processadas à 1200-2400 bps. Neste sistema o usuário insere um número de identificação pessoal (PIN, senha), usando um teclado numérico [16].

Se o ATM não está aceitando o cartão, problema provavelmente estará em:

Tarja magnética suja ou riscada.

Tarja magnética apagada, a causa mais comum de tarjas magnéticas apagadas é a exposição a ímãs, como aqueles pequenos usados para segurar recados ou fotos nas geladeiras.

2.3 Métodos de Autenticação

A identificação de um usuário e sua autenticação com segurança são premissas básicas para uma instituição financeira permitir o acesso por parte de seus clientes ao seu serviço de auto-atendimento. A identificação diz a um sistema quem você é, enquanto que a autenticação provê mecanismo eficiente de provar que você realmente é quem diz ser [LEONCIO, 2006].

Por isso, a autenticação precisa ser feita com base em alguma característica que somente o usuário identificado seja capaz de fornecer. As principais formas de validação de autenticidade são baseadas nos seguintes conceitos:

- “Algo que você sabe”;
- “Algo que você tem”;
- “Algo que você é”.

Dependendo da finalidade a que se destina e do nível de segurança que se requer para uma aplicação, cada um desses métodos apresenta vantagens e desvantagens.

2.4 Algo que você sabe

O exemplo mais comum neste caso é o uso de senhas ou PINs, como as senhas para acesso à caixa postal de e-mail, senhas bancárias, senhas utilizadas no local de trabalho para se obter acesso a determinado sistema, etc. Apesar de ser o método de autenticação mais usado e mais antigo, ele contém uma série de deficiências que não o torna muito confiável. A principal é que ele se baseia na capacidade dos usuários de memorizar inúmeras senhas, quase sempre de tamanhos e características diferentes. Além do mais, como a maioria das pessoas não tem muita imaginação na hora de criar as senhas, até para evitar esquecê-las facilmente, acabam por criá-las com características de fácil dedução, como nomes, sobrenomes, números de documentos, placas de carros, número de telefones e datas. Outro motivo é que essas senhas podem ser facilmente obtidas por pessoas mal intencionadas com o objetivo de tentar se autenticar como se fossem o titular da senha. Como vantagem para a utilização de senhas, pode-se destacar o baixo custo da sua implementação, pois pode ser usada em qualquer tipo de ambiente, sem a necessidade de hardwares especiais [LEONCIO, 2006].

2.5 Algo que você tem

Para “algo que você tem”, o exemplo mais conhecido é o uso de cartões magnéticos. Os sistemas de autenticação que se baseiam neste método, utilizam cartões ou *tokens* para validar seus usuários. Os clientes de bancos, para utilizar os terminais de auto-atendimento no acesso a sua conta-corrente,

são obrigados a utilizar um cartão associado a uma senha previamente cadastrada. Esses sistemas baseiam-se no fato de que apenas o titular de determinado cartão é quem vai utilizá-lo. As desvantagens desse método são:

- Os cartões podem ser facilmente perdidos ou roubados (devido ao seu pequeno tamanho)
- É caro e precisa de hardware especiais para ler os cartões.

O ponto positivo desse método, se comparado àquele que utiliza somente senhas, é que ele agrega maior nível de segurança às transações, pois considera o uso de cartão e senha ao mesmo tempo. Diante disso, uma pessoa mal intencionada agora precisa, além da senha, também do cartão para poder se passar por alguém [LEONCIO, 2006].

2.6 Algo que você é

O método de autenticação baseado em “algo que você é” está relacionado a biometria. A biometria torna possível autenticar um indivíduo a partir de alguma de suas características intrínsecas. Entre todos os métodos de autenticação biométricos atualmente existentes, o mais utilizado é a impressão digital. Outras técnicas de biometria também em uso são: Face, Geometria da mão, Íris, Retina e Voz [LEONCIO, 2006].

A grande vantagem da autenticação por meio de dispositivos biométricos é o fato de ser possível identificar o usuário sem a necessidade deste ter que memorizar senhas ou utilizar cartões.

A principal desvantagem é que seu uso depende da aquisição de hardwares especiais para capturar as informações dos indivíduos.

3. Riscos dos usuários e vulnerabilidades do ATM

Os principais riscos que um usuário de ATM sofre são os golpes que pessoas mal intencionadas aplicam que vão desde burlar os ATMs à se passar por funcionário do banco. A seguir segue uma descrição dos principais golpes aplicados nesses usuários:

Golpe do cartão engolido

O golpista, usando um produto aderente, faz com que o cartão magnético do banco utilizado pela vítima fique preso no caixa eletrônico. O estelionatário fica à distância, observando a vítima digitar a senha do cartão. Após várias tentativas, a vítima desiste de usar a máquina e deixa o cartão. O golpista retira o cartão e saca todo o dinheiro disponível na conta corrente [SERASA, 2007].

Golpe do cartão eletrônico

Envolve muita preparação dos golpistas. Em primeiro lugar, eles colocam no caixa eletrônico um dispositivo que prende o cartão magnético do cliente. Logo depois, os estelionatários esperam a vítima. Um deles fica em frente ao caixa eletrônico e coloca um aviso, com o logotipo do banco e o telefone para informações. A vítima, ao ver seu cartão retido, pede informações ao golpista. Esse afirma que o caixa deve estar com defeito, pois foi colocado um aviso do lado de fora da cabine. A vítima decide usar o telefone e é atendida por outro estelionatário, o qual se faz passar por funcionário do *telemarketing* do banco. A vítima fornece dados como o número da sua conta e a sua senha numérica e é orientada a procurar uma agência bancária para formalizar o extravio do cartão. Com a senha e o cartão em mãos, os golpistas sacam o dinheiro da conta [SERASA, 2007].

Fonte: SERASA

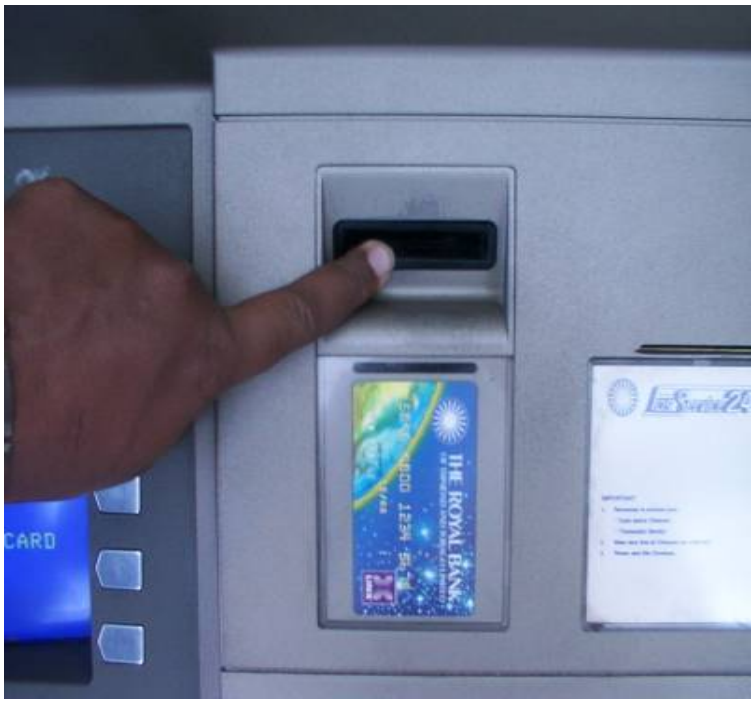
Figura 8 – Material utilizado para reter o cartão no ATM.

O material é feito de papel de radiografia (raio-X). Por ter uma coloração escura e por se parecer com o mesmo material utilizado onde se introduz o cartão nos caixas eletrônicos.

Fonte: SERASA

Figura 9 – Material introduzido da leitora de cartão.

O dispositivo é colocado na abertura onde se introduz o cartão magnético, deixando para fora uma pequena ponta do dispositivo para que ele fique preso e não seja totalmente engolido pela máquina.



Fonte: SERASA

Figura 10 – Material imperceptível no ATM.

Uma vez que as pontas são presas no caixa torna-se imperceptível ao cliente.

Fonte: SERASA

Figura 11 – Como o cartão é retido no leitor de cartão.

São feitos cortes em ambos os lados do dispositivo para ter certeza que o cartão ficará preso dentro do caixa eletrônico.

Fonte: HowStufWorks

Figura 12 – Retirando o cartão retido.

Uma vez que o cliente foi embora, o fraudador poderá despregar as pontas do dispositivo inserido na máquina e retirar o cartão da vítima.

Recadastramento bancário

Esse é realizado por telefone. O golpista liga para a vítima e diz ser representante do banco no qual ela possui conta. Na conversa, o estelionatário induz o correntista a fazer seu recadastramento bancário, digitando os números da sua agência, da sua conta e da sua senha. Com equipamentos capazes de identificar os sinais sonoros dos números digitados, os golpistas conseguem ter acesso a essas informações e sacar o dinheiro da vítima [SERASA, 2007].

Em um Hipermercado, na Barra da Tijuca, Rio de Janeiro, havia um quiosque do Banco Bradesco Dia e Noite alterado para que fosse realizada a clonagem dos cartões dos clientes que utilizavam aquele terminal. Para clonar o cartão magnético do banco, foi montado um dispositivo adicional de leitura sobreposto à leitora verdadeira:

Fonte: http://www.fraudes.org

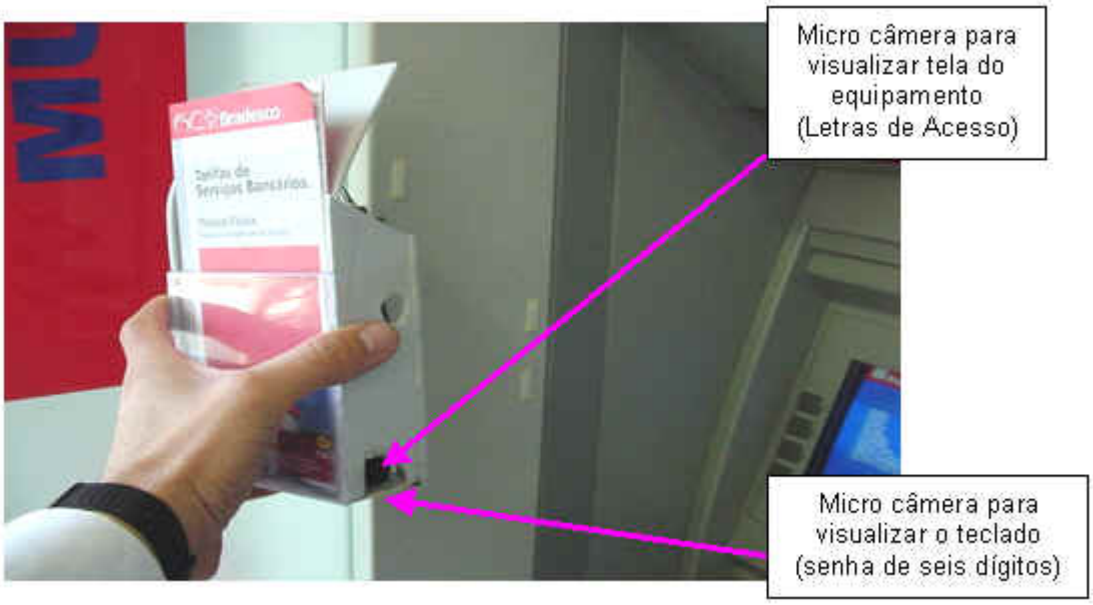
Figura 13 – Dispositivo sobreposto ao leitor de cartão.

A leitora adicional de cartões fica bem disfarçada sobre a leitora original da ATM:

Fonte: http://www.fraudes.org

Figura 14 – Dispositivo após instalado.

