Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

VAGNER COSTA PERETTI

PROPOSTA DE AUTENTICAÇÃO BIOMÉTRICA MULTIMODAL EM MOBILE BANKING

Brasília

2015

VAGNER COSTA PERETTI

PROPOSTA DE AUTENTICAÇÃO BIOMÉTRICA MULTIMODAL EM MOBILE BANKING

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MsC. Francisco Javier de Obaldía Diaz

Brasília

2015

VAGNER COSTA PERETTI

PROPOSTA DE AUTENTICAÇÃO BIOMÉTRICA MULTIMODAL EM MOBILE BANKING

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MsC. Francisco Javier de Obaldía Diaz

Banca Examinadora

_____

Prof. MsC. Francisco Javier de Obaldía Diaz

_____

Prof. MsC. Gilberto Oliveira Netto

_____

Profa. Dra. Tânia Cristina Silva Cruz

Brasília

2015

Dedico este trabalho de conclusão de curso, às pessoas mais importantes da minha vida: meus pais, irmãos e minha noiva.

AGRADESCIMENTOS

Agradeço a Deus, aos meus pais Maria das Graças e Acir Peretti, e irmãos Robson e Solange.

A minha noiva Larrucia Láize por seu apoio e compreensão, por me tranquilizar durante os momentos mais difíceis e pela disposição em me motivar a concluir este trabalho.

Agradeço também a todos os professores que tive durante o curso, que despertaram o interesse por novas tecnologias e me incentivaram a ir adiante.

On ne peut voir que ce que l'on observe, et l'on observe que ce qui se trouve déjà dans notre esprit.

Alphonse Bertillon

LISTA DE FIGURAS

LISTA DE QUADROS E TABELAS

RESUMO

O crescente uso da tecnologia biométrica em *mobile banking* está a revolucionar a forma como somos autenticados nos sistemas de informação. Uma alternativa para os métodos de autenticação atuais consiste na utilização de sistemas biométricos. Ao contrário da famosa *password,* a biometria permite realizar o processo de autenticação de forma significativamente mais prática e segura, uma vez que o usuário é identificado por suas características físicas únicas e intransferíveis, como por exemplo a impressão digital, a face, e a voz. Baseado na evolução do reconhecimento biométrico em *mobile banking*, este trabalho pretende apresentar um novo método de autenticação em *mobile banking* com elevado nível de confiabilidade, baseada na biometria multimodal utilizando a leitura biométrica da impressão digital, face e voz. Visa avaliar seus limites e potenciais reais, além de identificar sua aceitação por parte dos usuários, e sugerir um método de fusão das biometrias para sistemas multibiométricos baseado em pontuação. Para alcançar os objetivos procedeu-se de pesquisas bibliográficas relacionadas ao reconhecimento através da biometria, com foco na biometria multimodal. Também foi realizada uma pesquisa de campo acerca do conhecimento e a aceitação pelo usuário em relação ao uso da biometria como forma de autenticação.

Palavras-chave: autenticação biométrica. biometria multimodal. reconhecimento biométrico. *mobile banking*.

ABSTRACT

The increasing use of biometric technology in mobile banking is revolutionizing the way we are authenticated in information systems. An alternative to existing authentication methods is the use of biometrics. Unlike the known “password”, biometrics allows performing the authentication process significantly more practical and secure way, since the user is identified by their physical nontransferable unique characteristics, such as fingerprint, face, and voice. Based on the evolution of biometric recognition on mobile banking, this paper intend to present a new method of authentication in mobile banking with high level of reliability based on multimodal biometrics using biometric fingerprint, face and voice. Aims to assess its limitations and real potential, identify their acceptance by users, and suggest one of the biometrics fusion methods for multibiometric systems based on score. To achieve the goals we proceeded to bibliographic research related to the recognition by biometrics, focusing on multimodal biometrics. A field survey about knowledge and acceptance by the user regarding the use of biometrics as a means of authentication was also performed.

Keywords: biometric authentication. multimodal biometrics. biometric recognition. mobile banking.

SUMÁRIO

INTRODUÇÃO

Por conta do crescente número de fraudes bancárias precisamos cada vez mais de mecanismos de segurança para proteger informações e patrimônio contra pessoas não autorizadas. Conforme informações de relatórios contábeis do exercício de 2014, a Caixa Econômica Federal[1] teve um prejuízo de quase 250 milhões de reais com fraudes eletrônicas, já o Banco do Brasil[2] teve um prejuízo de quase 229 milhões de reais no mesmo ano.

Atualmente o método mais utilizado para autenticar indivíduos é a famosa *password*, que devido a métodos como Engenharia Social, *Phishing*, ataques de crackers, vírus, até mesmo seu compartilhamento ou esquecimento não a tornam o método mais eficaz na autenticidade do indivíduo.

As transformações a partir dos avanços tecnológicos proporcionaram mecanismos de autenticação baseados em características físicas do indivíduo. Dessa forma é possível utilizar determinada região do corpo para se autenticar, como por exemplo a impressão digital, íris, retina, face, voz, disposição das veias da mão, dentre outras. Em outras palavras o indivíduo passa a ter uma autenticação mais forte, utilizando além da atual *password,* suas características físicas. Nesse sentido as instituições financeiras estão trabalhando para implantar a autenticação biométrica em suas aplicações, especialmente no canal de atendimento *mobile banking*.

Com o avanço da tecnologia, já é possível encontrar *smartphones* que possuem sensores de impressão digital, câmeras e microfone. Várias instituições financeiras já utilizam o reconhecimento biométrico em caixas eletrônicos, e a tendência é que seja implantada em breve no *mobile banking*.

No intuito de aprofundar os conhecimentos sobre o reconhecimento através de biometria, destacando suas vantagens e desvantagens, é que a presente pesquisa pretende apresentar uma nova forma de autenticação em *mobile banking* baseado na leitura biométrica da impressão digital, face e voz.

---

[1] Demonstrações Contábeis Consolidadas do Conglomerado Prudencial - Dezembro de 2014

[2] Relatório da Administração do Banco do Brasil - 2014

O objetivo geral do presente trabalho é apresentar uma forma alternativa e segura de autenticação em sistemas *mobile banking* através da biometria multimodal. Os objetivos específicos são: contextualizar os métodos de reconhecimento biométrico utilizados atualmente, dissertar sobre as formas de autenticação biométrica, apresentar suas principais vantagens e desvantagens, identificar suas vulnerabilidades, dissertar sobre o funcionamento e tendências relacionadas a dispositivos móveis, apresentar a definição de mobile banking e suas tendências, propor uma forma de fusão biométrica com baixo índice de falha, apresentar as principais normas acerca do reconhecimento biométrico, e finalmente expor a aceitação pela sociedade sobre o uso da autenticação biométrica em *mobile banking*.

Para alcançar esses objetivos, procedeu-se através de pesquisas bibliográficas relacionadas ao reconhecimento através da biometria, com foco na biometria multimodal. Também foi realizada uma pesquisa de campo acerca do conhecimento e a aceitação pelo usuário em relação ao uso da biometria como forma de autenticação.

Espera-se demonstrar com este estudo a importância do uso da autenticação biométrica em *mobile banking*, bem como suas principais vantagens e desvantagens, normas, vulnerabilidades e por fim, verificar sua aceitação pela sociedade.

O presente trabalho foi então estruturado em 6 capítulos. No primeiro capítulo, apresentam-se o histórico e os principais tipos de biométrica; o segundo capítulo proporciona uma análise sobre os tipos de autenticação biométrica; no terceiro capítulo, apresenta-se o funcionamento e componentes dos dispositivos móveis; o quarto capítulo proporciona uma análise sobre o *mobile banking* e sua crescente adoção; no quinto capítulo é realizado o estudo de viabilidade sobre a autenticação com biometria multimodal, através de análise de desempenho, vantagens e desvantagens, vulnerabilidades, normas e por uma pesquisa de aceitação; em considerações finais são elucidadas as conclusões do estudo, bem como considerações acerca do tema, apresentação dos resultados da pesquisa realizada, e por fim são indicados temas para trabalhos futuros relacionados a formas alternativas de reconhecimento biométrico que ainda estão em fase de testes.

1 BIOMETRIA

A palavra biometria vem do grego: *bios* (vida) *metron* (medida). Consiste em um método automático de reconhecimento individual baseado em medidas biológicas e características comportamentais. As biometrias mais comumente implementadas ou estudadas incluem as impressões digitais, reconhecimento de face, íris, voz, e até a geometria das mãos. Todo sistema biométrico é preparado para reconhecer, verificar ou identificar uma pessoa que foi previamente cadastrada.