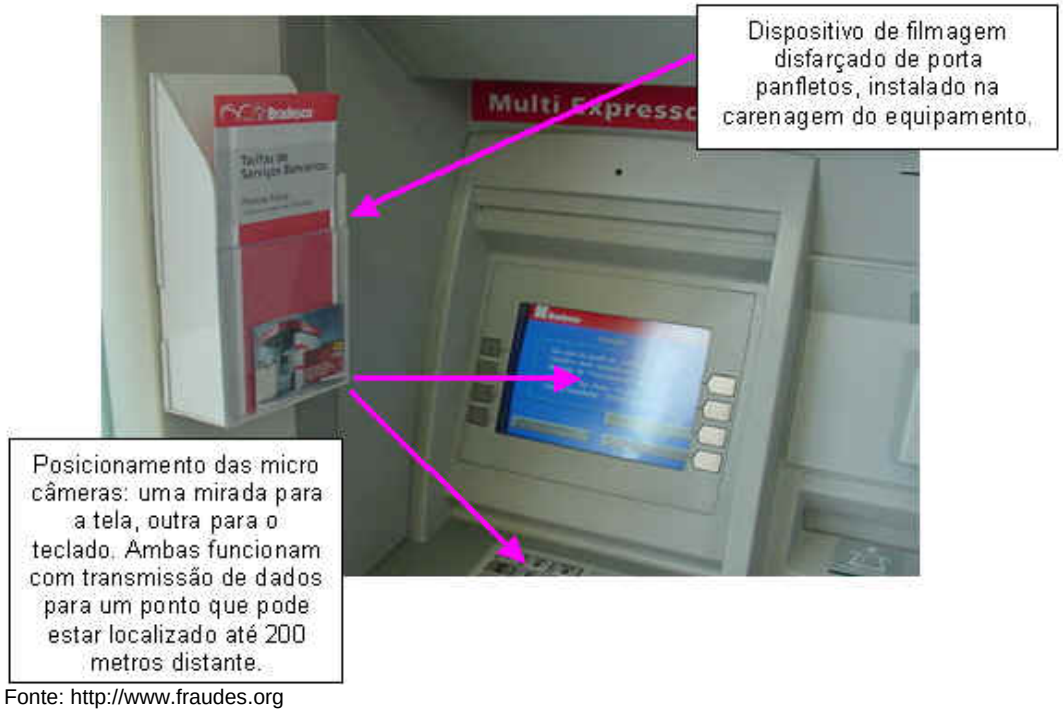
De posse do cartão clonado, os malfeitores precisam capturar as senhas, o que é feito graças a duas câmeras instaladas em um falso porta-panfleto que, na verdade, não faz parte da configuração original do quiosque.



Fonte: http://www.fraudes.org

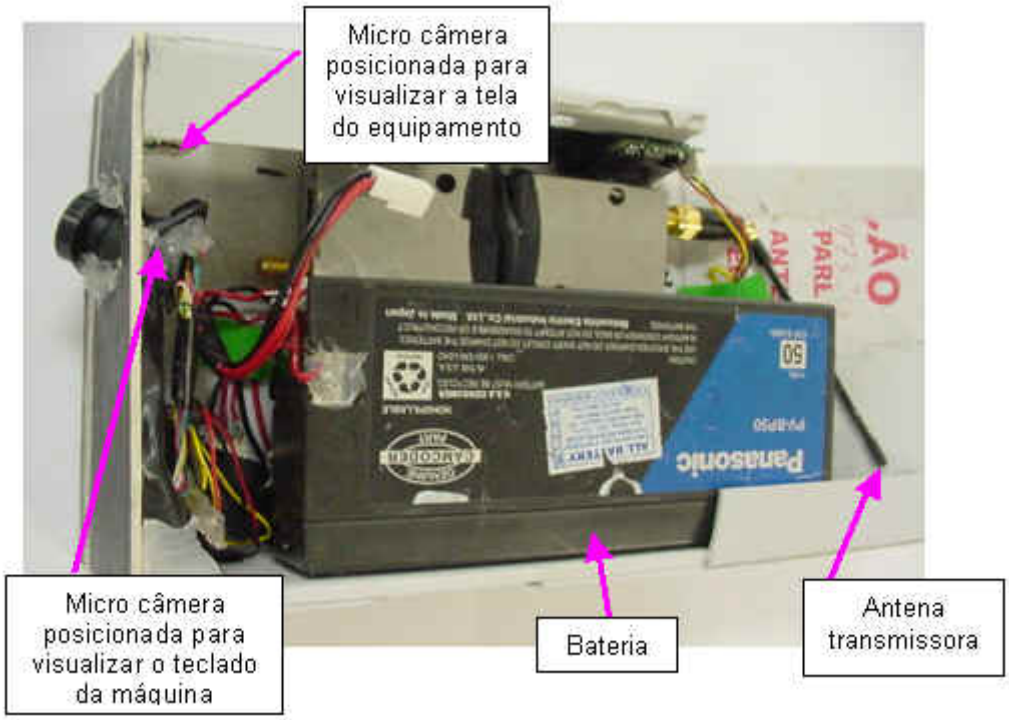
Figura 15 – Micro câmera instalada no porta-panfleto.

Usando velcro, fica assim o falso porta-panfleto instalado na carenagem do ATM.



Fonte: http://www.fraudes.org

Figura 16 – Disposição das câmeras.



Fonte: http://www.fraudes.org

Figura 17 – Micro câmeras dentro do porta-panfleto.

O mais recente golpe aplicado é o da digitação invertida da senha do usuário no ATM para acionar a polícia. A Federação Brasileira de Bancos - Febraban esclarece que é improcedente e falsa a lenda urbana divulgada por um *spam* que circula na internet,

Tal expediente, divulgado por meio de *spam*, é tecnicamente improvável. Para utilizar com maior segurança os meios eletrônicos de pagamento, a Febraban recomenda os seguintes cuidados:

1. Ao digitar sua senha, mantenha o corpo próximo à máquina, para evitar que outros possam vê-la ou descobri-la pelo movimento dos dedos no teclado. As pessoas atrás de você devem respeitar as faixas de segurança;

2. Prefira utilizar os caixas automáticos instalados em locais de grande movimentação e, se possível, em ambientes internos (shoppings, lojas de conveniência, postos de gasolina etc.);

3. Sempre que possível, faça seus saques no horário comercial, quando o movimento de pessoas é maior, evitando o período noturno. Quando precisar realmente sacar dinheiro à noite, leve um ou mais acompanhantes adultos para que fiquem fora da cabine, como se estivessem na fila;

4. Nunca aceite ou solicite ajuda de estranhos, mesmo que não lhe pareçam suspeitos;

5. Esteja atento à presença de pessoas suspeitas ou curiosas no interior da cabine ou nas proximidades. Na dúvida, não faça a operação;

6. Caso não consiga concluir uma operação, aperte a tecla ANULA ou CANCELA;

7. Em caso de retenção do cartão no caixa automático, aperte a tecla ANULA ou CANCELA e comunique-se imediatamente com o banco. Tente utilizar o telefone da cabine para comunicar o fato. Se ele não estiver funcionando, pode tratar-se de tentativa de golpe. Nesses casos, nunca aceite ajuda de desconhecidos, mesmo que digam trabalhar no banco, nem digite senha alguma na máquina;

8. Não se preste a receber créditos de pessoas desconhecidas em sua conta. Propostas desse tipo são feitas por golpistas, nas proximidades de caixas automáticas e de agências;

Evite usar datas de nascimento, iniciais, número de casa ou número de telefone.

Fique diretamente em frente do teclado numérico do ATM quando você estiver digitando sua senha (PIN). Isto previne que qualquer pessoa que esteja esperando para usar a máquina veja sua informação pessoal.

Se alguém ou alguma coisa deixá-lo inconfortável, cancele sua transação e deixe a máquina imediatamente. Contate seu banco para se

certificar de que a transação foi cancelada e avise o banco caso haja alguma pessoa suspeita.

Muitos comerciantes varejistas fecham suas lojas à noite. É fortemente recomendável que eles retirem o dinheiro das máquinas quando fecharem, assim como fazem com seus caixas registradores, e deixem a porta do compartimento de segurança totalmente aberta do mesmo modo que fazem com a gaveta vazia de um caixa-registrador. Isto deixa óbvio a qualquer pessoa que possa querer roubá-lo de que hoje não é “dia de pagamento”.

Fonte: HowStuffWorks

Figura 18 - Máquina ATM pública bem iluminada

Por razões de segurança, usuários de ATM devem buscar uma máquina que esteja localizada em um lugar público bem iluminado. Lei federal exige que apenas os últimos quatro dígitos do número da conta do usuário seja impresso no extrato de transações para que, caso o extrato seja esquecido na máquina, o número da conta está seguro. Contudo, a digitação de seu número de identificação pessoal com quatro dígitos (senha – PIN) no teclado numérico deve ainda ser protegida de observação, que pode ser conseguida pelo posicionamento da mão e corpo de forma que a senha não possa ser registrada por câmeras ou empregados de lojas. A senha (PIN) do usuário não é registrada no extrato, mas o número da conta é.

4 Biometria e Tipos de Autenticação Biométrica

A biometria é um grupo de tecnologias em segurança de alto nível. O elemento chave dessa tecnologia é sua habilidade em estabelecer identidades e reforçar a segurança. Este é um ponto extremamente importante no nosso mundo atual. Aviões, bancos, presídios, redes de computadores, sistemas de pagamento e até mesmo o processo de votação são todos suscetíveis à brechas de segurança. A biometria é agora ativa nessas diversas áreas e está indo além dos mercados tradicionais de segurança e de forças policiais, nos quais a indústria primeiramente se fez conhecer.

Mais do que um sistema que proporciona segurança e rapidez para quem utiliza, é um mecanismo que não permite fraudes. Trata-se de uma ciência de identificação baseada na medição precisa de traços biológicos. A tecnologia serve como uma barreira entre os dados das organizações e o acesso não autorizado [SERPRO, 2007].

Atualmente, existem diversos aparelhos biométricos que realizam a identificação de características humanas por meio de escaneamento da impressão digital, reconhecimento da íris e voz, verificação da assinatura e geometria das mãos. Essas tecnologias permitem aos usuários, sejam eles agências do governo, bancos, comerciantes ou trabalhadores, terem um extraordinário controle sobre as transações e confiança nas informações, sem que isto traga nenhum constrangimento para clientes ou empregados [SERPRO, 2007].

A identificação biométrica acontece em duas fases: na primeira o usuário é registrado no sistema, permitindo a captura de suas características que são convertidas em um modelo que as representa matematicamente. A segunda fase é a autenticação, na qual o usuário apresenta suas características biométricas que são comparadas e validadas com o modelo armazenado [SERPRO, 2007].

Ambientes que necessitam de alta segurança encontraram na biometria sua fonte de maior confiança no controle de acesso físico.

O número de fraudes no comércio eletrônico cresce a todo momento, tornando a utilização de sistemas mais avançados uma necessidade urgente. Cartões magnéticos com senhas não são mais confiáveis e é esperado que sejam substituídos pelos mundialmente reconhecidos *smart cards*, um dispositivo de alta segurança capaz de guardar dados biométricos para a identificação do usuário. No ato da compra, a pessoa pode assinar digitalmente suas transações com um certificado presente no cartão. A validação se dará apenas mediante identificação biométrica, por meio da impressão digital. Dessa forma, aplicações bancárias, via internet ou mesmo em postos de vendas, poderiam oferecer muito mais segurança e os prejuízos com as fraudes seriam substancialmente reduzidos.

Em muitos filmes, vemos psicopatas que decepam os dedos ou arrancam a retina da vítima para ter acesso a salas restritas ou contas de banco. E isso não é um ato exclusivo da ficção. No caso de um leitor biométrico não ter recursos de rejeição à ausência de sinais vitais, um dedo pode ser cortado e utilizado para fazer a autenticação, assim como a cabeça de um indivíduo. Existem casos em que é menor a chance de essa ação acontecer. Por exemplo, em leitores de retina. Se um olho for retirado de uma pessoa para ser usado em um sistema de leitura de retina ou reconhecimento da íris, dificilmente será bem-sucedido, uma vez que o processo depende de uma análise dos vasos sanguíneos do fundo do olho [SERPRO, 2007].

A utilização da biometria é um processo cada vez mais maduro e evoluiu muito nos últimos cinco anos. Com isso, o custo da tecnologia está caindo e viabilizando novos projetos. O sucesso de cada projeto depende da aceitação do usuário do sistema e da quantidade de falhas produzidas na autenticação [SERPRO, 2007].

4.1 Biometria

O termo abrangente “biometria”, por si, refere-se a uma ciência, envolvendo a análise estatística de características biológicas. Quando falamos sobre biometria, entretanto, estamos tratando de tecnologias que analisam as características humanas para fins de segurança. A ciência estatística da

biometria continua como pano de fundo e deverá ser tratada separadamente. Uma definição longa, porém conclusiva da biometria como segurança tem sido divulgada há anos, e diz o seguinte:

A biometria é uma característica única mensurável ou um traço do ser humano que automaticamente reconhece ou verifica sua identidade [www.consultoresbiometricos.com.br].

Portanto, as tecnologias biométricas são concernentes às partes físicas do corpo e aos traços pessoais dos seres humanos. É importante notar o termo “automático” na definição acima. Isso significa principalmente que a tecnologia biométrica deve reconhecer ou verificar uma característica humana rápida e automaticamente [www.consultoresbiometricos.com.br].

No desenvolvimento de sistemas de identificação biométricos, são necessárias características físicas e comportamentais para o reconhecimento, que são:

- Tão únicas quanto possível, ou seja, um traço idêntico jamais aparecerá em duas pessoas: singularidade;
- Existem em tantas pessoas quanto possível: universalidade;
- Podem ser medidas com instrumentos técnicos simples: mensurabilidade;
- São fáceis e confortáveis de serem medidas: uso amigável

Os sistemas biométricos são uma evolução natural dos sistemas manuais de reconhecimento amplamente difundidos há muito tempo, como análise grafológica de assinaturas, a analise de impressões digitais e o reconhecimento da voz [CLAUDIA, 2003].

4.2 Histórico da Biometria

De um modo não-sofisticado, a biometria já existe há séculos. Partes de nossos corpos e aspectos de nosso comportamento têm sido usados no

decorrer da História como um modo de identificação. O estudo das imagens digitais data da Antiguidade da China; nós sempre lembramos e identificamos uma pessoa pelo seu rosto ou pelo som de sua voz; e uma assinatura é o método estabelecido para autenticação em bancos, para contratos legais e em muitas outras ocasiões [www.consultoresbiometricos.com.br].

Um cientista chamado Francis Galton é considerado um dos fundadores do que chamamos hoje de Biometria: a aplicação de métodos estatísticos para fenômenos biológicos. Sua pesquisa em habilidades e disposições mentais, a qual incluía estudos de gêmeos idênticos, foi pioneira em demonstrar que vários traços são genéticos. Galton abriu o Laboratório de Antropométrica na Exibição Internacional de Saúde em 1884, onde ele coletou estatísticas de milhares de pessoas. Em 1892, Galton inventou o primeiro sistema moderno de impressão digital. Adotado pelos departamentos de polícia em todo o mundo, a impressão digital era a forma mais confiável de identificação, até o advento da tecnologia do DNA no século XX [PEDROSA, 2003]

Os avanços comerciais na área da biometria começaram na década de setenta. Durante este período, um sistema chamado Identimat foi instalado em um número de locais secretos para controle de acesso. Ele mensurava a forma da mão e olhava principalmente para o tamanho dos dedos. A produção do Identimat acabou na década de oitenta. Seu uso foi pioneiro na aplicação da geometria da mão e pavimentou o caminho para a tecnologia biométrica como um todo [www.consultoresbiometricos.com.br].

Paralelamente ao desenvolvimento da tecnologia de mão, a biometria digital estava progredindo nas décadas de sessenta e setenta. Durante este tempo, algumas companhias estavam envolvidas com identificação automática das imagens digitais para auxiliar às forças policiais. O processo manual de comparação de imagens digitais com registros criminais era longo e necessitava de muito trabalho manual. No final dos anos sessenta o FBI começou a checar as imagens digitais automaticamente e na metade da década de setenta já havia instalado uma quantidade de sistemas de scanners digitais automáticos. Desde então, o papel da biometria nas forças policiais tem crescido rapidamente e os *Automated Fingerprint Identification Systems* (AFIS)

são utilizados por um número significante de forças policiais em todo o mundo. Com base nesse sucesso, a biometria por scanner de digitais está agora explorando o campo dos mercados civis [PEDROSA, 2003].

4.3 Tipos de Autenticação Biométrica

A identificação biométrica pode ser feita por características físicas ou comportamentais, variando de grau e complexidade da análise. Características físicas incluem impressão digital, reconhecimento da face, identificação da íris, identificação da retina e geometria da mão. Características comportamentais, por sua vez, fazem o reconhecimento da assinatura, reconhecimento da voz ou reconhecimento da dinâmica da digitação [DOUGLAS, 2004].

4.3.1 Íris

A íris é o anel colorido que circunda a pupila do olho. Cada íris possui uma estrutura única, caracterizando um padrão complexo. Pode ser uma combinação de características específicas como coroa, glândula, filamentos, sardas, sulcos radiais e estriamentos. É conhecido que uma duplicação artificial da íris é virtualmente impossível devido às suas propriedades únicas. A íris é estreitamente ligada ao cérebro humano e dizem ser uma das primeiras partes a se desintegrar após a morte. É portanto muito improvável que uma íris artificial possa ser recriada ou que uma íris morta possa ser usada para fraudar a passagem no sistema biométrico [www.consultoresbiometricos.com.br].

O processo de reconhecimento da íris dá-se da seguinte forma:

- Captura: uma câmera de vídeo preto e branco captura uma imagem da íris. Isso deverá ser feito em um ambiente bem iluminado. Lentes de contato não interferem na captura da imagem. Óculos e óculos escuros, entretanto, não devem ser usados pois podem afetar o processo de captura.

- Extração: o equipamento biométrico extrai as características únicas da íris no exemplo captura. Então elas são convertidas em um código matemático único e armazenadas como um *template*.

- Comparação: a verificação um-para-um (1:1) ou a identificação um-para-muitos (1:n) podem ser desempenhadas.

4.3.2 Retina

A retina é a camada de veias sangüíneas situada na parte de trás do olho. Assim como na íris, a retina forma um padrão único e começa a se desintegrar logo após a morte. As biometrias de retina são geralmente tidas como o método biométrico mais seguro. O acesso não-autorizado em um sistema de retina é virtualmente impossível. Um procedimento preciso de cadastramento é necessário, o que envolve o alinhamento da vista para alcançar uma leitura otimizada [www.consultoresbiometricos.com.br].

O processo de varredura da retina ocular é o seguinte:

- Captura: O olho é posicionado em frente ao sistema, aproximadamente 3 polegadas de um leitor ocular. O usuário final deverá olhar para um ponto verde por alguns segundos, visível através do leitor. Quando isso for feito, o olho estará suficientemente focado para que o scanner capture o padrão da retina. Uma área conhecida como fóvea, situada no centro da retina, é lida e um padrão único das veias sangüíneas é capturado.

- Extração: O equipamento biométrico mapeia a posição das veias sangüíneas; uma representação matemática única é extraída e armazenada como um *template*;

- Comparação: Normalmente é feita a identificação um-para-muitos (1:n). O processo de captura se repete e o novo exemplo é comparado com o *template*.

4.3.3 Face

Identificar um indivíduo através da análise da face é um processo complexo que normalmente requer artifícios inteligentes sofisticados e técnicas de aprendizagem computacional (*machine learning techniques*). Uma quantidade de fornecedores biométricos está envolvida na venda desses sistemas, usando tanto vídeos padrões como imagens termais para capturar imagens faciais. A face é um componente chave da maneira como os seres

O processo de reconhecimento facial é o seguinte:

- Captura: técnicas padrões de vídeo usam uma imagem facial, ou uma coleção de imagens, capturada por uma câmera de vídeo. A posição precisa da face do usuário e as condições de iluminação podem afetar o desempenho do sistema. Normalmente a imagem facial completa é capturada e um número de pontos podem ser mapeados na face. Por exemplo, a posição dos olhos, boca e narinas podem ser traçadas para que um *template* único seja construído. Alternativamente, um mapa facial tridimensional pode ser criado a partir da imagem capturada.

As técnicas termais de imagem sob desenvolvimento analisam o calor, causado pelo fluxo de sangue sob a face. Uma câmera termal captura o padrão de veias sangüíneas ocultas por baixo da pele. Pelo fato de câmeras de infravermelho serem usadas para capturar imagens faciais, a luz não é importante e os sistemas podem capturar as imagens no escuro. Entretanto, tais câmeras são significantemente mais caras que as padrões.

- Extração: o equipamento biométrico converte o exemplo da imagem facial em um padrão e depois em um código matemático único, o qual é armazenado na forma de um *template*.

- Comparação: A verificação um-para-um (1:1) é o método mais comum de comparação. Entretanto, certos sistemas são capazes de fazer a identificação um-para-muitos (1:n). Uma nova imagem facial é capturada e comparada com o *template* previamente armazenado.

4.3.4 Geometria da Mão

A biometria de geometria da mão tira uma imagem tridimensional da mão e mede o seu tamanho e o comprimento dos dedos e das articulações. É um dos preferidos da indústria e tem sido utilizado por muitos anos - predominantemente para aplicações de controle de acesso. Apesar da geometria da mão não alcançar os maiores níveis de precisão, seu uso é conveniente e a vantagem primordial é a grande quantidade de usuários que podem ser processados rapidamente [www.consultoresbiometricos.com.br].

O processo de geometria da mão é o seguinte:

- Captura: o usuário coloca sua mão no leitor; alinha os dedos em guias especialmente posicionados. Uma câmera posicionada acima da mão captura uma imagem. Medidas tridimensionais de pontos selecionados da mão são então tomadas.

- Extração: o equipamento biométrico extrai as medidas 3D em um identificador matemático único e então um *template* é criado.

- Comparação: a geometria da mão é usada predominantemente para identificação um-para-um (1:1). Um novo exemplo 3D é comparado com um banco de dados de *templates*.

4.3.5 Geometria do Dedo

Alguns fornecedores biométricos utilizam a geometria de dedo, ou a medição da forma do dedo, para determinar a identidade. Essa tecnologia não tem raízes nas Forças Policiais e usa princípios similares aos da geometria de mão. A geometria de um ou dois dedos pode ser analisada, dependendo do sistema biométrico que esteja sendo usado. As medidas de atributos únicos do dedo, como a largura, comprimento, espessura e o tamanho das articulações são tomadas. Sistemas de geometria do dedo podem desempenhar a verificação um-para-um (1:1) ou a identificação um-para-muitos (1:n)). A principal vantagem é que esses sistemas são robustos e podem acomodar uma grande quantidade de usuários [www.consultoresbiometricos.com.br].

O processo de geometria do dedo é o seguinte:

- Captura: assim como na verificação da imagem digital, o método de captura depende do sistema que está sendo usado. Existem atualmente duas técnicas principais no mercado.

A primeira mede a geometria de dois ou mais dedos. A câmera tira medidas 3D quando um usuário final coloca o seu dedo indicador ou do meio, das mãos direita e esquerda, em um leitor.

A segunda técnica requer que o usuário coloque o dedo em um túnel para que as medidas 3D do dedo possam ser tomadas.

- Extração: as medidas 3D são extraídas pelo equipamento biométrico e então um *template* é criado.

- Comparação: o novo exemplo 3D é comparado com o *template*.

4.3.6 Palma

A biometria da palma pode ser estreitamente associada com a impressão digital e particularmente com a tecnologia AFIS. Os dados das linhas papilares, vales e minúcias são encontrados na palma, assim como nas imagens digitais. Normalmente eles são analisados usando técnicas de captura óptica. Essa área da indústria biométrica está particularmente focada na comunidade policial, tendo em vista que imagens latentes da palma são tão úteis em resoluções de crimes quanto as impressões digitais latentes. Entretanto, alguns fornecedores também estão visando o mercado de controle de acesso e esperam migrar para aplicações civis, seguindo os passos da impressão digital [www.consultoresbiometricos.com.br].

O processo básico de identificação da palma é o seguinte:

- Captura: a biometria da palma é predominantemente utilizada para identificação um-para-muitos (1:n). Um sistema de palma captura imagens quando uma mão é colocada num scanner. Imagens latentes ou com tinta também podem ser lidas num sistema da mesma forma como num AFIS.

- Extração: os dados das minúcias são extraídos pelo equipamento biométrico e os dados da palma são armazenados como um *template* no banco de dados.

- Comparação: uma nova imagem capturada, tanto por técnicas de tempo real, latente ou impressão em papel, é comparada com um banco de dados de imagens palmares.

4.3.7 Assinatura

A biometria de assinatura geralmente é denominada como uma Verificação Dinâmica de Assinatura (DSV) e observa a forma como assinamos nossos nomes. É a forma de assinar, mais do que a assinatura acabada, que realmente importa. O DSV pode ser diferenciado do estudo estatístico de assinaturas em papel. Algumas características podem ser extraídas e medidas pelo DSV. Por exemplo, o ângulo no qual a caneta é segurada, o tempo que se leva para assinar, a velocidade e a aceleração da assinatura, a pressão exercida quando segura-se a caneta e o número de vezes que a caneta é levantada do papel - tudo isso pode ser extraído como características comportamentais únicas. O DSV não é baseado em uma imagem estática, portanto mesmo que uma assinatura seja copiada, um impostor precisará saber a dinâmica da assinatura. Isso torna a falsificação muito difícil [www.consultoresbiometricos.com.br].

A outra vantagem da biometria de assinatura é que a assinatura é um dos modos mais aceitos para validação de identidade. Também é utilizada em situações para vincular um indivíduo legalmente, como a assinatura de um contrato. Esses fatores levaram a biometria de assinatura a diversos mercados e aplicações, desde a vinculação legal de documentos à checagem de títulos, gerenciamento de documentos e computação com base em caneta eletrônica (*pen-based computing*) [www.consultoresbiometricos.com.br].