1.1 Histórico

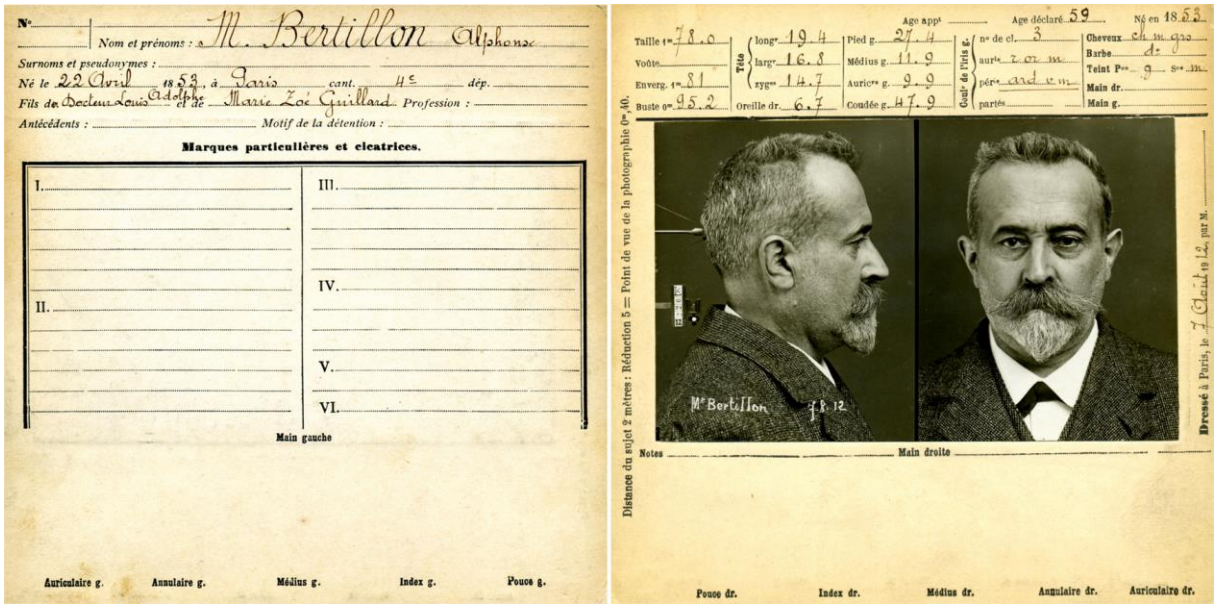
O primeiro método de identificação biométrica oficialmente aceito surgiu em 1879. O método (vide Figura 1) foi desenvolvido por Alphonse Bertillon, na época também chamado de Bertillonage em homenagem ao seu criador, o sistema antropométrico se baseava na combinação de medidas físicas como a dimensão da cabeça, as impressões digitais dos dedos polegar, médio, anular e indicador direitos tiradas de acordo com elaborados procedimentos. As métricas junto com cor de cabelo, de olhos e fotos de frente e de perfil eram arquivadas em um cartão conforme Figura 2. (MESSIAS, 2007).

Figura 1 – Sistema antropométrico de Alphonse Bertillon

Fonte: (Grand Rapids Historical Commission)

A técnica foi adotada pela polícia de Paris em 1882 e rapidamente copiada por toda a França e Europa. O método de Bertillon fracassou devido à dificuldade de classificação, armazenamento e consulta dos dados coletados, além do fato de com o passar dos anos as medidas e a aparência mudam.

Figura 2 – Cartão de Alphonse Bertillon



Fonte: (Grand Rapids Historical Commission)

Posteriormente o método de Bertillon foi substituído por outro sistema baseado em impressões digitais, criado por William Herschel. Herschel era magistrado principal em Hooghly – Índia, e estava com problemas no cumprimento de contratos com os comerciantes locais. Herschel notou a necessidade de identifica de maneira única os habitantes, até mesmo aqueles não alfabetizados, então teve a ideia de pedir que colocassem a assinaturas e a impressão digital nos documentos. (MESSIAS, 2007).

Conforme descrito em seu livro “The Origin of the finger prints”, Herschel chegou à conclusão que as impressões digitais não se repetem nas pessoas e que elas não mudam com o tempo. Posteriormente, Herschel aplicou este mesmo método nas prisões com o objetivo de reconhecer os reincidentes que usavam nomes falsos. Devido à eficácia desse método, a Índia Inglesa sancionou uma lei para o uso desse sistema, que serviria também posteriormente como base para os estudos de Francis Galton. (ARAÚJO; PASQUALI, 2004).

Em 1870 o médico escocês Henry Faulds, que fundou o Hospital Tsukiji em Tóquio - Japão, começou a vislumbrar nas digitais um caminho para comprovar identidades. Faulds contribuiu com as análises dos pontos característicos, a analogia entre as impressões humanas e dos primatas, estudos sobre hereditariedade e etnia, utilização dos termos "*loop*" ("*Where the loops occur the innermost lines...*") e "*whorl*" *("…on both thumbs form similar spiral whorls*") para designar os padrões encontrados nas impressões digitais, nomenclaturas estas que seriam posteriormente utilizadas por Galton e Henry. (ARAÚJO; PASQUALI, 2004).

Em 1880, Galton tomou conhecimento dos trabalhos de Henry Faulds e Willian Herschel e reconhece ser o sistema baseado nas impressões digitais superior ao de Alphonse Bertillon, que até o momento mais o fascinava, devido às características antropológicas que este sistema adotava. Galton contribuiu para o processo que consiste na contagem de linhas, que para ser executada os Papiloscopistas utilizam uma lupa. Tal linha, em homenagem a Francis Galton, é chamada de "Linha de Galton". (ARAÚJO; PASQUALI, 2004).

A classificação final ficou por conta do oficial Edward Richard Henry que, juntamente com Azizul Hacque e Hemchandra Bose, criou e adotou na cidade indiana de Bengala em 1897, um sistema que proporciona o arquivamento das impressões digitais por classificação (Figura 3) o que facilita a busca de uma pessoa dentre várias outras. O sistema de classificação de Henry baseava-se nos tipos que podiam ser encontrados nos dez dedos das mãos, conforme Figura 3. Esses tipos eram anotados com a primeira letra do nome, A, R ou U, W ou C, e colocados acima de cada datilograma: (ARAÚJO; PASQUALI, 2004)

- *Arch*: as linhas formam-se de um lado e tendem a sair do outro lado da digital. Mostram forma abaulada e não apresentam deltas.
- *Radia Loop*: as linhas se formam à esquerda, curvam-se no centro e tendem a retornar para o mesmo lado de formação. Apresentam um delta à direita da região nuclear.
- *Ulnar Loop*: as linhas se formam à direita, curvando-se no centro com tendência a retornar para o mesmo local de formação. Apresenta um delta à esquerda da região nuclear.

- *Whorl*: apresenta dois deltas, sendo um à direita e outro à esquerda do núcleo. As cristas internas a esses deltas apresentam um padrão concêntrico, espiralado, oval ou mesmo sinuoso com um centro bem definido.
- *Composites*: linhas semelhantes aos padrões *loop, whorl* e *arch*.

Figura 3 – Tipos de classificação de acordo com o Sistema Henry

Fonte: (ARAÚJO; PASQUALI, 2004)

O sistema funcionou tão bem que foi adotado em toda Índia. Pouco tempo depois, um comitê da Scotland Yard testou e aprovou o sistema, implantado na Inglaterra em 1901. (GASPAR, 2009).

No Brasil o método de Bertillon chegou a ser adotado em 1894, porém posteriormente foi substituído pelo método de Juan Vucetich Kovacevich, conforme Decreto nº 4.764, art. 57, parágrafo único, de 5 de Fevereiro de 1903 (BRASIL):

> Art. 57 – a identificação dos delinquentes será feita pela combinação de todos os processos atualmente em uso nos países mais adiantados, constando do seguinte, conforme o modelo do Livro de Registro Geral, anexo a este Regulamento:
> a) exame descritivo (retrato falado);
> b) notas cromáticas;
> c) observações antropométricas;
> d) sinais particulares, cicatrizes, tatuagens;
> e) impressões digitais;
> f) fotografia de frente de perfil.
> Parágrafo Único – Estes dados serão na sua totalidade subordinados à classificação dactiloscópica, de acordo com o método instituído por D. Juan Vucetich, considerando-se, para todos os efeitos, a impressão digital como prova mais concludente e positiva da identifidade do indivíduo, dando-se-lhe a primazia no conjunto das outras observações, que servirão para corroborá-la.

1.2 Tipos de Biometria

Com o desenvolvimento da tecnologia, os métodos de autenticação biométrica foram sendo descobertos gradativamente. Atualmente temos diversas formas de se identificar um indivíduo, porém nem todas são razoavelmente aceitas ou viáveis. Podem ser divididas em características físicas, que incluem partes do nosso organismo, ou em características comportamentais, que podem ser identificadas no padrão de digitação, uso do mouse, uso do *smartphone,* voz, dentre outras.

Os sistemas biométricos utilizam basicamente quatro estágios que devem ser corretamente aplicados: (Consultores Biométricos)

- **Captura** - Um exemplo físico ou comportamental é capturado pelo sistema durante o cadastramento;
- **Extração** - Um dado único é extraído do exemplo e um *template* é criado;
- **Comparação** - O *template* é então comparado com um novo exemplo;
- **Combinação/Não- Combinação** - O sistema decide se o atributo extraído do novo exemplo constitui um par ou não.

No estágio da comparação, as amostras biométricas podem ser comparadas de dois modos distintos: Verificação e Identificação. O Quadro 1 retrata a comparação entre os modos.

Quadro 1 – Modos de comparação de uma amostra biométrica

Comparação	**Verificação**	**Identificação**
Modo	1:1	1:N
Reconhecimento	Positivo	Negativo
Pergunta	Esta amostra biométrica pertence à ABC?	A quem pertence esta amostra biometria?

Fonte: (PERETTI, 2015)

Na fase de reconhecimento, a identificação só pode ser positiva quando diferentes indivíduos são impedidos de utilizar a mesma identidade. Um reconhecimento é negativo quando impede que um único indivíduo faça uso de diferentes identidades.

O reconhecimento através de métodos biométricos físicos consiste na identificação baseada nas características físicas do indivíduo, como por exemplo, a face, impressão digital, padrão de veias da mão, retina íris, dentre outras. Já o reconhecimento através de métodos biométricos comportamentais consiste na identificação do indivíduo através do que ele realmente é, e não depende do que ele sabe ou possua. São exemplos de biometria comportamental o modo de caminhar, o movimento labial, a voz, a dinâmica de digitação, desafios cognitivos, dentre outros.