O processo básico do DSV é o seguinte:

- Captura: os dados da assinatura podem ser capturados através de uma caneta ou superfície sensível, ou ambos. O método baseado na caneta incorpora sensores dentro da mesma. O método da superfície deixa que a

superfície sinta as características únicas da assinatura. Outra variação tem sido desenvolvida e é conhecida como emissão acústica. Ela mede o som que a caneta faz contra o papel. Normalmente em sistemas DSV, assim como em todas as biometrias, um usuário irá cadastrar uma certa quantidade de vezes para que o sistema possa construir um perfil das características da assinatura.

- Extração: as características únicas da assinatura são extraídas, codificadas por um equipamento biométrico e armazenadas como um *template*.

- Comparação: as biometrias de assinatura normalmente são utilizadas para verificações um-para-um (1:1). O novo exemplo de assinatura será comparado com o *template* armazenado.

4.3.8 Voz

Essas biometrias estão focalizadas no som da voz. É importante distinguir esta tecnologia daquelas que reconhecem palavras e fazem certos comandos. O software de reconhecimento de voz pode reconhecer palavras e digitar uma letra ou automatizar instruções dadas por um telefone. Isso não é uma tecnologia biométrica. Para evitar qualquer confusão com o reconhecimento de voz, os termos reconhecimento da fala, verificação da fala e identificação da fala deverão ser usados quando se referindo à biometria. Em outras palavras, use a locução “da fala” ou “identidade da fala” no lugar de “voz” [www.consultoresbiometricos.com.br].

O som da voz humana é causado pela ressonância nas cordas vocais. O comprimento da corda vocal, o formato da boca e as cavidades nasais são importantes. O som é medido quando afetado por essas características específicas. A técnica de medição da voz pode usar tanto métodos dependentes de texto ou não. Ou seja, a voz pode ser capturada com um usuário falando uma senha específica de frases combinadas, palavras ou números (dependente), ou qualquer forma de frase, palavras ou números (independente). Atualmente, as técnicas dependentes de texto são dominantes nos sistemas comerciais disponíveis de identificação da fala [www.consultoresbiometricos.com.br].

A biometria de identificação da fala é particularmente útil para aplicações baseadas na telefonia. Todos estão acostumados a falar no telefone e os sistemas biométricos podem facilmente ser incorporados em redes de telefonia privadas ou públicas. Entretanto, barulhos e interferências no ambiente onde está a rede de telefonia podem afetar o desempenho dos sistemas de identificação da fala [www.consultoresbiometricos.com.br].

O processo básico de identificação da fala é o seguinte:

- Captura: o usuário fala num microfone e dita uma frase previamente selecionada (dependente) ou randômica (independente). Este processo geralmente é repetido algumas vezes para se construir um perfil da voz.

- Extração: o equipamento biométrico extrai o sinal único da voz e então um *template* é criado.

- Comparação: a verificação um-para-um (1:1) é o método preferencial. O usuário fala em um microfone; o novo exemplo de voz é então comparado com o *template* armazenado.

4.3.9 Impressão Digital

A impressão digital é formada por um conjunto de cristas ou *ridges*, usando o termo inglês.

Localmente, as cristas encontram-se distribuídas paralelamente umas às outras, segundo determinada orientação e espaçamento. As cristas alternam periodicamente com as depressões resultando num comportamento semelhante a uma senóide[2]. Neste conjunto de cristas, orientado e espaçado, existem perturbações resultando no aparecimento das anomalias locais que são a terminação ou bifurcação de uma crista, conhecidas por minúcias [PACHECO, 2003].

Existem duas formas de fazer a autenticação utilizando a impressão digital: assistida e automática. A assistida é feita por peritos que, por inspeção

visual, determinam se uma impressão é ou não igual a outra, através das minúcias [PACHECO, 2003].

A autenticação automática, através de hardware e software, recorre ao processamento digital de imagem. Esta forma tem a vantagem de libertar o ser humano de tarefas rotineiras e diminuir o tempo de resposta. Neste trabalho, realiza-se a autenticação automática por impressão digital, representada por imagem monocromática [PACHECO, 2003].

As biometrias de digitais são amplamente conhecidas como um método preciso de identificação e verificação biométrica. A maior parte dos sistemas de digitais um-para-muitos (1:n) e um-para-um (1:1) analisa pequenos atributos únicos na imagem da digital, que são conhecidos como minúcias. Elas podem ser definidas como os contornos das linhas papilares ou bifurcações (ramificações das linhas papilares). Outros sistemas de impressões digitais analisam os pequenos poros no dedo que, assim como as minúcias, são posicionados de forma única para diferenciar uma pessoa de outra. A densidade da imagem digital ou a distância entre as linhas papilares também podem ser analisadas [www.consultoresbiometricos.com.br].

Certas condições podem afetar as impressões de diferentes indivíduos. Por exemplo, sujeira, dedos secos ou rachados podem reduzir a qualidade da captura da imagem. Idade, sexo e etnia também podem impactar a qualidade das imagens digitais. A forma como um usuário interage com um scanner de digitais é outra consideração importante. Pressão muito forte na superfície do scanner, por exemplo, pode distorcer uma imagem. Alguns scanners são ergonomicamente desenhados para aperfeiçoar o processo de captura de impressões digitais [www.consultoresbiometricos.com.br].

Uma diferença chave entre as várias tecnologias de digitais no mercado é a forma de captura da imagem. Sistemas de verificação um-para-um (1:1) usam quatro técnicas principais de captura: óptica, termal ou tátil, captação e

[2] Uma senóide ou onda seno (sinusóide ou onda sinusoidal) é uma forma de onda cujo gráfico é idêntico ao da função seno generalizada

ultra-som. Produtos um-para-muitos (1:n) capturam imagens digitais usando a técnica óptica ou por varredura eletrônica das imagens de um papel [3].

Verificação da Imagem Digital

O processo de verificação um-para-um (1:1) é o seguinte:

- Captura: A técnica de imagem óptica normalmente envolve a geração de uma fonte de luz, a qual é refracionada através de um prisma, em cuja superfície de vidro o dedo é colocado a luz brilha na ponta do dedo e a impressão é feita pela imagem do dedo que é capturada.

Técnicas táteis ou termais utilizam uma sofisticada tecnologia de chip de silicone para conseguir os dados da imagem digital. O usuário posiciona um dedo no sensor que sentirá o calor ou a pressão do dedo e o dado será capturado.

Sensores de captação de silicone medem as cargas elétricas e dão um sinal elétrico quando o dedo é colocado em sua superfície. O elemento chave da técnica de captação, assim como dos métodos táteis e termais, é o sensor. Usando a captação, as mínimas elevações e aprofundamentos das linhas papilares e os vales na ponta do dedo são analisados. Um sinal elétrico é dado quando as linhas papilares entram em contato com o sensor. Nenhum sinal é gerado pelos vales. Essa variação na carga elétrica produz a imagem digital [www.consultoresbiometricos.com.br].

A captura de imagem por ultra-som utiliza ondas de som abaixo do limite de audição humano. Um dedo é colocado no scanner e ondas acústicas são usadas para medir a densidade do padrão da imagem digital.

- Extração: O equipamento biométrico extrai os dados contidos na imagem digital. Uma representação matemática única é então armazenada na forma de um *template*.

- Comparação: Durante o processo de comparação, um novo exemplo é comparado com o *template*. Dependendo da base que está configurada para a aplicação, pode-se obter um par como resultado ou não.

Identificação da Imagem Digital

O processo de identificação um-para-muitos é o seguinte:

- Captura: para identificações padrões um-para-muitos (1:n), os indivíduos são cadastrados usando um processo de captura óptica em tempo real como o descrito acima na verificação da imagem digital. Sistemas AFIS de Forças Policiais, também conhecidos como estações de cadastramento, capturam as imagens de todos os dez dedos. Um AFIS civil, entretanto, não precisa capturar todas as imagens e pode operar efetivamente utilizando uma ou duas. Impressões latentes, tomadas de uma cena de um crime, ou imagens com tinta em um papel, também podem ser capturadas pelo AFIS utilizando-se um scanner rolado (*flatbed scanner*).

- Extração: Para um AFIS, o processo de *binning* das imagens digitais refina o processo de extração. Dados das minúcias são extraídos e armazenados na forma de um *template* no banco de dados.

- Comparação: Um novo exemplo, capturado tanto com técnicas em tempo real, quanto latente ou em papel, é comparado com um banco de dados de imagens digitais.

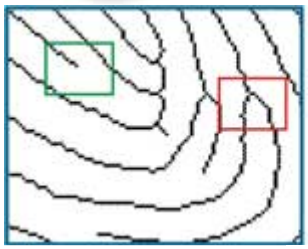
A impressão digital é capturada de um leitor.

A imagem é pré-processada (melhor contraste e clareza).

Ruídos e defeitos são eliminados.

As características da impressão são detectadas e analisadas.

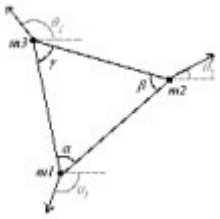
As minúcias são identificadas.



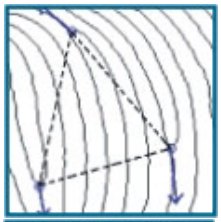
Final de uma papila

Bifurcação

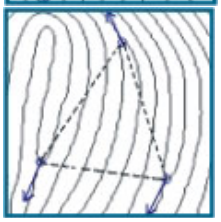
A procura das impressões no banco de dados é baseada em algumas medidas; triângulos são determinados conectando-se 3 minúcias. Ângulos internos e cada ângulo das minúcias são computados. Essas medidas não variam com a rotação e a translação.



Esse método permite que uma impressão desejada possa ser localizada no banco mesmo com variação da posição do dedo lido em relação ao cadastrado.



Impressão desejada



Impressão encontrada

Fonte: http://www.graule.com

Processo de identificação da impressão digital.

Fatores como a facilidade de uso e a percepção do público mudam o tempo todo. Cada um dos fatores a seguir tem sido separado pela simplicidade e estão graduados como baixo, médio, alto ou muito alto:

- Nível de Precisão: Qual é a precisão geral da biometria?
- Facilidade de Uso: Instruções especiais são necessárias? Quão fácil é para se usar efetivamente a biometria?
- Barreiras ao Ataque: Quão boa é a biometria na prevenção de acessos fraudulentos?
- Aceitabilidade do Público: Quão confortável o público se sente com a biometria?
- Estabilidade à Longo Prazo: As características físicas ou comportamentais mudam com o tempo?

Uma resposta específica é dada para os seguintes fatores:

- Padrões: Existem padrões? Os padrões estão sendo desenvolvidos?

	Íris	Retina	Face	Impressão Digital
Nível de Precisão	Muito alta	Muito alta	Alta	Alta
Facilidade de Uso	Média	Baixa	Média	Alta
Barreiras ao Ataque	Muito alta	Muito alta	Média	Alta
Aceitabilidade do Público	Média	Média	Alta	Média
Estabilidade à Longo Prazo	Alta	Alta	Média	Alta
Padrões	-	-	-	ANSI/NIST Data Interchange & FBI Image Compression Standards
Interferência	Óculos utilizado pelo usuário	-	Iluminação fraca; envelhecimento da face; óculos; pêlos faciais	Umidade, sujeira ou imagens digitais danificadas; idade; sexo e raça do usuário final.
	Geometria da Mão	**Geometria do Dedo**	**Palma**	**Voz**
Nível de Precisão	Alta	Alta	Alta	Alta
Facilidade de Uso	Alta	Alta	Alta	Alta
Barreiras ao Ataque	Alta	Alta	Alta	Média
Aceitabilidade do Público	Alta	Média	Média	Alta
Estabilidade à Longo Prazo	Média	Média	Alta	Média
Padrões	-	-	ANSI/NIST Data Interchange & FBI Image Compression Standards	Speaker Verification API (SVAPI)
Interferência	Doenças como artrite e reumatismo nos usuários finais	Doenças como artrite e reumatismo nos usuários finais	Umidade, sujeira ou imagens digitais danificadas; idade; sexo e raça do usuário final.	Barulhos no ambiente; resfriados e outros fatores que modificam a voz.

Fonte: Biometria Medidas de Segurança

Tabela 1 – Perfil dos métodos de autenticação biométrica

5 Solução Proposta

Foi desenvolvida uma interface em Java de autenticação que representa um ATM de um banco chamado Seu Banco, para simular o acesso de um usuário ao serviço de Caixa eletrônico deste banco.

Na proposta apresentada, o usuário será autenticado no ATM da instituição financeira ao pressionar sua impressão digital, previamente cadastrada pela instituição. A aplicação irá verificar se o usuário está realmente cadastrado na base de dados da instituição financeira.

A simulação será feita mediante a utilização de um computador como se fosse um ATM onde um usuário que irá interagir. Nesta simulação faremos a apresentação do acesso bem sucedido e do acesso não autorizado.

5.1 Requisitos da Aplicação

Como pré-requisito para o funcionamento da aplicação, será necessário que o cliente já possua sua impressão digital previamente cadastrada na base de dados da instituição financeira.

Mostrar como a utilização da solução pelas instituições financeiras que resolverem adotá-la pode trazer vantagens de segurança, obtidas com a autenticação biométrica.

Na simulação o resultado esperado é que o usuário pressione sua impressão digital sobre o leitor biométrico e que o mesmo seja autenticado pela aplicação e, após a autenticação do usuário, será mostrada a tela o nome do usuário e as opções de um ATM, extrato, saque, pagamentos e etc.

Caso o usuário não seja autenticado a mensagem “Usuário não identificado. Tente novamente” deverá ser exibida na tela.

A estrutura da solução proposta está no desenvolvimento de uma aplicação Java que simulará o ATM para autenticar um usuário de uma instituição financeira.

A autenticidade do usuário é verificada fazendo uma consulta na base de dados local que irá conter os seguintes dados: CPF, Número de Conta Corrente, Agencia, ID impressão digital e o *template* da impressão digital.

Por não ser objeto de estudo desse trabalho estas opções (saque, extrato e etc.) não estarão ativas, ou seja, são utilizadas somente como ilustração.

5.2 Leitor Biométrico utilizado para o trabalho

Para o desenvolvimento desse projeto foi utilizado o leitor biométrico da Microsoft® o Microsoft FingerPrint Reader. No Anexo I pode ser encontrado algumas características técnicas desse leitor.

Fonte: http://www.microsoft.com

Figura 19 - Biométrico utilizado.

A escolha desse leitor se deu principalmente pelo seu baixo custo em relação a outros leitores disponíveis no mercado, por não haver necessidade de tratamento de superfície, é resistente a choques, superfície sem riscos e sem corrosão, não apresenta problemas de encontro à eletricidade estática e por ser um dos leitores compatíveis com a API e o Driver utilizados, que serão tratados no capítulo 5.4.

Este leitor, originalmente, é utilizado para autenticação em computadores pessoais em substituição a senhas de rede ou locais, o driver e a aplicação foram desenvolvidos para esse fim.

Com a utilização do driver FingerCap USB, desenvolvido pela Griaule foi possível utilizar este leitor em conjunto com a API para o desenvolvimento da aplicação que simulará o ATM.

5.3 Computador e Sistema Operacional utilizados

O computador utilizado para a realização do trabalho e implementação da simulação tem a seguinte configuração:

- Processador Semprom 3000+ 787MHz.
- 512 MB de RAM.
- HD 40 GB.
- Sistema Operacional Windows XP Professional - SP2
- Interface USB (para utilização do leitor biométrico)

A escolha de um sistema operacional da Microsoft deveu-se aos seguintes motivos:

- O leitor biométrico utilizado na simulação é da mesma marca, garantindo melhor compatibilidade.
- O driver utilizado está disponível (até a conclusão deste trabalho) somente para sistemas operacionais da Microsoft.

5.4 Driver e SDK do Leitor Biométrico

Foi utilizado para o desenvolvimento desse projeto o Driver FigerCap USB Driver disponibilizado e desenvolvido por Griaule Fingertprint Recognation em parceria com a Universidade Estadual de Campinas – UniCamp.

A SDK utilizada foi a GrFinger Biometric SDK 4.2, um Kit de Desenvolvimento de Software (SDK) de reconhecimento de impressões digitais que permite integrar a biometria em um grande leque de aplicações.

Esta é uma lista dos leitores suportados nativamente, além de suas características técnicas. Estes leitores representam cerca de 90% do mercado mundial.

Microsoft Fingerprint Reader
tipo: ótico
resolução: 512 DPI
tamanho da imagem: 355x390 pixels
cores: 256 tons de cinza
conexão: USB 1.0, 1.1 ou 2.0
sistemas suportados: Windows XP/2003/2000/Me/98 SE

Digital Persona U.are.U 4000
tipo: ótico
resolução: 512 DPI
tamanho da imagem: 355x390 pixels
cores: 256 tons de cinza
conexão: USB 1.0, 1.1 ou 2.0
sistemas suportados: Windows XP/2003/2000/Me/98 SE

SecuGen Hamster FDU02
tipo: ótico
resolução: 500 DPI
tamanho da imagem: 260x300 pixels
cores: 256 tons de cinza
conexão: USB 1.1
sistemas suportados: Windows XP/2003/2000/Me/98/NT

Geomok (Testech) Bio-I
tipo: bioluminescente
resolução: 500 DPI
tamanho da imagem: 288x352 pixels
cores: 256 tons de cinza
conexão: USB 1.1 ou 2.0
sistemas suportados: Windows XP/2003/2000

Crossmatch V250/V300/V300 LC/V300 LC2/V500
tipo: ótico
resolução: 500 DPI
tamanho da imagem: 504x480 pixels
cores: 256 tons de cinza
conexão: USB 2.0
sistemas suportados: Windows XP/2000

5.5 Pré-Requisitos para a solução proposta

Os pré-requisitos para o funcionamento da solução são:

- Que o cliente possua uma impressão digital com o mínimo de falhas;
- Que a impressão digital seja previamente cadastrada na base de dados da instituição financeira e vinculada a determinada agência e conta corrente.

5.6 Dificuldades encontradas e suas soluções

Foram várias as dificuldades encontradas durante o desenvolvimento deste trabalho, entre elas as quais é relevante destacar:

- Pouco conhecimento sobre linguagem Java: para minimizar este problema foi necessário contar com a ajuda de colegas de trabalho, além da participação em fóruns de discussão e leitura bibliografia específica sobre Java.
- Dificuldade em encontrar um leitor biométrico de impressão digital no mercado e o custo do mesmo: o preço do leitor biométrico foi de R$ 190,00 (cento e noventa reis).
- Pouca leitura técnica sobre terminais de auto-atendimento: esta dificuldade foi resolvida por meio de consulta a profissionais da área.

5.7 Vantagens e desvantagens da solução proposta

Como vantagem para a utilização desta proposta pode-se destacar:

- A impressão digital, por ser única para qualquer pessoa, não pode ser clonada, exigindo a presença do usuário durante a utilização do ATM.
- Não haverá necessidade de memorizar senhas, assim seria mais fácil para pessoas idosas utilizarem os serviços do ATM.

- O número de fraudes em instituições financeiras será reduzido, consequentemente diminuindo as despesas da instituição.

Como desvantagens pode ser citado:

- Usuários com problemas na impressão digital teriam dificuldades em utilizar essa solução.

- As instituições financeiras teriam um custo adicional para adaptar seus ATMs atuais para o uso de leitores biométricos.

- O número de “seqüestros relâmpagos” poderá aumentar, já que é exigida a presença do usuário para realizar operações no ATM.

6. Viabilidade da Solução Proposta

As aplicações mercadológicas das tecnologias biométricas é extremamente diverso. Contudo, as aplicações biométricas podem ser simplesmente categorizadas, sendo elas para uso em forças policiais ou para uso civil.

Os bancos andam analisando uma variada gama de tecnologias biométricas há anos. As fraudes e as brechas na segurança precisam ser controladas caso os bancos queiram continuar competindo na sempre diversificada indústria de serviços financeiros. Conexões fracas como o Automated Teller Machines (ATMs) e transações no momento da venda são particularmente vulneráveis à fraudes e podem ser asseguradas pelas biometrias [www.consultoresbiometricos.com.br].

Abaixo foi realizada uma análise da viabilidade da solução proposta, considerando taxas de erro com o leitor e a API utilizada, custos com treinamento, manutenção e aquisição dos equipamentos e links.

AUTO-ATENDIMENTO: TIPOS E LOCALIZAÇÕES DOS EQUIPAMENTOS

em milhões de unidades	Ano	Em agências	Em ante-salas de auto-atend.	Quiosque em locais públicos	Em postos de atend.	Total	Variação (2006 /2005)
ATMs Saque e depósito	2000	4.602	7.476	2.975	586	15.639	
	2001	4.717	11.677	3.340	2.803	22.537	
	2002	11.490	14.157	4.396	3.190	33.233	
	2003	16.145	16.636	5.201	3.577	41.559	2,6%
	2004	15.268	24.530	4.214	4.208	48.220	
	2005	14.535	28.446	4.322	4.749	52.052	
	2006	14.224	29.783	4.036	5.384	53.427	
ATM's A adaptadas a PCD's	2006	1.295	5.790	311	473	7.869	
Cash-dispenser	2000	27.150	13.635	1.063	5.770	47.618	
	2001	36.991	13.700	1.557	5.818	58.066	
	2002	33.781	12.916	2.195	5.475	54.367	
	2003	32.210	12.132	2.833	5.131	52.306	-4,0%
	2004	18.212	20.031	12.158	6.307	56.708	
	2005	14.582	23.945	12.886	7.850	59.263	
	2006	16.162	20.631	12.019	8.086	56.898	
Terminal de depósito	2000	9.086	6.236	14	364	15.700	
	2001	10.263	7.627	7	219	18.116	
	2002	9.599	6.889	8	476	16.972	
	2003	8.935	6.151	9	733	15.828	
	2004	5.946	11.444	592	1.192	19.174	
	2005	3.402	14.816	224	1 120	19.562	-8,4%
	2006	4.400	12.277	5	1.241	17.923	
Terminal de extrato e saldo (1)	2000	11.663	8.776	30	1.791	22.260	
	2001	12.159	10.974	150	976	24.259	
	2002	4.747	2.825	821	916	9.309	
	2003	3.474	762	1.491	1.381	7.108	4,4%
	2004	957	1.222	133	1.089	3.401	
	2005	814	1.306	145	1.094	3.359	
	2006	798	986	156	1.567	3.507	
Dispensador de cheques	2000	5.961	1.206	12	5	7.184	6,0%
	2001	6.791	2.260	9	32	9.092	
	2002	8.037	1.884	573	56	10.550	
	2003	9.282	1.963	598	80	11.923	
	2004	5.018	7.344	1.622	90	14.074	
	2005	4.434	9.050	1.620	396	15.500	

Fonte: FEBRABAN

Tabela 2 – Auto-atendimento: tipos e localizações dos equipamentos

Para encontrar a taxa de erro do algoritmo em conjunto com o leitor biométrico utilizado, a Griaule realizou testes em quatro bancos de dados, cada um com 12 amostras de 150 dedos, num total de 1,8 mil imagens, obtidas por um leitor de impressões digitais. O da Griaule, utilizado no desenvolvimento desse trabalho, apresentou a taxa média de 2,155% [www.griaule.com].

A consulta a base de dados de templates é realizada a uma velocidade de 300 templates por segundo sendo cada imagem possui 100 x 100 pixels com tamanho médio de 400 bytes [MANUAL, GRFINGER].

A velocidade dos links utilizados nos ATMs atualmente, variam entre 64Kbps com custo de entorno de R$1.000,00 a 128Kbps com um custo médio de R$1.800,00 (Estes valores variam de acordo com a operadora a localidade do Link). O que irá definir a velocidade do link à utilizado é a quantidade de transações realizadas por mês, acima de 10.000 transações é recomendado utilizar link de 128Kbps, casos onde o número de transações é menor o link de 64Kbps pode ser utilizado [MOURA, 2007].

Com base no custo da aquisição do leitor biométrico que foi de R$190,00 e nos dados da tabela – 2 o custo de aquisição total desses leitores gira em torno dos R$ 10.810.240,00. O custo com manutenção desses equipamentos seria de 25% do valor da aquisição e será pago após o término do período de garantia que é de um ano.

Para o treinamento seria cobrado R$35,00 a hora à ser pago ao instrutor sendo um instrutor por agência [MOURA, 2007].

7. Resultados Obtidos

Foi necessário analisar o nível de precisão durante a comparação entre as impressões digitais já cadastradas no banco de dados e as atuais, capturadas pelo leitor. Para determinar essa precisão existe um método (getScore()) na classe MatchingResult da API GrFinger .

No banco de dados haviam 36 *templates* cadastrados e foram utilizadas 5 impressões digitais para alcançarmos os resultados a segui.

Os resultados obtidos foram satisfatórios, após realização de vários teste foi possível avaliar, alterando o score do método getScore() a qualidade exigida da impressão digital, os seguintes dados.

Score 10: 90 % das impressões digitais encontradas

Score 40: 80 % das impressões digitais encontradas

Score 60: 70 % das impressões digitais encontradas

Score 80: 65% das impressões digitais encontradas

Score 100: 20% das impressões digitais encontradas

Com isso foi possível chegar a conclusão de que o score ideal para o desenvolvimento desse trabalho se encontra entre 40 e 60 para a identificação pois deve combinar entre 60 e 80 por cento das minúcias encontradas no banco de dados.