1.2.1 Impressão digital

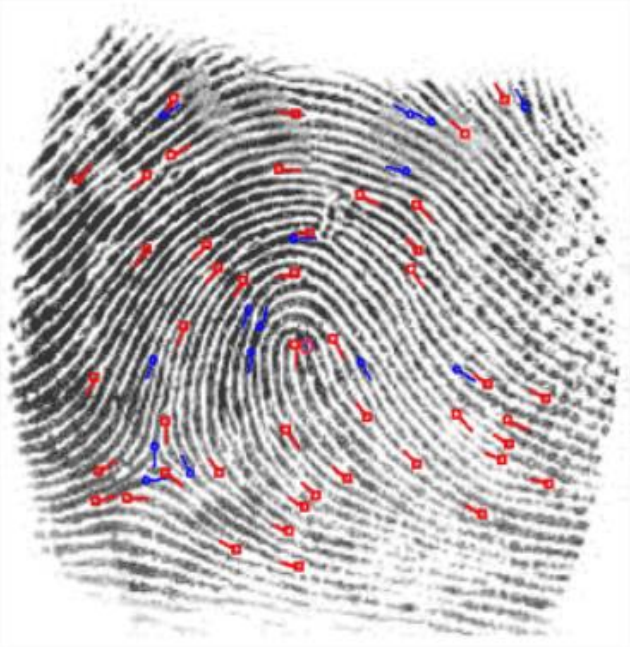
Considerada uma das formas mais antigas de reconhecimento, a impressão digital está sendo o método de autenticação biométrico mais utilizado. Atualmente podemos encontrar leitores por toda parte, seja em relógios para registro de ponto nas empresas, academias, universidades, bibliotecas, catracas de edifícios corporativos, *smartphones, notebooks,* e até nos terminais de autoatendimento bancário.

Na identificação pela impressão digital, são usados algoritmos que analisam a posição de detalhes como as terminações, bifurcações, cruzamentos e indeterminado. Uma digital tem em média entre 30 e 40 detalhes únicos, e conforme estudos do FBI, duas pessoas não apresentam mais do que 8 pontos coincidentes. (MÜLLER, 2007).

Pinheiro (2008) afirma que as impressões digitais são únicas para cada indivíduo e são consideradas o segundo tipo biométrico mais seguro para determinar a identidade, sendo o primeiro o teste de DNA. Para o reconhecimento através de impressões digitais é necessário utilizar um dispositivo capaz de capturar com precisão as minúcias, e também de um software que analise a imagem capturada e faça o reconhecimento da digital. É o tipo biométrico mais utilizado em todo mundo, pouco invasivo ao usuário e de baixo custo.

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), onde o sistema compara características biométricas com a informação previamente registradas no banco de dados, e um-para-um (1:1) onde o sistema efetua a busca em todo um banco de dados, analisam as minúcias (Figura 4). 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. (Consultores Biométricos).

Figura 4 – Minúcias da impressão digital



Fonte: (International Biometric Group)

Reconhecimento

O processo de reconhecimento pode ser dividido basicamente em duas etapas, sendo que a primeira consiste em identificar e cadastrar o indivíduo (Figura 5), e a segunda consiste em identificar e autenticar ou não um indivíduo (Figura 6).

Figura 5 – Fluxo de identificação e cadastramento

Fonte: (BASTOS et al., 2008)

Figura 6 – Fluxo de identificação e autenticação

Fonte: (BASTOS et al., 2008)

Captura

Uma diferença chave entre as várias tecnologias de digitais no mercado é a forma de captura da imagem, que pode obtida de diversas formas basicamente classificadas de acordo com o tipo do Sistema de verificação.

Sistemas de verificação um-para-um (1:1)

Utilizam as principais técnicas de captura descritas abaixo: (Consultores Biométricos)

- **Óptica** – envolve geração de luz, a qual é refracionada através de um prisma em uma superfície de vidro onde o dedo é colocado. A luz ilumina a ponta do dedo e a impressão é feita pela imagem que é capturada.
- **Capacitiva** - utilizam sensores de captação de silício que medem as cargas elétricas através de um sinal elétrico quando o dedo é colocado em sua superfície. 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, e nenhum sinal é gerado pelos vales. Essas variações na carga elétrica produzem a imagem digital.
- **Térmica** – elimina os problemas de pele ressecada ou molhada, porém pode sofrer variações na representação das características.
- **Ultrassónica** – utiliza ondas de som abaixo do limite de audição humano. O dedo é colocado no scanner e ondas acústicas são usadas para medir a profundidade dos sulcos com base no sinal refletido.

Sistemas de verificação um-para-muitos (1:N)

Capturam imagens digitais usando a técnica óptica ou por varredura eletrônica das imagens de um papel:

- **Óptica**: para identificações padrões um-para-muitos (1:N), os indivíduos são cadastrados usando um processo de captura óptica em tempo real. Sistemas AFIS (*Automated Fingerprint Identification System*) de Forças Policiais, também conhecidos como estações de cadastramento, capturam as imagens de todos os dez dedos. (Consultores Biométricos).
- **Varredura eletrônica**: Um AFIS (*Automated Fingerprint Identification System*) 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*). (Consultores Biométricos).

O AFIS (*Automated Fingerprint Identification System*) é predominantemente usado para Forças Policiais, mas também vem impressionando nas aplicações civis. Para forças policiais, as imagens digitais são coletadas de cenas de crimes, conhecidas como impressões latentes, ou são tomadas de suspeitos criminais quando eles são apreendidos. Em aplicações civis, como em esquemas de identificação nacional de larga escala, as imagens digitais podem ser capturadas através do posicionamento do dedo em um scanner ou através da varredura óptica de uma impressão com tinta num papel. Um AFIS pode varrer e capturar dados de imagens digitais e então comparar o dado capturado com o banco de dados. (Consultores Biométricos).

Extração

Após o processo de captação, é necessário realizar a extração de características da digital. As características extraídas são armazenadas em bancos de dados na forma de *Templates.* O processo de extração está dividido em basicamente em quatro etapas:

- **Melhoramento da imagem** – Transformada de Fourier, Exponenciação e Transformada inversa. (CASTRO, 2008).
- **Binarização da imagem** – consiste em transformar as linhas da impressão digital, adquiridas em 256 níveis de cinza a dois níveis: preto e branco. O processo não pode destruir as minúcias, terminação de linha e bifurcações, presentes na impressão digital. (CASTRO, 2008).
- **Esqueletização** – consiste em reduzir os dados redundantes e preservar a continuidade das cristas de uma impressão. O esqueleto deve ter todas as informações contidas na imagem original: posição, orientação e comprimento dos segmentos. (CASTRO, 2008).

- **Extração** – consiste em identificar as características a serem posteriormente utilizadas como base para comparação e confirmação da identidade do indivíduo. (CASTRO, 2008).

Comparação

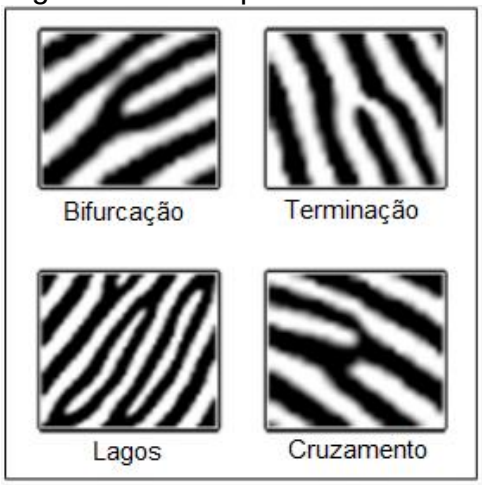
A etapa de comparação é responsável por identificar as características comuns entre um exemplar de impressão digital e outro previamente cadastrado. Os sistemas biométricos geralmente armazenam essas características em bancos de dados na forma de *Templates.* As principais técnicas utilizadas são o método das Minúcias e o da Correlação.

As técnicas baseadas no método das minúcias, que consistem na identificação extração das mesmas, e posteriormente no mapeamento e comparação dessas, pode ser bastante oneroso em termos de processamento, e principalmente se a imagem for de baixa qualidade. Outro item a ser levado em consideração é que no método de identificação pelas minúcias, não se leva em conta o padrão das cristas e sulcos.

As minúcias podem ser classificadas basicamente em quatro tipos (Figura 7):

- **Bifurcação** – caracterizada pele convergência de duas cristas paralelas;
- **Terminação** – caracterizada pela finalização abrupta de uma crista;
- **Lagos** – caracterizada pela união de duas bifurcações em uma mesma crista;
- **Cruzamento** – caracterizada pela intersecção da crista com uma bifurcação;

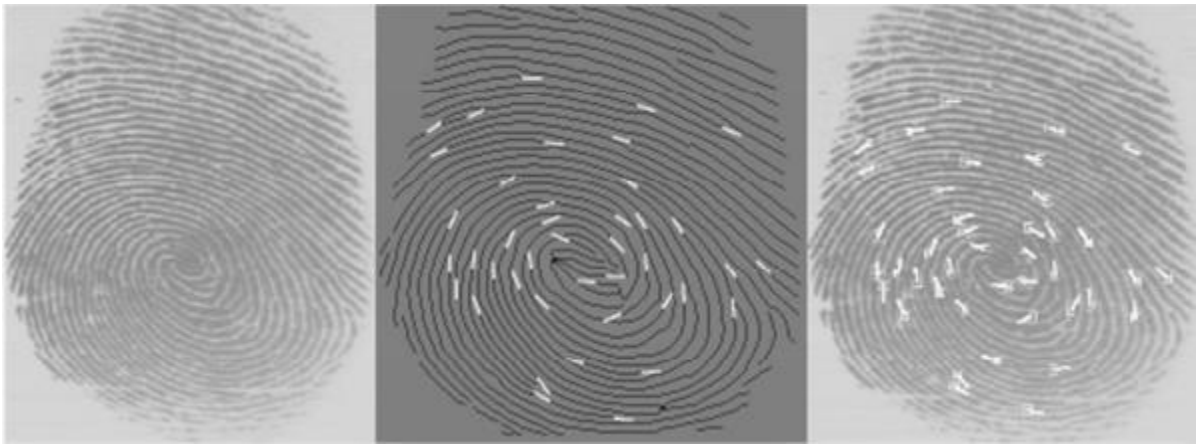
Figura 7 – Exemplos de minúcias



Fonte: (CASTRO, 2008)

O método de Correlação é baseado nas informações relacionadas às cristas da impressão digital, e não às minúcias. Conforme a Figura 8, nesse método vetores são mapeados em cada crista identificada, e posteriormente a comparação é feita levando em consideração a coerência e ao ângulo entre as imagens. Sua principal desvantagem se deve a necessidade da imagem a ser comparada estar no mesmo ponto central e ângulo da imagem previamente cadastrada.

Figura 8 – Exemplo de correlação por vetores



Fonte: (KAMAROSKI; BARDELLI, 2008)

Podemos encontrar outros métodos como por exemplo o da Confiabilidade, onde a identificação é feita através de um cálculo do nível de semelhanças das impressões digitais comparadas, descartando a necessidade dos exemplares estarem na mesma posição.

A maioria dos sensores de impressão digital apresentam interferência no reconhecimento de digitais, quando há sujeira ou ressecamento nos dedos. Ainda há usuários que possuem uma digital muito superficial, e há outros que trabalham com produtos químicos em contato com as mãos, o que dificulta ainda mais o processo de identificação.

1.2.2 Face

A face é a principal forma que as pessoas utilizam para reconhecer e recordar umas das outras. Inconscientemente criamos vários *Templates* com a imagem facial das pessoas que conhecemos e armazenamos em uma “base de dados”. Mas até

mesmo nós nos confundimos e por ventura nos enganamos ao reconhecer uma pessoa.

O reconhecimento pela face é baseado na análise do indivíduo através da leitura da face, um processo complexo que normalmente requer artifícios inteligentes sofisticados e técnicas de aprendizagem computacional (*machine learning techniques*). A inteligência artificial é necessária para simular a interpretação humana das faces, se adaptando às diversas mudanças que ocorrem com estas e para comparar precisamente os novos exemplos com os *Templates* previamente armazenados. (PINHEIRO, 2008)

O processo de detecção da face consiste em mapear suas características, como por exemplo a localização da boca, olhos, nariz, cor de pele, contorno da face, sobrancelhas, dentes, etc. Esse mapeamento é muito utilizado principalmente em situações em que há outros objetos no campo de captura da imagem, ou onde há objetos obstruindo partes da face, como por exemplo óculos, bigode ou barba.

O método de detecção de face é considerado de alta aceitabilidade e universalidade, além da fácil coletabilidade, até mesmo sem necessidade de interação do usuário. Pode ser dividido entre imagens estáticas, no caso de fotos, ou dinâmicas no caso de vídeos. Variações na iluminação, ruídos e objetos na imagem, podem influenciar na eficiência dos algoritmos.

Para Vigliazzi (2006), os programas tecnicamente mapeiam a geometria e as proporções da face para reconhecer o rosto de um indivíduo. São registrados vários pontos delimitadores na face, os quais permitem definir proporções, distâncias e formas de cada elemento do rosto e, com base nesses dados, iniciar as comparações. Os pontos principais são: olhos, nariz, queixo, maçãs do rosto, orelhas e lábios.

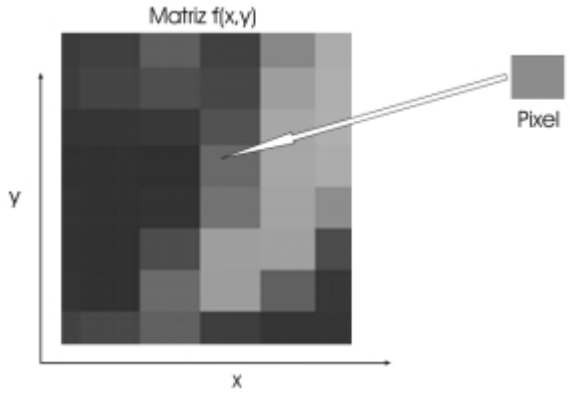
Vigliazzi (2006) completa afirmando que a tecnologia de reconhecimento facial leva em conta as medidas do rosto que nunca se alteram, mesmo que a pessoa seja submetida a cirurgias plásticas. As medidas básicas são:

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

O processo completo de reconhecimento facial consiste basicamente em três etapas: captura da imagem, extração dos padrões e comparação de características faciais.

Uma imagem digital refere-se à função bidimensional de intensidade de luz f(x,y), onde x e y denotam as coordenadas espaciais e o valor de f em qualquer ponto (x,y) é proporcional ao brilho (ou nível de cinza) da imagem naquele ponto (Figura 9). A imagem digital pode ser considerada como sendo uma matriz cujos índices de linhas e colunas identificam um ponto na imagem e o correspondente valor do elemento da matriz identifica o nível de cor naquele ponto. Os elementos dessa matriz digital são chamados de elementos da imagem, elementos da figura "pixels". (Tecnologia Radiológica).

Figura 9 – Representação matemática de uma imagem



Fonte: (Tecnologia Radiológica)

A essa grade de quadrados chamamos de "imagem matriz", e cada quadrado na imagem é chamado de pixel. O pixel é a abreviatura para “*picture element*” ou elemento de uma imagem. É a menor parte de uma imagem digital e cada um destes pontos contém informações que determinam suas características. O pixel é usado como unidade de medida para descrever a dimensão geométrica de uma imagem. Quanto mais pixels por polegada tiver uma imagem melhor será a qualidade ou resolução. Cada pixel carrega a informação sobre o nível de cinza ou cor que ele representa. (Tecnologia Radiológica).

O processo de aquisição de imagens da face consiste em obter um registro com as características individuais. Atualmente as imagens podem ser adquiridas basicamente em quatro formas distintas: (COSTA; OBELHEIRO; FRAGA, 2006)

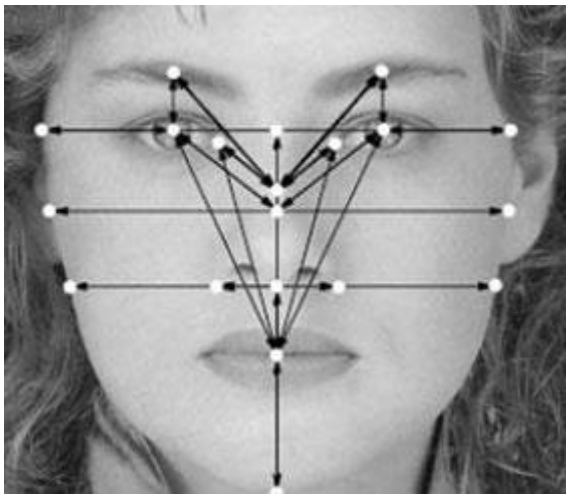
- **Imagem 2D** – as imagens da face são registradas em duas dimensões (eixos x e y) e podem ser obtidas de forma estática, quando originadas por exemplo de fotos digitalizadas de documentos, ou podem ser obtidas de forma dinâmica, onde são obtidas ao vivo utilizando câmeras analógicas ou digitais. Sistemas baseados em imagens 2D geralmente apresentam problemas no reconhecimento. Isso ocorre devido ao método ser influenciado pelo ângulo de visão, variações de iluminação, reflexos ou mudanças na face, como barba, bigode, uso de óculos, até mesmo o próprio envelhecimento.
- **Imagem 3D** – as imagens são registradas três dimensões (eixos x, y e z), e consequentemente contêm mais informações. É baseada na geometria da cabeça do usuário é invariante à pose. Uma desvantagem dos modelos que utilizam imagem 3D é não tratar expressões faciais, pois tratam a face como um objeto rígido.
- **Sequência de imagens** – as imagens da face são obtidas através de câmeras que registram uma sequência de vídeo, com uma frequência de inclusão de 1 a 4 quadros por segundo. Devido à baixa amostragem a resolução das imagens da cace é de baixa qualidade, tornando difícil a sua utilização em sistemas de reconhecimento facial. Câmeras com propriedades de zoom que permitam focar no rosto do indivíduo podem ser usadas para melhorar a resolução, embora se perca parte do campo de visão.
- **Termograma da face** – as imagens da face são obtidas utilizando radiação infravermelha de baixa potência, invisível ao olho humano, e podem ser capturadas em ambientes sem iluminação. Esse método é utilizado como suplemento no processo de detecção da face, entretanto, outras fontes de calor podem afetar o processo de identificação.

Técnicas padrões de vídeo usam uma imagem facial, ou uma coleção de imagens, capturadas 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. (Consultores Biométricos).

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 sanguíneas 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 câmeras padrões. (Consultores Biométricos).

No processo de extração o objetivo é fazer com que a imagem recém-capturada fique no mesmo padrão, tamanho, resolução e posição de outras imagens existentes na base de dados armazenadas como *templates*. Primeiramente são selecionados apenas os setores relevantes da imagem, e após a seleção toda a informação relevante é extraída da imagem. Para extrair essas informações, alguns algoritmos utilizam-se de vetores que melhor representam a distribuição da imagem da face (Figura 10).