Foi possível verificar que impressões digitais que apresentam falhas só foi possível serem identificadas após várias tentativas independente do score utilizados, ou seja, usuários que apresentam esse problema teriam problemas ao tentar se autenticar em um ATM.

Exceto esses casos de impressões digitais com falhas, os resultados foram satisfatórios. Não houve problema para identificar impressões digitais normais, sem falhas.

8. Conclusão

Neste trabalho foi apresentada uma proposta para a utilização de biometria (Impressão digital) para autenticar usuários. O estudo se propôs a apresentar uma nova forma de acesso a serviços baseado na utilização de leitura biométrica da impressão digital de clientes, utilizando-se como exemplo de aplicação os caixas eletrônicos de instituições financeiras.

Com a simulação apresentada neste trabalho foi possível demonstrar que a utilização de autenticação biométrica por clientes de instituições financeiras (exemplo estudado) é viável, sendo possível aplicar a mesma metodologia a outros tipos de estabelecimento, por agregar segurança no processo de autenticação e por ser um método que pode facilitar a utilização dos terminais, caso estudos mais aprofundados possam minimizar algumas desvantagens como problemas de leitura quando as digitais possuem defeitos.

Apesar de ser um método de autenticação que garante maior segurança contra fraudes, por meio dos testes efetuados com o sistema de identificação proposto, verificou-se que usuários que apresentam falhas nas impressões digitais teriam problemas ao tentar se autenticar em um ATM, sendo necessário repetir o processo de autenticação para que fossem identificados.

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

Por isso, são apresentadas a seguir sugestões de estudos futuros, como sugestão para melhorar a metodologia proposta e ampliar a aplicação do conceito da biometria para autenticação de usuários.

9. Trabalhos futuros

O assunto abordado neste trabalho permite a realização de outras pesquisas relacionadas ao tema que podem agregar melhorias na solução proposta ou serem apresentadas como um novo trabalho. São elas:

- Propor e apresentar uma solução para ter um controle transacional entre vários ATMs e a instituição financeira.

- Apresentar estudo sobre as máquinas de cartões de crédito e débito utilizados em departamentos comerciais e como estes poderiam ser adaptados para aceitar a leitura de impressão digital em conjunto com *smart card* onde ficará armazenado o padrão da impressão digital do usuário.

- Propor e apresentar uma solução utilizando outro tipo de autenticação biométrica para ATMs.

- Propor e apresentar uma solução utilização biometria para autenticação em internet banking.

10. Referências Bibliográficas

IESNA Committee Lighting for Automatic Teller Machines, Illuminating Engineering Society of North America, January 1997.

SERASA <http://www.serasa.com.br/guiaidoso/97.htm>. Acesso em 16 abr. 2007.

Consultores Biométricos <http://www.consultoresbiometricos.com.br/>. Acesso em 16 abr. 2007.

VIGLIAZZI, DOUGLAS. Biometria Medidas de Segurança. Edição n. 2, Florianópolis: Editora. Visual Books.

LEÒNCIO, HENRIQUE C. M. O Uso de Certificados Digitais ICP Brasil, Padrão A3, Como Tecnologia de Acesso a Conta-Cottente em Canal de Auto-Atendimento Internet. Brasília. 2006.

BRAIN, MARSHALL Marshall Brain's More How Stuff Works, John Wiley and Sons Ltd, Nova York, Outubro. 2002.

SERPRO, Serviço Federal de Processamento de Dados <http://www.serpro.gov.br/noticiasSERPRO/20070222_03>. Acesso em 16 abr. 2007.

PEDROSA, FELIPE NEGREIROS. Autenticação de Impressões Digitais. Instituto Tecnológico da Aeronáutica.

PACHECO, CÉSAR ALEXANDRE RODRIGUES DOS ANJOS. Autenticação com Impressão Digital. Lisboa 2003.

HOWSTUFFWORKS <http://money.howstuffworks.com/atm.htm>. Acesso em 16 abr. 2007.

HAY, RYAN. Biometrics Physical Security. SANS Institute 2004.

DEITEL, HARVEY & DEITEL PAUL. Java: Como Programar Edição nº 6. Editora Pearson .

FEBRABAN , Federação Brasileira de Bancos, www.febraban.org.br. Acesso 28 abr. 2007.

GrFinger 4.2 Developer's Manual, 2006.

MOURA, JOÃO, INFORMATIVO BANCOOB Nº56, Maio 2007.

Griaule Tecnologia de Impressões Digitais, www.griaule.com. Acesso em 03 abr. 2007.

Anexo I – Data Sheet do leitor biométrico

Microsoft®

Fingerprint Reader

Version Information	
Product Name	Microsoft® Fingerprint Reader
Fingerprint Reader Version	Microsoft Fingerprint Reader 1.0
Product Dimensions	
Fingerprint Reader Length	3.23 inches (82.0 millimeters)
Fingerprint Reader Width	1.97 inches (50.0 millimeters)
Fingerprint Reader Depth/Height	0.60 inches (15.7 millimeters)
Fingerprint Reader Weight	3.78 ounces (107 grams)
Cable Length	55.9 ± 1.18 inches (1420 ± 30.0 millimeters)
Compatibility and Localization	
Interface	USB Compatible
Operating Systems	Microsoft Windows® XP Professional Edition/Home Edition/Media Center Edition/Tablet PC Edition
Top-line Systems Requirements	• Microsoft Windows XP Professional Edition/Home Edition/Media Center Edition/Tablet PC Edition • Pentium 233 MHz or higher • 128 MB of RAM • 45 MB of available of available hard disk space • USB Port • CD drive
Compatibility Logos	Designed for Microsoft Windows XP
Software Version	Microsoft Internet Explorer, version 6.0 or later, and MSN® Internet Explorer, versions 8.0 and 9.0. digitalPersona Fingerprint Password Manager version 1.0 is required to use the fingerprint reader.
Product Feature Performance	
Storage Temperature & Humidity	-40 °F (-40 °C) to 140 °F (60 °C) at <5% to 65% relative humidity (non-condensing)
Operating Temperature & Humidity	32 °F (0 °C) to 104 °F (40 °C) at <5% to 80% relative humidity (non-condensing)
Fingerprint Reader Technology	
Scanner Type	Optical
Fast User Switching	Yes
Browser Password Replacement	Yes
Certification Information	
Country of Manufacture	People's Republic of China (PRC)
ISO 9002 Qualified Manufacturer	Yes
Agency and Regulatory Approvals	• FCC Declaration of Conformity (USA) • UL and cUL Listed Accessory (USA and Canada) • ICES-003 report on file (Canada) • TUV GS Certificate (Germany) • CE Declaration of Conformity, Safety and EMC (European Union) • GOST Certificate (Russia) • VCCI Certificate (Japan) • ACA Declaration of Conformity (Australia) • BSMI Certificate (Taiwan) • MIC Certificate (Korea) • NOM Certificates (Mexico) • CB Scheme Certificate (International) • WHQL (International) ID: 873350

Anexo II – Código fonte dos métodos de autenticação

```
package com.griaule.grFingerSample;

import java.io.InputStream;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;

import javax.swing.SwingUtilities;

import com.griaule.grFinger.Context;
import com.griaule.grFinger.FingerCallBack;
import com.griaule.grFinger.FingerprintImage;
import com.griaule.grFinger.FingerprintTemplate;
import com.griaule.grFinger.GrErrorException;
import com.griaule.grFinger.GrFinger;
import com.griaule.grFinger.ImageCallBack;
import com.griaule.grFinger.MatchingResult;
import com.griaule.grFinger.StatusCallBack;
import com.griaule.grFinger.Version;


public class Util implements StatusCallBack,ImageCallBack,FingerCallBack{

	private GrFinger grFinger;
	private Atm ui;
	private boolean autoIdentify = false;
	private boolean autoExtract = true;
	private FingerprintImage fingerprint;
	private FingerprintTemplate template;
	public Connection dbConnection;
	private PreparedStatement enrollStmt;
	private PreparedStatement identifyStmt;
```

```
	private PreparedStatement clearDbStmt;
	private PreparedStatement verifyStmt;
	private PreparedStatement insertedIdStmt;

	private String driver = "com.mysql.jdbc.Driver";
	private String url ="jdbc:mysql://localhost/atm";
	private String user="root";
	private String passw="123456";
	public int idUsuario;
	public Usuario usuario;



	public Util() {
		ui = new Atm(this);
		ui.setVisible(true);

		try {
//			Initializa DLL and e todos os utilitarios.
			grFinger = new GrFinger();
			Class.forName(this.driver);
			dbConnection = DriverManager.getConnection(this.url,
this.user, this.passw);

			enrollStmt = dbConnection.prepareStatement("INSERT
INTO Clientes(template) values(?)");
			identifyStmt = dbConnection.prepareStatement("SELECT *
FROM Clientes");
			clearDbStmt = dbConnection.prepareStatement("DELETE
FROM Clientes");
			verifyStmt = dbConnection.prepareStatement("SELECT
template FROM Clientes WHERE ID=?");
			insertedIdStmt =
dbConnection.prepareStatement("SELECT MAX(ID) FROM Clientes");

		} catch (GrErrorException e) {
			e.printStackTrace();
```

```
            } catch (ClassNotFoundException e) {
                  e.printStackTrace();
            } catch (SQLException e) {
                  e.printStackTrace();
            }


      }

      public static void main(String[] args)  {
            Util executavel = new Util();
            executavel.start();
      }


      private void start()  {
            try {
//                Inicializa GrCapture.
                  grFinger.initializeCapture(this);
            } catch (GrErrorException e) {
                  e.printStackTrace();
            }

      }


//       Função verifica se o leitor está plugado.
      public void onPlug(String idSensor) {
            try {
//                Iniciar a captura do sensor.
                  grFinger.startCapture(idSensor,this,this);
            } catch (GrErrorException e) {
                  e.printStackTrace();
            }
```

```
        }


//      Função verifica se o leitor está desplugado..
        public void onUnplug(String idSensor) {
                try {
//                      Para a captura sensor.
                        grFinger.stopCapture(idSensor);
                } catch (GrErrorException e) {
                        e.printStackTrace();
                }

        }

//      Função chamada quando a impressão digital é capturada
        public void onImage(String idSensor, FingerprintImage fingerprint) {

                this.fingerprint=fingerprint;
//               quando tem imagem, o template e extraido

                if (autoExtract) {
//                      extrai o template da imagem.
                        extract();
//                      identifica a impressão digital
                        if (autoIdentify) identify();
                }

        }

//      Função chamada quando há mpressão digital sobre o leitor .
        public void onFingerDown(String idSensor) {
        }

//      Função chamada quando é retirada a impressão digital do leitor.
        public void onFingerUp(String idSensor) {
```

```
	}


//	Identifica a impressão atual no banco de dados
	public void identify() {


			byte buffer[] = new
byte[GrFinger.GR_MAX_SIZE_TEMPLATE];


			try {
				if (!this.ui.getPainelCentralErro().isShowing() &&
!this.ui.getPainelCentralSucesso().isShowing() &&
!this.ui.getPainelCentralSaque().isShowing() &&
!this.ui.getPainelSaqueSucesso().isShowing()){ // Caso a tela de erro esteja
sendo apresentada nao validar ninguem


					// Inicia o processo de identificação com o
template informado

	grFinger.identifyPrepare(template,Context.DEFAULT_CONTEXT);
					// Busca os templates gravados no banco de
dados
					ResultSet rs = identifyStmt.executeQuery();
					// verifica todos os templates do banco de
dados
					boolean var = false;
					while (rs.next()){
						InputStream stream =
rs.getBinaryStream("template");
						int size = stream.read(buffer);


						  // Cria um novo template
						FingerprintTemplate referenceTamplate
= new FingerprintTemplate(buffer,size);
	//					 Compara o template atual.
						MatchingResult result =
grFinger.identify(referenceTamplate,Context.DEFAULT_CONTEXT);
						if (result.doesMatched()){
							var = true;
```

```
                                                    if (result.getScore() > 50){
                                                        int idUsuarioAnterior =
this.idUsuario;
                                                        this.idUsuario =
rs.getInt("ID");
                                                        this.usuario =
buscarUsuario(this.idUsuario);
                                                        if
(ui.getPainelCentralNovaAutenticacao().isShowing()){
                                                            if (this.idUsuario ==
idUsuarioAnterior)

        carregarTelaSaqueSucesso();
                                                            else

        apresentarMensagemFalhaLeitura2();
                                                        }else{

        carregarTelaUsuarioLogado();
                                                        }
                                                    }
                                                }
                                            }
                                            if (!var){
                                                apresentarMensagemFalhaLeitura();
                                                return;
                                            }
                                        }

                    } catch (Exception e) {
                        e.printStackTrace();
                    }

        }
//      Extrai a impressão digital da imagem atual
        public void extract() {

            try {
```

```
                    template =
grFinger.extract(fingerprint,Context.DEFAULT_CONTEXT);
                    String msg = "Template extraído com sucesso. ";
                    switch (template.getImageQuality()){
                        case FingerprintTemplate.GR_HIGH_QUALITY:
                            break;
                        case FingerprintTemplate.GR_MEDIUM_QUALITY:
                           break;
                        case FingerprintTemplate.GR_BAD_QUALITY:
                        break;
                    }
                    System.out.println(msg);

                } catch (GrErrorException e) {
                    e.printStackTrace();
                }

        }


        public void setAutoIdentify(boolean state) {
                autoIdentify = state;

        }

        public void setAutoExtract(boolean state) {
                autoExtract = state;

        }

        public void stop() {
//              Finaliza a biblioteca e fecha o banco de dados.
                try {
                    enrollStmt.close();
                    clearDbStmt.close();
```

```
                identifyStmt.close();
                verifyStmt.close();
                insertedIdStmt.close();
                dbConnection.close();
                grFinger.finalizeCapture();

        } catch (SQLException e) {
                e.printStackTrace();
        } catch (GrErrorException e) {
                e.printStackTrace();
        }

}

public Version getGrFingerVersion() {
//         Busca versão do GRFinger
        try {
                return grFinger.getVersion();
        } catch (GrErrorException e) {
                e.printStackTrace();
        }
        return null;
}


public void carregarTelaUsuarioLogado(){
        try{
                SwingUtilities.invokeLater(new Runnable(){
                        public void run() {
                                try{

ui.getContentPane().remove(ui.getLabelImagem());
                                        if (ui.labelNomeUsuario != null){

ui.getPainelCentralSucesso().remove(ui.labelNomeUsuario);
```

```
        ui.labelNomeUsuario.setText("Bem vindo " + usuario.getNome());
                                                }

        ui.getPainelCentralSucesso().add(ui.getLabelNomeUsuario(usuario.getN
ome()));

        ui.getContentPane().add(ui.getPainelCentralSucesso());
                                                ui.repaint();
                                        }catch (Exception e) {
                                                e.printStackTrace();
                                        }
                                }


                        });
                }catch (Exception e) {
                        e.printStackTrace();
                }
        }


        public void carregarTelaSaqueSucesso(){
                try{
                        SwingUtilities.invokeLater(new Runnable(){

                                public void run() {
                                        try{

        ui.getContentPane().remove(ui.getPainelCentralNovaAutenticacao());

        ui.getContentPane().add(ui.getPainelSaqueSucesso());ui.repaint();
                                        }catch (Exception e) {
                                                e.printStackTrace();
                                        }
                                }


                        });
```

```
            }catch (Exception e) {
                e.printStackTrace();
            }
        }

        public void apresentarMensagemFalhaLeitura(){
            try{
                if (this.ui.getPainelCentralNovaAutenticacao().isShowing()){

        this.ui.getContentPane().remove(this.ui.getPainelCentralNovaAutenticac
ao());
                }else{

        this.ui.getContentPane().remove(this.ui.getLabelImagem());
                }
                this.ui.getContentPane().add(this.ui.getPainelCentralErro());
                this.ui.repaint();
            }catch (Exception e) {
                e.printStackTrace();
            }
        }



        public void apresentarMensagemFalhaLeitura2(){
            try{

        this.ui.getContentPane().remove(ui.getPainelCentralNovaAutenticacao())
;
                this.ui.getContentPane().add(this.ui.getPainelCentralErro());
                this.ui.repaint();
            }catch (Exception e) {
                e.printStackTrace();
            }
        }

        public void removerPainel(){
            try{
```

```
        this.ui.getContentPane().remove(this.ui.painelCentralSucesso);
                }catch (Exception e) {

                }
        }


        public Usuario buscarUsuario(int id) throws Exception{
                Usuario usuario = new Usuario();
                String sql = ("select descnome from Clientes where id = " + id);
                java.sql.PreparedStatement ps =
this.dbConnection.prepareStatement(sql);
                ResultSet rs = ps.executeQuery();
                if (rs.next()){
                        usuario.setNome(rs.getString("descnome"));
                }
                return usuario;
        }

}
```