Figura 10 – Representação dos vetores



Fonte: (FERNANDES, 2011)

Uma das técnicas mais utilizadas devido à sua simplicidade é o algoritmo PCA (Análise de Componentes Primária). É uma técnica estatística utilizada para reduzir a dimensionalidade de um conjunto de dados onde há um grande número de variáveis inter-relacionadas. Isto é feito de forma que o máximo de variância presente nos dados seja mantido. (SILVA, 2008).

A PCA tem como objetivo determinar uma transformação linear de um conjunto de *n* variáveis originais $X_1, X_2, ..., X_n$ em um novo conjunto de *p* variáveis $Y_1, Y_2, ..., Y_p$ de forma que essas últimas sejam descorrelacionadas. Essas novas variáveis $Y_1, Y_2, ..., Y_p$ precisam ter a mesma variância das variáveis originais e estejam ordenadas de tal forma que $var(Y_1) \geq var(Y_2) \geq var(Y_p)$. Essas novas variáveis Y_p são chamadas Componentes Principais. (SILVA, 2008).

Na etapa de comparação, um determinado *template* é comparado com um conjunto de vários outros *templates* existentes na base de dados do sistema. O processo de comparação é baseado em três tipos de métodos: holísticos, estruturais e híbridos:

1. **Métodos holísticos** - usam toda a região da face no processo. Dentre as várias técnicas existentes, a análise de componentes principais (PCA), baseada em *Eigenfaces* (Autofaces), é a mais utilizada. (COSTA; OBELHEIRO; FRAGA, 2006).

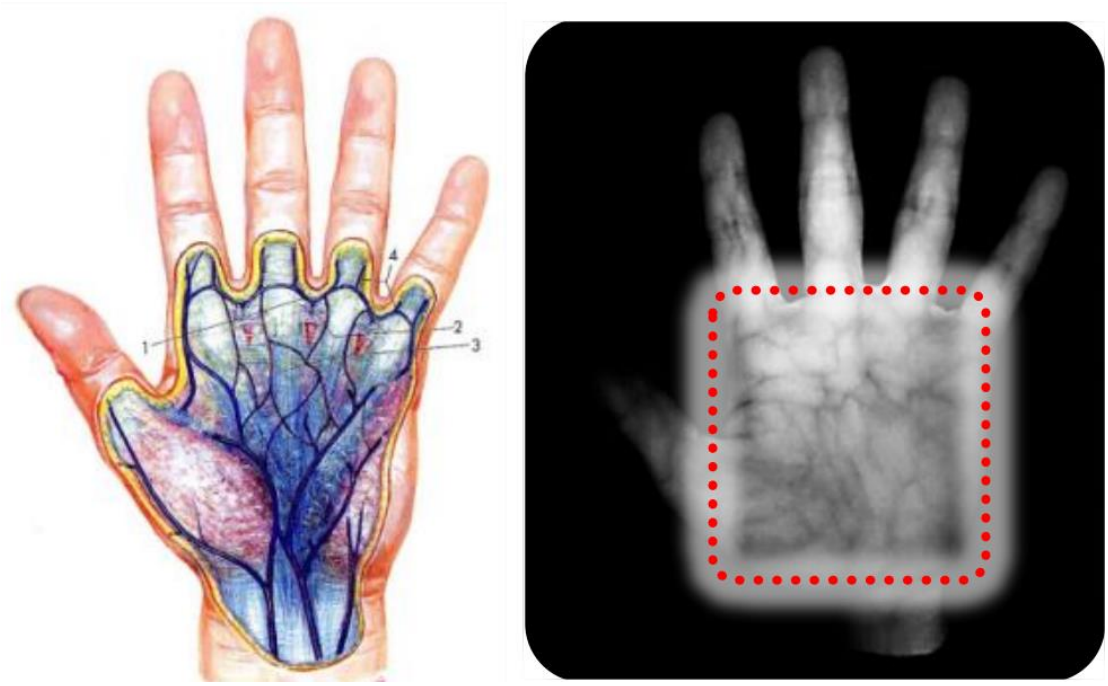
2. **Métodos estruturais** - utilizam medidas geométricas (ângulos e distâncias) relativas entre diversos pontos, como olhos, nariz, boca e bochechas. (COSTA; OBELHEIRO; FRAGA, 2006).

3. **Métodos híbridos** – fornecem o melhor dos dois métodos anteriores, na tentativa de se aproximar do sistema de percepção humano, que se utiliza tanto da aparência global da face quanto das características locais. (COSTA; OBELHEIRO; FRAGA, 2006).

1.2.3 Padrão de veias da mão

O reconhecimento através do padrão das veias da mão apresenta uma confiabilidade enorme, além da praticidade para o usuário final, já que não é necessário contato físico. Algumas instituições financeiras do Brasil já estão adotando esse método de autenticação em seus terminais de autoatendimento. Outro fator que chama a atenção é que para realizar a captura é necessário possuir sangue fluindo pelas veias (Figura 11), o que impossibilita que uma mão decapitada seja utilizada.

Figura 11 – Veias da palma da mão



Fonte: (Fujitsu)

O processo de captura é simples, podendo ser feita com dispositivos que utilizam sensores com feixe de luz visível ou sensores com luz infravermelho, já que a hemoglobina absorve os raios infravermelhos, fazendo com que as veias apareçam em cor preto na imagem digital.

Apesar do processo de captura ser considerado simples, sistemas baseados nesse método fazem um pré-processamento da imagem com o uso de filtros de ajuste do contraste e do brilho para obter as características do padrão das veias. Este pré-processamento auxilia na etapa de segmentação da imagem, que consiste

em limiarizar a imagem para segmentar as veias da palma da mão, e posteriormente aplicar filtros Gaussianos afim de reduzir os ruídos da imagem. (SOUZA, 2012).

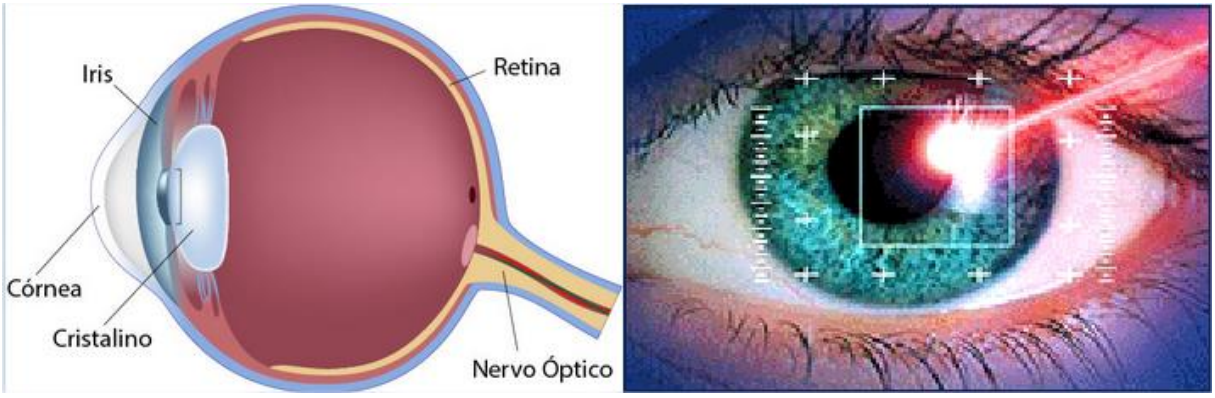
O reconhecimento é baseado na análise das características, como a forma, espessura e localização espacial das veias. Tanto a região da palma quanto a do dorso podem ser utilizadas para o reconhecimento baseados no padrão das veias, que é imutável e único para cada indivíduo. (SOUZA, 2012).

1.2.4 Íris

A íris (Figura 12) é a parte colorida do nosso olho e está localizada ao redor da pupila. Ela pode ter várias cores, em sua maioria preto, castanho, azuis e verdes, e tem como função controlar a quantidade de luz que entra no olho, através do controle de abertura da pupila. Segundo Pinheiro (2008), a íris apresenta 249 pontos de diferenciação que podem ser utilizados no reconhecimento de um indivíduo.

Vários fatores podem influenciar na detecção das características da íris, como por exemplo, a iluminação, doenças que causam a má formação da íris (Aniridia), embaçamento da visão (Catarata) ou até mesmo o surgimento de um tumor (Melanoma).

Figura 12 – Anatomia do olho



Fonte: (Tranjan Hospital de Olhos)

Já Vigliazzi (2006) considera o reconhecimento através da íris estável e seguro, já que é as caraterísticas subjetivas, como por exemplo, o tecido que divide

a íris, não sofrem mudança com o envelhecimento do indivíduo, e também pela complexidade única da íris.

A captura da imagem da íris é feita por meio de câmeras, em ambiente com luz visível e infravermelha. Outro fator importante para a qualidade da imagem capturada é a distância entre o olho do indivíduo e a câmera, já que mais detalhes são capturados quando o indivíduo está dentro do campo de visão da câmera. (NAKAMOTO, 2012).

Pinheiro (2008) define os procedimentos de reconhecimento da íris em três etapas:

1- Segmentação da imagem da íris da imagem capturada inicialmente;

2- Execução de algoritmo de extração para segmenta a íris da pupila;

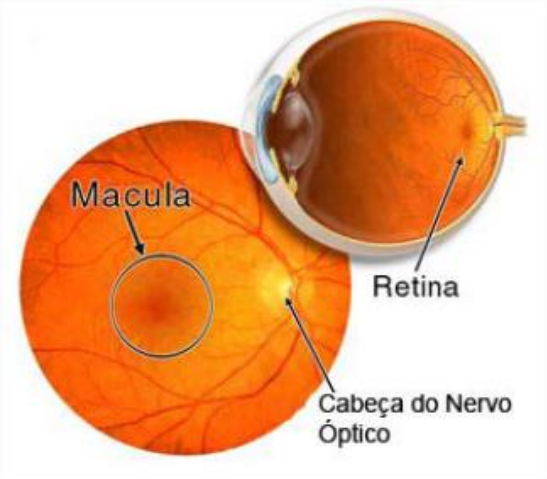
3- Extração das características para gerar o *template* a ser armazenado no banco de dados.

1.2.5 Retina

A retina é uma fina membrana que reveste o interior do olho, repleta de receptores sensíveis a luz, e possui a função de transmitir estímulos nervosos ao cérebro. Essa membrana possui vasos sanguíneos e seu padrão é considerado único. (GTA).

O reconhecimento através da retina é preciso e seguro, porém o custo é elevado e o processo de captura da imagem da íris exige muito da interação do indivíduo. Assim como o reconhecimento da íris, o indivíduo tem que se posicionar a uma distância aceitável da câmera e olhar para um ponto específico, onde através de luz infravermelho a câmera possa focalizar e capturar os padrões. (VIGLIAZZI, 2006).

Figura 13 – Visualização dos vasos sanguíneos da retina



Fonte: (GTA)

Os sistemas de reconhecimento através da retina utilizam os padrões dos vasos sanguíneos para a identificação do indivíduo. Os padrões que compreendem a espessura e forma do vaso sanguíneo, além de sua localização espacial, são extraídos das imagens e são utilizadas para o processo de classificação. Por utilizar um feixe de luz sob os olhos do indivíduo para poder adquirir uma imagem do padrão dos vasos sanguíneos da retina, o processo é considerado altamente invasivo, além do fato que as imagens capturadas são altamente ruidosas. (SOUZA, 2012).

1.2.6 Voz

Segundo Pinheiro (2008) o método de reconhecimento através da voz é considerado vulnerável e impreciso, pois apresenta interferência de aspectos internos e externos como ruídos e estado emocional do indivíduo. Além do fato de que vários tipos de patologias como por exemplo a laringite, podem influenciar com rouquidão ou até mesmo privar temporariamente a voz de um indivíduo, prejudicando a qualidade e ocasionando falhas no reconhecimento.

Para análise da voz os protocolos consideram padrões harmônicos e a pronúncia de textos, levando-se em consideração a forma dos intervalos vocais, que modificam o índice espectral de uma onda acústica enquanto passa por meio dele, resultando na fala. (NAKAMOTO, 2012).

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 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. (Consultores Biométricos)

O processo de aquisição é considerado fácil, tornando o processo de aceitação do usuário mais rápido. Atualmente os sistemas de reconhecimento por voz se dividem em 4 classes:

1. **Texto Fixo** – Durante a fase de registro o usuário pronuncia uma palavra ou frases pré-determinadas pelo sistema, que posteriormente serão utilizadas na fase de reconhecimento (COSTA; OBELHEIRO; FRAGA, 2006).
2. **Dependente do Texto** – na fase de registro o sistema solicita ao usuário que pronuncie palavras ou frases previamente registradas pelo sistema, tornando o procedimento de registro mais longo do que na classe anterior. Na fase de reconhecimento, o sistema solicita ao usuário que pronuncie palavras ou frases específicas (COSTA; OBELHEIRO; FRAGA, 2006).
3. **Independente do Texto** – o usuário possui liberdade de registrar as frases que lhe convêm. O sistema reconhece qualquer discurso do usuário. (COSTA; OBELHEIRO; FRAGA, 2006).
4. **Conversacional** – utiliza um protocolo misto de conhecimento e biometria. O usuário deve responder perguntas cujas respostas são secretas. (COSTA; OBELHEIRO; FRAGA, 2006)

O processo de extração das características é baseado em três formas diferentes, onde essas características são representadas por uma sequência de vetores: (1) por meio de PCA (*Principal Component Analysis*) e FA (*Factor Analysis*);

(2) por estimativas de médias e covariâncias; e (3) por estimativas de divergências (COSTA; OBELHEIRO; FRAGA, 2006).

Na fase de extração, o processo de comparação das características extraídas dos dados de voz pode ser feito por vários métodos, segue exemplos:

- **DTW** (*Dynamic Time Warping*) - Este método é mais utilizado nos sistemas dependentes do texto. Permite a compensação da variabilidade humana inerente ao padrão de voz (COSTA; OBELHEIRO; FRAGA, 2006).
- **MÉTODOS ESTATÍSTICOS** (HMM e GMM) - Estes métodos operam na modelagem paramétrica do sinal de voz. A modelagem pode ser dependente do tempo ao utilizar cadeias de Markov ocultas (HMM), ou não dependentes do tempo ao se utilizar modelos de misturas Gaussianas (GMM). Em ambos os métodos os valores dos parâmetros devem ser obtidos por intermédio de um treinamento de dados (COSTA; OBELHEIRO; FRAGA, 2006).
- **VQ** (*Vector Quantisation*) – método raramente é utilizado em sistemas, pois seu desempenho está condicionado à quantidade de dados disponíveis. (COSTA; OBELHEIRO; FRAGA, 2006).
- **Redes Neurais** – é utilizado em sistemas independentes do texto. Em pesquisas é realizado treinamento das características com usuários legítimos e impostores (COSTA; OBELHEIRO; FRAGA, 2006).
- **SVM** (*Support Vector Machines*) – método utilizado em teorias de aprendizagem estatísticas. Os resultados têm sido superiores aos métodos GMMs. (COSTA; OBELHEIRO; FRAGA, 2006).

Os sistemas de reconhecimento de voz são considerados simples de serem utilizados, porém as taxas de erro são muito dependentes da aplicação. Ainda há problemas relacionados ao usuário, ambiente e até mesmo ao canal, que acabam influenciado na qualidade do sinal de voz adquirido e consequentemente no desempenho. (COSTA; OBELHEIRO; FRAGA, 2006).

1.2.7 Dinâmica de digitação

É uma técnica transparente ao usuário, onde é observado o intervalo em que o indivíduo pressiona as teclas consecutivamente, o tempo em que as teclas permanecem pressionadas, até mesmo a frequência que teclas erradas são digitadas.

O processo de captura de dados para o reconhecimento é transparente e ocorre por meio da própria digitação, ou seja, durante a digitação é realizada a identificação do usuário no sistema (PINHEIRO, 2008). A técnica parte do pressuposto que cada pessoa possui um ritmo diferente de digitação, assim, mesmo se um impostor tiver conhecimento da senha de outro indivíduo, dificilmente conseguirá ser autenticado.

O principal benefício do uso da dinâmica de digitação é a possibilidade de reforçar a segurança da informação, mas com baixo custo. Porém há uma grande desvantagem já que a dinâmica de digitação depende do comportamento do usuário, o que nem sempre é o mesmo. Isso ocorre devido aos indivíduos mudarem de comportamento a qualquer momento em nossas vidas, dependendo ainda em que situação o indivíduo se encontra.

1.2.8 Modo de Caminhar

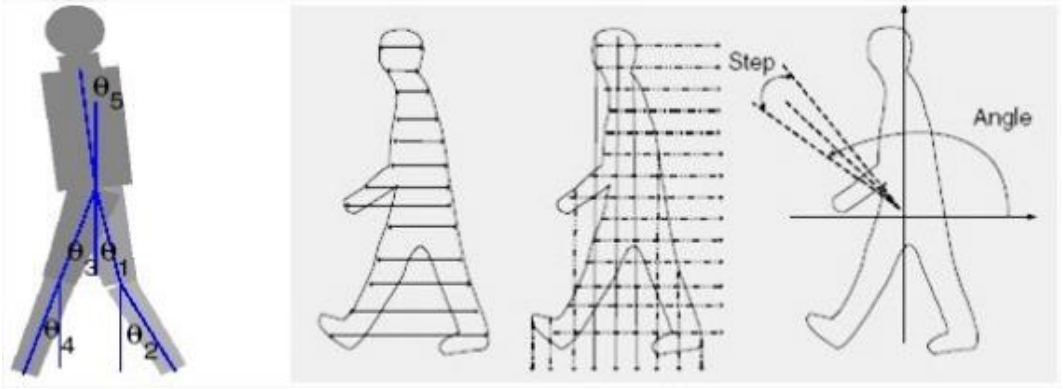
O reconhecimento pelo modo de caminhar é baseado em padrões do caminhar de um determinado indivíduo, onde são observadas características como sua altura, distância entre os passos, postura, frequência dos passos, entre outras. Esse padrão é armazenado em um banco de dados de um determinado sistema, que posteriormente pode identificar o indivíduo previamente registrado.

O processo de reconhecimento de usuário se divide em quatro fases: aquisição de uma sequência de imagens a partir de um vídeo, subtração do plano de fundo da imagem entre o usuário, extração das características e o reconhecimento. (SOUZA, 2012).

Os métodos utilizados (Figura 14) para etapa de classificação podem ser divididos em dois grupos:

- O primeiro é baseado em modelos onde o usuário é classificado através de um modelo esquelético previamente cadastrado. De forma geral, este método guarda medidas de um conjunto de partes do esqueleto do usuário para um reconhecimento posterior. (SOUZA, 2012).

Figura 14 – Métodos de classificação



Fonte: (SOUZA, 2012)

- O segundo método é baseado na coleta de um número estimado de frames de um vídeo. A ideia é associar parâmetros baseados em pontos e ângulos no espaço dimensional da imagem. (SOUZA, 2012).