Anexo III – Código fonte da inteface com o usuário

```
package com.griaule.grFingerSample;

import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Font;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.MouseEvent;
import java.awt.event.MouseListener;
import java.awt.event.WindowEvent;
import java.awt.event.WindowListener;

import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.sql.ResultSet;

import java.util.Date;
import java.util.Properties;

import javax.swing.ImageIcon;
import javax.swing.JButton;
import javax.swing.JLabel;
import javax.swing.JOptionPane;
import javax.swing.JPanel;
import javax.swing.JTextField;
import javax.swing.JWindow;
import javax.swing.SwingConstants;



public class Atm extends JWindow implements WindowListener {
```

```
	private static final long serialVersionUID = 1L;

	private JPanel panel;
	public JPanel painelCentralSucesso;
	public JPanel painelCentralErro;
	public JPanel painelCentralSaque;
	public JPanel painelCentralNovaAutenticacao;
	public JPanel painelSaqueSucesso;
	private JLabel labelImagem;
	private JLabel labelMensagem;
	private JLabel labelData;
	private JLabel labelHora;
	private JButton botaoSair;
	private static final String fileName = "Server.properties";
	private Util prototipo;
	private JButton botaoVoltar;
	private JButton botaoExtratosImpressos;
	private JButton botaoExtratosTela;
	private JButton botaoAplicacoes;
	private JButton botaoPagamentos;
	private JButton botaoTransferencia;
	private JButton botaoSaque;
	private JButton botaoSolicitarTalao;
	private JButton botaoOutros;
	private JButton botaoConfirmar;
//	private JButton botaoTerminar;
	private JButton botaoSaque5;
	private JButton botaoSaque10;
	private JButton botaoSaque20;
	private JButton botaoSaque50;
	public JLabel labelNomeUsuario;
	private JLabel labelMensagemErro;
	private JLabel labelValor;
	private JTextField tfValor;
```

```
	private JLabel labelNovaAutenticacao;
	private JLabel labelConfirmacao;


	public Atm(Util ui) {
		this.prototipo = ui;
		this.prototipo.setAutoIdentify(true);
		initialize();
		addWindowListener(this);
	}


	protected void mostrarMensagemErro(String msg, String titulo) {
		mostrarMensagem(msg, titulo,
JOptionPane.ERROR_MESSAGE);
	}


	protected void mostrarMensagem(String msg, String titulo, int tipoMsg) {
		JOptionPane.showMessageDialog(this, msg, titulo, tipoMsg);
	}


	protected void initialize() {
		this.setBounds(0, 0, 1024, 768);
		try{
			getContentPane().add(getPainelPrincipal());
			getPainelPrincipal().setAlignmentX(SwingConstants.LEFT);
			getContentPane().add(getLabelImagem(),
BorderLayout.CENTER);
		}catch (Exception e) {
			e.printStackTrace();
			mostrarMensagemErro("Ocorreu um erro ao executar essa
operação", "Erro!");
			fecharAplicacao();
		}
```

```
		final JLabel label_1 = new JLabel();
		label_1.setHorizontalAlignment(SwingConstants.CENTER);
		label_1.setIcon(new
ImageIcon(getClass().getResource("img/teste.png")));
		this.addWindowListener(new java.awt.event.WindowAdapter() {
			public void windowClosing(java.awt.event.WindowEvent e) {
				prototipo.stop();
			}
		});
	}


	protected boolean mostraConfirmacao(String msg) {
		return JOptionPaneAtm.showConfirmDialog(this, msg,
"Confirmação", JOptionPane.QUESTION_MESSAGE,
				JOptionPane.YES_NO_OPTION) ==
JOptionPane.OK_OPTION;
	}


	protected void fecharAplicacao() {
		System.exit(0);
	}


	public void windowActivated(WindowEvent e) {
	}

	public void windowClosed(WindowEvent e) {
	}

	public void windowClosing(WindowEvent e) {
	}

	public void windowDeactivated(WindowEvent e) {
	}
```

```
public void windowDeiconified(WindowEvent e) {
}

public void windowIconified(WindowEvent e) {
}

public void windowOpened(WindowEvent e) {
}


public String getProperty(String parametro) {
	Properties pProps = null;
	FileInputStream fis;

	try {
		fis = new FileInputStream(fileName);
		pProps = new Properties();
		pProps.load(fis);
		fis.close();
	} catch (FileNotFoundException e) {
		return getProperty(parametro);
	} catch (IOException e) {
		e.printStackTrace();
	}

	return pProps.getProperty(parametro);
}


public JTextField getTfValor(){
	if (this.tfValor == null){
		this.tfValor = new JTextField();
		this.tfValor.setBounds(560,300,150,30);
		this.tfValor.setEnabled(true);
```

```
                this.tfValor.setEditable(true);
//              this.tfValor.setText("äbc");
                this.tfValor.getText();
            }
            return this.tfValor;
        }


        public Usuario buscarUsuario(int id) throws Exception{
            Usuario usuario = new Usuario();
            String sql = ("select descnome from enroll where id = " + id);
            java.sql.PreparedStatement ps =
this.prototipo.dbConnection.prepareStatement(sql);
            ResultSet rs = ps.executeQuery();
            if (rs.next()){
                usuario.setNome(rs.getString("descnome"));
            }
            return usuario;
        }


        public JLabel getLabelImagem(){
            if (this.labelImagem == null){
                this.labelImagem = new JLabel();

        this.labelImagem.setHorizontalAlignment(SwingConstants.CENTER);
                this.labelImagem.setIcon(new
ImageIcon(getClass().getResource("img/teste.png")));
            }
            return this.labelImagem;
        }


        public JLabel getLabelData(){
            if (this.labelData == null){
                this.labelData = new JLabel();
```

```
        this.labelData.setText((DateUtil.getDataPorExtenso(DateUtil.getDataAtu
al())).toUpperCase());
                        this.labelData.setBounds(900,20,160,20);
                        this.labelData.addMouseListener(new MouseListener(){

                                public void mouseClicked(MouseEvent arg0) {
                                        System.exit(0);
                                }
                                public void mousePressed(MouseEvent arg0) {
                                }
                                public void mouseReleased(MouseEvent arg0) {
                                }
                                public void mouseEntered(MouseEvent arg0) {
                                }
                                public void mouseExited(MouseEvent arg0) {
                                }
                        });
                }
                return this.labelData;
        }


        public JLabel getLabelHora(){
                if (this.labelHora == null){
                        this.labelHora = new JLabel();
                        this.labelHora.setText(DateUtil.getHoraComoString(new
Date()) + " hs");
                        this.labelHora.setBounds(930,40,160,20);
                }
                return this.labelHora;
        }


        public JLabel getLabelNomeUsuario(String nome){
                if (this.labelNomeUsuario == null){
```

```
                this.labelNomeUsuario = new JLabel();
                this.labelNomeUsuario.setText("Bem vindo " + nome + "!");
                this.labelNomeUsuario.setFont(new Font("verdana",1,20));
                this.labelNomeUsuario.setBounds(350,0,500,180);
            }
            return this.labelNomeUsuario;
        }


        public JLabel getLabelMensagemNaoIdentificado(){
            if (this.labelMensagem == null){
                this.labelMensagem = new JLabel();
                this.labelMensagem.setText("Usuário não identificado!
Volte e tente novamente.");
                this.labelMensagem.setFont(new Font("verdana",1,30));
                this.labelMensagem.setBounds(100,0,1000,580);
                this.labelMensagem.setForeground(Color.RED);
            }
            return this.labelMensagem;
        }


        public JLabel getLabelMensagemErro(){
            if (this.labelMensagemErro == null){
                this.labelMensagemErro = new JLabel();
                this.labelMensagemErro.setFont(new
Font("verdana",1,30));
                this.labelMensagemErro.setBounds(350,0,500,180);
                this.labelMensagemErro.setText("Usuário não identificado.
Tente novamente.");
                this.labelMensagemErro.setForeground(Color.RED);
            }
            return this.labelMensagemErro;
        }
```

```
	public JLabel getLabelValor(){
		if (this.labelValor == null){
			this.labelValor = new JLabel();
			this.labelValor.setText("Selecione o valor desejado:");
			this.labelValor.setFont(new Font("verdana",1,25));
			this.labelValor.setBounds(300,90,500,30);
		}
		return this.labelValor;
	}


	public JLabel getLabelNovaAutenticacao(){
		if (this.labelNovaAutenticacao == null){
			this.labelNovaAutenticacao = new JLabel();
			this.labelNovaAutenticacao.setText("Pressione o dedo
novamente sobre o leitor !");
			this.labelNovaAutenticacao.setForeground(Color.BLUE);
			this.labelNovaAutenticacao.setFont(new
Font("verdana",1,30));
			this.labelNovaAutenticacao.setBounds(150,300,800,40);
//			this.labelNovaAutenticacao.add(getBotaoTerminar());

		}
		return this.labelNovaAutenticacao;
	}


	public JLabel getLabelConfirmacao(){
		if (this.labelConfirmacao == null){
			this.labelConfirmacao = new JLabel();
			this.labelConfirmacao.setText("SAQUE REALIZADO COM
SUCESSO !");
			this.labelConfirmacao.setForeground(Color.BLUE);
			this.labelConfirmacao.setFont(new Font("verdana",1,30));
			this.labelConfirmacao.setBounds(200,300,700,40);
		}
```

```
            return this.labelConfirmacao;
        }


        private JButton getBotaoExtratosImpressos(){
            if (this.botaoExtratosImpressos == null){
                this.botaoExtratosImpressos = new JButton();
                this.botaoExtratosImpressos.setText("SALDO");
                this.botaoExtratosImpressos.setFont(new Font
("verdana",1,18));
                this.botaoExtratosImpressos.setBounds(10,170,400,60);
            }
            return this.botaoExtratosImpressos;
        }


        private JButton getBotaoExtratosTela(){
            if (this.botaoExtratosTela == null){
                this.botaoExtratosTela = new JButton();
                this.botaoExtratosTela.setText("EXTRATO");
                this.botaoExtratosTela.setFont(new Font ("verdana",1,18));
                this.botaoExtratosTela.setBounds(10,270,400,60);
            }
            return this.botaoExtratosTela;
        }


        private JButton getBotaoAplicacoes(){
            if (this.botaoAplicacoes == null){
                this.botaoAplicacoes = new JButton();
                this.botaoAplicacoes.setText("INVESTIMENTOS");
                this.botaoAplicacoes.setFont(new Font ("verdana",1,18));
                this.botaoAplicacoes.setBounds(10,370,400,60);
            }
            return this.botaoAplicacoes;
```

```
	}


	private JButton getBotaoPagamentos(){
		if (this.botaoPagamentos == null){
			this.botaoPagamentos = new JButton();
			this.botaoPagamentos.setText("PAGAMENTOS");
			this.botaoPagamentos.setFont(new Font ("verdana",1,18));
			this.botaoPagamentos.setBounds(10,470,400,60);
		}
		return this.botaoPagamentos;

	}


	private JButton getBotaoTransferencia(){
		if (this.botaoTransferencia == null){
			this.botaoTransferencia = new JButton();
			this.botaoTransferencia.setText("TRANSFERÊNCIAS");
			this.botaoTransferencia.setFont(new Font
("verdana",1,18));
			this.botaoTransferencia.setBounds(610,170,400,60);
			}
		return this.botaoTransferencia;
	}


	private JButton getBotaoSaque(){
		if (this.botaoSaque == null){
			this.botaoSaque = new JButton();
			this.botaoSaque.setText("SAQUE");
			this.botaoSaque.setFont(new Font ("verdana",1,18));
			this.botaoSaque.setBounds(610,270,400,60);
			this.botaoSaque.addActionListener(new ActionListener(){
```

```
                        public void actionPerformed(ActionEvent arg0) {
                                try{

getContentPane().remove(getPainelCentralSucesso());

getContentPane().add(getPainelCentralSaque());
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
        }
        return this.botaoSaque;
}

private JButton getBotaoSaque5(){
        if (this.botaoSaque5 == null){
                this.botaoSaque5 = new JButton();
                this.botaoSaque5.setText("R$ 5,00");
                this.botaoSaque5.setFont(new Font ("verdana",1,18));
                this.botaoSaque5.setBounds(10,170,400,60);
        this.botaoSaque5.addActionListener(new ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{

getContentPane().remove(getPainelCentralSaque());

getContentPane().add(getPainelCentralNovaAutenticacao());
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }
```

```
                });
        }
        return this.botaoSaque5;
}

private JButton getBotaoSaque10(){
        if (this.botaoSaque10 == null){
                this.botaoSaque10 = new JButton();
                this.botaoSaque10.setText("R$ 10,00");
                this.botaoSaque10.setFont(new Font ("verdana",1,18));
                this.botaoSaque10.setBounds(10,270,400,60);
                this.botaoSaque10.addActionListener(new ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{

getContentPane().remove(getPainelCentralSaque());

getContentPane().add(getPainelCentralNovaAutenticacao());
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
        }
        return this.botaoSaque10;
}

private JButton getBotaoSaque20(){
        if (this.botaoSaque20 == null){
                this.botaoSaque20 = new JButton();
                this.botaoSaque20.setText("R$ 20,00");
                this.botaoSaque20.setFont(new Font ("verdana",1,18));
```

```
                this.botaoSaque20.setBounds(610,170,400,60);
                this.botaoSaque20.addActionListener(new ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{

getContentPane().remove(getPainelCentralSaque());

getContentPane().add(getPainelCentralNovaAutenticacao());
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
        }
        return this.botaoSaque20;
}

private JButton getBotaoSaque50(){
        if (this.botaoSaque50 == null){
                this.botaoSaque50 = new JButton();
                this.botaoSaque50.setText("R$ 50,00");
                this.botaoSaque50.setFont(new Font ("verdana",1,18));
                this.botaoSaque50.setBounds(610,270,400,60);
                this.botaoSaque50.addActionListener(new ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{

getContentPane().remove(getPainelCentralSaque());

getContentPane().add(getPainelCentralNovaAutenticacao());
                                        repaint();
                                }catch (Exception e) {
```

```
                                        e.printStackTrace();
                                }
                        }

                });
        }
        return this.botaoSaque50;
}
private JButton getBotaoCheque(){
        if (this.botaoSolicitarTalao == null){
                this.botaoSolicitarTalao = new JButton();
                this.botaoSolicitarTalao.setText("CHEQUE");
                this.botaoSolicitarTalao.setFont(new Font ("verdana",1,18));
                this.botaoSolicitarTalao.setBounds(610,370,400,60);
        }
        return this.botaoSolicitarTalao;
}


private JButton getBotaoOutros(){
        if (this.botaoOutros == null){
                this.botaoOutros = new JButton();
                this.botaoOutros.setText("SAIR");
                this.botaoOutros.setFont(new Font ("verdana",1,18));
                this.botaoOutros.setBounds(610,470,400,60);
        }
        return this.botaoOutros;
}


private JButton getBotaoConfirmar(){
        if (this.botaoConfirmar == null){
                this.botaoConfirmar = new JButton();
                this.botaoConfirmar.setText("Confirmar");
                this.botaoConfirmar.setFont(new Font ("verdana",1,25));
```

```
                this.botaoConfirmar.setBounds(440,750,220,40);
                this.botaoConfirmar.addActionListener(new
ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{

        getContentPane().remove(getPainelCentralSaque());

        getContentPane().add(getPainelCentralNovaAutenticacao());
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
        }
        return this.botaoConfirmar;
}


private JButton getBotaoVoltar(){
        if (this.botaoVoltar == null){
                this.botaoVoltar = new JButton();
                this.botaoVoltar.setText("Voltar");
                this.botaoVoltar.setFont(new Font("verdana",1,18));
                this.botaoVoltar.setBounds(450,400,120,40);
                this.botaoVoltar.addActionListener(new ActionListener(){

                        public void actionPerformed(ActionEvent arg0) {
                                try{
                                        prototipo.idUsuario = 0;
                                        prototipo.usuario = null;

        getContentPane().remove(getPainelCentralErro());
```

```
        getContentPane().add(getLabelImagem(), BorderLayout.CENTER);
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
        }
                return this.botaoVoltar;
        }


/*      private JButton getBotaoTerminar() {
                if (this.botaoTerminar == null){
                        this.botaoTerminar = new JButton();
                        this.botaoTerminar.setText("TERMINAR");
                        this.botaoTerminar.setFont(new Font("verdana",1,18));
                        this.botaoTerminar.setBounds(450,400,200,40);
                        this.botaoTerminar.addActionListener(new ActionListener(){

                                public void actionPerformed(ActionEvent arg0) {
                                        try{

        getContentPane().remove(getPainelCentralNovaAutenticacao());

        getContentPane().add(getPainelSaqueSucesso(),
BorderLayout.CENTER);
                                        repaint();
                                }catch (Exception e) {
                                        e.printStackTrace();
                                }
                        }

                });
```

```
		}
			return this.botaoTerminar;
	}*/


	private JButton getBotaoSair(){
		if (this.botaoSair == null){
			this.botaoSair = new JButton();
			this.botaoSair.setText("CONCLUIR");
			this.botaoSair.setFont(new Font("verdana",1,18));
			this.botaoSair.setBounds(450,400,150,40);
			this.botaoSair.addActionListener(new ActionListener(){

				public void actionPerformed(ActionEvent arg0) {
					try{

	getContentPane().remove(getPainelSaqueSucesso());
//
	getContentPane().remove(getLabelNomeUsuario(nome));

	getContentPane().add(getLabelImagem(), BorderLayout.CENTER);
							repaint();
					}catch (Exception e) {
							e.printStackTrace();
					}
				}


			});
		}
			return this.botaoSair;
	}


	protected JPanel getPainelPrincipal() throws Exception {
		if (this.panel == null){
			this.panel = new JPanel();
```

```
                this.panel.setLayout(null);
                this.panel.setBackground(Color.LIGHT_GRAY);
                this.panel.setBounds(0,0,this.getWidth(),50);
                this.panel.setSize(this.getWidth(), 75);
                this.panel.add(getLabelData());
                this.panel.add(getLabelHora());
        }
        return this.panel;
}


public JPanel getPainelCentralSucesso() throws Exception{
        if (this.painelCentralSucesso == null){
                this.painelCentralSucesso = new JPanel();
                this.painelCentralSucesso.setLayout(null);

this.painelCentralSucesso.setBounds(0,75,this.getWidth(),710);

this.painelCentralSucesso.add(getBotaoExtratosImpressos());
                this.painelCentralSucesso.add(getBotaoExtratosTela());
                this.painelCentralSucesso.add(getBotaoAplicacoes());
                this.painelCentralSucesso.add(getBotaoPagamentos());
                this.painelCentralSucesso.add(getBotaoTransferencia());
                this.painelCentralSucesso.add(getBotaoSaque());
                this.painelCentralSucesso.add(getBotaoCheque());
                this.painelCentralSucesso.add(getBotaoOutros());
        }
        return this.painelCentralSucesso;
}


public JPanel getPainelCentralErro() throws Exception{
        if (this.painelCentralErro == null){
                this.painelCentralErro = new JPanel();
                this.painelCentralErro.setLayout(null);
                this.painelCentralErro.setBounds(0,75,this.getWidth(),710);
```

```
                this.painelCentralErro.add(getBotaoVoltar());

        this.painelCentralErro.add(getLabelMensagemNaoIdentificado());
            }
            return this.painelCentralErro;
        }


        public JPanel getPainelCentralSaque() throws Exception{
            if (this.painelCentralSaque == null){
                this.painelCentralSaque = new JPanel();
                this.painelCentralSaque.setLayout(null);

        this.painelCentralSaque.setBounds(0,75,this.getWidth(),710);
                this.painelCentralSaque.add(getBotaoSaque5());
                this.painelCentralSaque.add(getBotaoSaque10());
                this.painelCentralSaque.add(getBotaoSaque20());
                this.painelCentralSaque.add(getBotaoSaque50());
              this.painelCentralSaque.add(getLabelValor());
//              this.painelCentralSaque.add(getTfValor());
                this.painelCentralSaque.add(getBotaoConfirmar());
            }
            return this.painelCentralSaque;
        }


        public JPanel getPainelCentralNovaAutenticacao() throws Exception{
            if (this.painelCentralNovaAutenticacao == null){
                this.painelCentralNovaAutenticacao = new JPanel();
                this.painelCentralNovaAutenticacao.setLayout(null);

        this.painelCentralNovaAutenticacao.setBounds(0,75,this.getWidth(),710);

        this.painelCentralNovaAutenticacao.add(getLabelNovaAutenticacao());
//
        this.painelCentralNovaAutenticacao.add(getBotaoTerminar());
```

```
            }

            return this.painelCentralNovaAutenticacao;
        }


        public JPanel getPainelSaqueSucesso() throws Exception{
            if (this.painelSaqueSucesso == null){
                this.painelSaqueSucesso = new JPanel();
                this.painelSaqueSucesso.setLayout(null);

        this.painelSaqueSucesso.setBounds(0,75,this.getWidth(),710);
                this.painelSaqueSucesso.add(getBotaoSair());
                this.painelSaqueSucesso.add(getLabelConfirmacao());
            }

            return this.painelSaqueSucesso;
        }


}
```