A técnica baseada no modo de caminhar é considerada não invasiva pois o vídeo pode ser capturado à distância através de câmeras, ainda que sem a necessidade de colaboração do indivíduo. Através de um algoritmo é construído um modelo do padrão de movimento de um indivíduo. Porém a precisão desta técnica pode diminuir, assim como outras técnicas biométricas baseadas no comportamento, caso o indivíduo se mova de modo muito diferente do habitual, o que depende muito da situação e do angulo em que o indivíduo se encontra.

1.3 Considerações Finais do Capítulo

Neste capítulo, descreveu-se de forma resumida o histórico da Biometria e sua utilização pela sociedade como prova de não repúdio. Também foram abordadas uma variedade de técnicas biométricas, comportamentais e físicas, além de descrever suas particularidades nos processos de captura, extração, comparação e combinação.

2 AUTENTICAÇÃO BIOMÉTRICA

Segundo Silva (2008) a autenticação provê a garantia da identidade de um usuário, ou seja, é responsável por verificar se um indivíduo é quem ele diz ser, por meio de suas credencias, sendo que as credencias são as evidências apresentas que comprovem sua identidade como um usuário válido.

Pinheiro (2008) complementa que a identificação é a função em que o usuário declara sua identidade ao sistema, e a autenticação é a função responsável pela validação dessa declaração e que somente após a validação é que o sistema poderá conceder ou negar acesso.

Pinheiro (2008) define três métodos de autenticação de um usuário. Estes métodos podem ser combinados a fim de aumentar o nível de segurança. Os métodos de autenticação são baseados em:

- **No que se sabe**: autenticação condicionada ao que o usuário conhece, como por exemplo, senhas, datas, informações pessoais, etc. É o método menos seguro.
- **No que se possui**: autenticação baseada no que o usuário possui, como por exemplo, *Tokens* e *Smart Cards.* Estes dispositivos utilizam esse método que é mais seguro do que o baseado apenas no que se sabe.
- **No que você é**: autenticação baseada em características individuas do usuário, como por exemplo, impressão digital, disposição das veias da mão, íris, geometria da mão, retina, entre outros. Esta autenticação é considerada a mais segura em relação aos outros métodos.

2.1 Autenticação através do conhecimento

Atualmente é a forma mais utilizada para confirmar uma identidade para um sistema de autenticação. Geralmente é utilizada na forma de senhas, frases de segurança ou número de identificação pessoal (PIN), e é caracterizada por algo que o indivíduo tenha conhecimento.

Segundo Leoncio (2006), a autenticação por senhas contém uma série de deficiências que não a torna confiável. Essa forma de autenticação depende da capacidade dos usuários de criar e memorizar inúmeras senhas, quase sempre de tamanhos e características diferentes. Como a maioria das pessoas não tem muita experiência na hora de criar as senhas, até para evitar esquecê-las facilmente, acabam repetindo senhas criadas anteriormente ou as criam com características de fácil dedução, como por exemplo, datas, nomes, números de telefone, de documentos, placas de carros.

Silva (2008) também identificou alguns problemas para a utilização de identificação por algo-que-você-sabe, conforme descrito abaixo:

- As senhas podem ser facilmente visualizadas ou descobertas, dependendo da criptografia utilizada em seu meio de transporte;
- Um intruso pode acessar um computador do sistema e ler o arquivo de senhas;
- A senha pode ser descoberta através de tentativas;
- A senha de acesso pode ser descoberta através de tentativas com todas as combinações possíveis.

2.1.1 Identificação de usuário e senha

Considerada uma das formas mais utilizadas em sistemas web, a autenticação do usuário é feita através de uma senha, o que torna possível definir níveis de acesso e permissão para usuário, definição da duração do acesso, assim como ocorre em sistemas que a sessão é expirada após um período de tempo.

Um grave problema do uso de senhas está relacionado a capacidade do usuário criar senhas fortes. Senhas fracas e repetidas são comuns na maioria dos sistemas, como por exemplo, nome de filhos ou algum membro da família, datas de nascimento, números de documentos, telefones, sequências de letras ou números (abc, 12345), e o problema ainda é agravado pela ausência de rotatividade de senhas.

Outro problema muito recorrente é o gerenciamento e armazenamento com segurança de credenciais. O compartilhamento de senha ocorre com frequência, já que o indivíduo pode anotar sua senha em um papel e compartilhá-la com quem confia. Anotação em agendas ou arquivos desprotegidos são falhas graves para segurança, e são muito exploradas por indivíduos mal intencionados.

2.1.2 Senhas temporárias

São utilizadas apenas uma vez na autenticação e posteriormente perdem sua validade. Esse tipo de senha evita o ataque de captura e reutilização da senha, já que na próxima autenticação o sistema não aceitará uma senha já utilizada. Conhecidas como códigos *Tokens*, são geradas por um sistema e enviadas para dispositivos físicos que apenas o indivíduo possua acesso, sendo muito utilizadas em Sistemas Bancários. É considerada mais segura do que o método baseado apenas no que se sabe.

2.1.3 Perguntas aleatórias

Nessa forma de autenticação o usuário deve responder a uma série de desafios com informações que ele possua. O sistema gera os desafios baseados nas informações que possui do usuário quando foi cadastrado, como por exemplo, nome da mão, primeiros dígitos do CPF, dia ou ano de nascimento. Geralmente são utilizadas como complemento a uma autenticação com senha. Sistemas Bancários utilizam esse método em seus caixas eletrônicos.

2.2 Autenticação através da propriedade

Autenticação baseada em um objeto ou dispositivo que o indivíduo possui, como por exemplo, cartões inteligentes, certificado digital, ou dispositivos *token* que geram senhas temporárias. Quando utilizada em conjunto com senhas proporcionam um nível maior de segurança.

Sua desvantagem está relacionada a perda ou roubo do objeto ou dispositivo, e para alguns casos há possibilidade de clonagem. Ainda há um custo adicional a ser levado em conta para produção e substituição dos dispositivos extraviados.

2.2.1 Smartcards

Smartcards são cartões utilizados para transportar de forma segura credenciais e chaves de usuários. As credenciais ficam armazenadas permanentemente na memória ROM encontrada no chip do cartão.

A maioria dos brasileiros também não sabe como é feita a segurança dos cartões de crédito, sabem apenas que é seguro por causa do chip. O funcionamento dos cartões com chip está baseado na ISO 7816, e a lei que regulamenta as operações com cartões de crédito é a 12.865/13. (CardWerk Technologies)

O chip é dividido em seções e cada uma possui uma função específica, mas apenas uma é utilizada para transmitir dados. O chip também é composto de um processador e módulos de memória. Na memória ROM estão guardadas as informações do cartão. A memória RAM é utilizada durante a execução das transações entre o cartão e o terminal de pagamento. (Smartcard News).

2.2.2 Tokens

Tokens são dispositivos eletrônicos que basicamente geram códigos aleatórios, validos por um pequeno período de tempo, o que dificulta ainda mais a utilização do código por pessoas mal intencionadas. Dependendo do dispositivo os códigos podem ser gerados a cada fração de tempo previamente definido, ou a cada interação do usuário, que ao pressionar um botão um novo código valido é gerado.

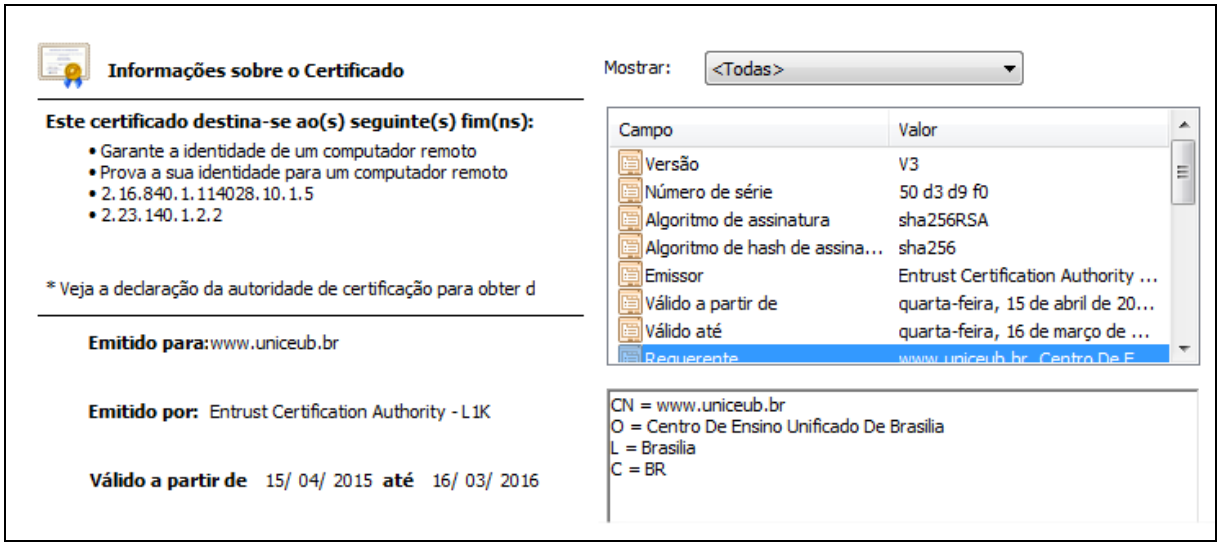
Na década de 90 os *tokens* utilizavam uma solução chamada OTP (*One-Time Password*), criada pela empresa Security Dynamics e parametrizado na RFC 2289. Por ser um algoritmo proprietário, a indústria necessitava de um algoritmo público, então foi criado o OATH (*Initiative for Open Authentication*), que utilizam o algoritmo HOTP (*HMAC-Based One-Time Password*) padronizado na RFC 4226. (Open AuTHentication).

Para cada dispositivo há um segredo único, que é utilizada para gerar os códigos de segurança aleatórios em um determinado período de tempo. O contador deve ser sincronizado entre o dispositivo gerador (cliente) e o dispositivo validador (servidor). Para isso um segredo é compartilhado entre o cliente e o servidor, e caso o servidor identifique tentativas de autenticação sem sucesso a partir de um cliente, o mesmo poderá recusar futuras conexões. (Open AuTHentication).

2.2.3 Certificado digital

O certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa ou empresa, através da ligação entre os atributos do proprietário, a uma chave pública de uma entidade que o certificou. Com ele é possível obter a certeza de estar se relacionando com a pessoa ou com a empresa que se diz ser. O certificado (Figura 15) contém dados como nome do proprietário, entidade emissora, prazo de validade e uma chave pública.

Figura 15 – Exemplo de um certificado digital



Fonte: (PERETTI, 2015)

Atualmente é utilizado para assegurar a comunicação de transações online, troca de documentos ou mensagens eletrônicas, etc. É um documento eletrônico que associa uma chave pública, fornecida por uma entidade confiável, a uma

identidade (legitima o proprietário) e que assegura que o Documento o não está com os dados comprometidos (íntegros). (Benefix Sistemas).

O certificado é assinado digitalmente para garantir a integridade das informações contidas nele. A Autoridade Certificadora (AC) é responsável pela assinatura dos certificados, que são atestamentos feitos por essa AC que diz confiar nestes dados, certificando assim, as chaves públicas dos protagonistas. (MÜLLER, 2007).

A legislação que instituiu a assinatura digital como instrumento de valor jurídico no Brasil foi a Medida Provisória Nº 2.200-2, de 24 de agosto de 2001, que pode ser encontrada em http://www.iti.gov.br/.

O mecanismo de assinatura digital pode ser resumido em dois processos criptográficos. O primeiro é a geração do *hash* (resumo da mensagem), que ocorre através de algoritmos como MD5 ou SHA-256, com a função de impossibilitar que a mensagem original seja exposta. Já o segundo processo consiste na criptografia do *hash* criado, que ocorre utilizando a chave privada de uma Autoridade Certificadora. Durante todo o processo o documento não sofre alteração, apenas o *hash* cifrado é anexado ao documento. (MÜLLER, 2007).

2.3 Autenticação através da característica

Para algo que você é, a segurança é baseada em uma característica de preferência única que o sujeito possua e que ainda possa ser mensurável, como exemplo a geometria das mãos, digitais, íris, disposição das veias da mão, ou até mesmo seu comportamento.

É notável que essas técnicas sozinhas não provem garantia suficiente da identidade de um usuário, o que se faz necessário desenvolver um sistema de autenticação que possa combinar mais de um tipo de autenticação para provar sua real identidade, como por exemplo, mesclar senhas com cartões, ou senhas com a autenticação biométrica.

Segundo Lourenço (2009), para ser utilizada na identificação do indivíduo a característica biométrica deve satisfazer os seguintes requisitos:

- **Universalidade**: Todos os indivíduos devem possuir a característica que será utilizada;
- **Singularidade**: A característica tem que variar de um indivíduo para o outro, permitindo com isso identificá-lo;
- **Permanência**: A característica não deve variar no tempo ou variar de forma irrisória ou em tempo mensurável de forma que, de tempos em tempos, seja possível coletar a característica novamente;
- **Desempenho**: Precisão e agilidade com que a característica é processada para a identificação do indivíduo a ponto de atingir uma medição aceitável;
- **Aceitabilidade**: O dispositivo de leitura biométrica deve ser aceito pelos indivíduos;
- **Proteção**: O dispositivo de leitura biométrica e o Sistema de Informação responsável pelo armazenamento das credenciais devem possuir uma imunidade aceitável contra violações do sigilo da credencial e da criação de cópias biométricas aceitáveis.

Segundo Alecrim (2005) existem várias características biológicas que podem ser usadas em um processo de identificação. Abaixo segue uma breve descrição de cada uma delas:

- **Impressão digital**: Ela funciona com o reconhecimento dos padrões de sulcos da pele dos dedos da mão. Cada pessoa tem um desenho diferente e único, que pode ser usado para identificar um indivíduo.
- **Retina**: o reconhecimento por retina é um dos meios mais seguros de biometria. O método analisa a forma dos vasos sanguíneos no fundo do olho com um feixe de luz de baixa intensidade. A desvantagem desse método é o incômodo, sendo invasivo à pessoa.
- **Íris**: Um método mais fácil e menos incômoda do que a análise de retina, a identificação por meio da íris se baseia na leitura do padrão colorido em torno da pupila.

- **Face**: O método de análise da face usa características como formato do rosto, do nariz, dos olhos, entre outros, para identificar um indivíduo. Mudanças no rosto ou pessoas muito semelhantes, como irmãos gêmeos, podem atrapalhar a identificação, por isso esse sistema não é muito confiável e nem muito usado.
- **Palma da mão**: Esse método é bastante utilizado, assim como a impressão digital, sendo baseado no formato da mão e nas veias da palma da mão e da corrente sanguínea ativa. É uma técnica bem simples e rápida. Alterações profundas da mão e das veias ocasionadas por um machucado podem prejudicar a leitura e exigir um recadastramento.
- **Voz**: A identificação por voz é uma forma pouco aplicada de identificação biométrica. Ela utiliza a dicção de uma frase, que funciona como senha, para reconhecer a pessoa. Esse método não funciona bem em ambientes com muito ruído, como é nas agências bancárias, por isso não é muito utilizada nesses casos.
- **Assinatura**: A assinatura é uma forma clássica de biometria para autenticar um indivíduo. Consiste na comparação da assinatura da pessoa com suas assinaturas anteriores guardadas num banco de dados, utilizando uma mesa digitalizadora para capturar as informações. Fatores como velocidade, força aplicada e outros detalhes sutis são analisados para verificar a autenticidade. Não é, necessariamente, uma tecnologia biométrica, mas é bastante utilizada nos bancos.

2.4 Considerações Finais do Capítulo

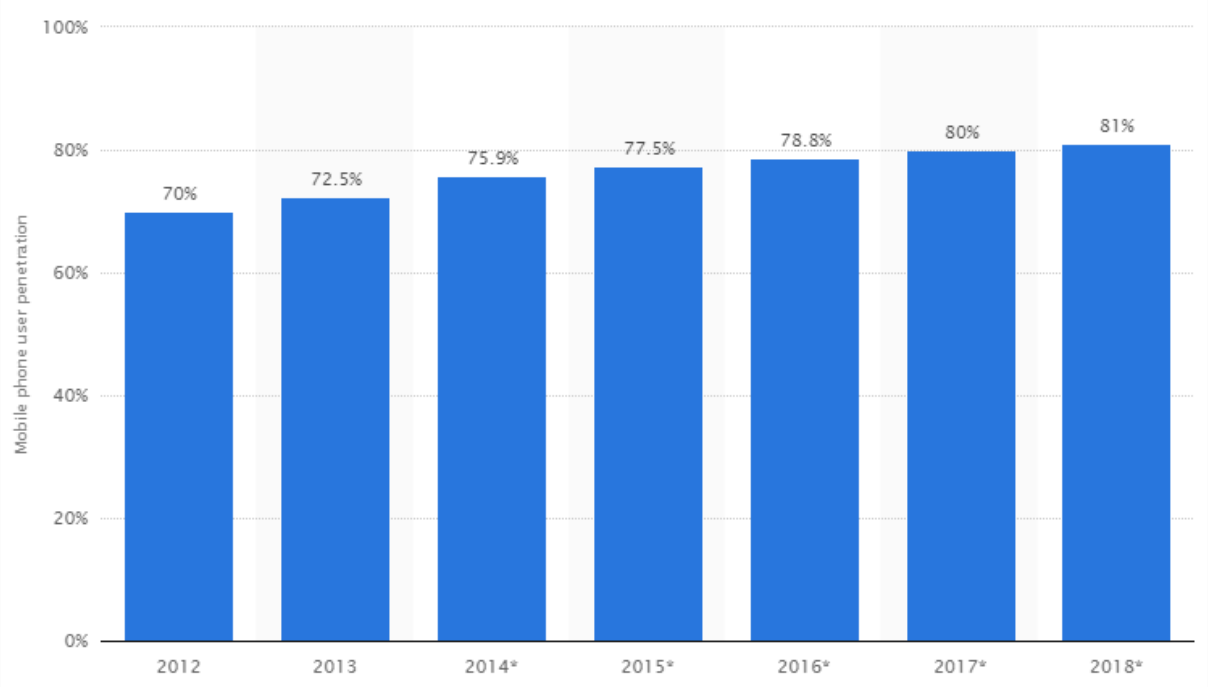
Neste capítulo foram descritas as principais formas de autenticação biométricas em Sistemas de Informação, baseadas no conhecimento, na propriedade e nas características físicas do indivíduo. Em todas as formas de autenticação apresentadas, o principal objetivo é comprovar a identidade de uma pessoa.

3 DISPOSITIVOS MÓVEIS

Dispositivos Móveis são aparelhos que possuem fácil mobilidade, capazes de se comunicar através de redes sem fio, como *bluetooth*, redes 3G/4G ou *Wi-Fi*, e geralmente utilizam bateria como fonte de alimentação. São exemplos de dispositivos móveis os *tablets*, *smartphones*, *netbooks* e PDA (Personal digital assistants). Até o ano de 2010 possuíam uma capacidade limitada de poder computacional (processamento e armazenamento) devido ao seu tamanho físico e a tecnologia da época, mas com o avanço tecnológico atualmente temos *smartphones* com alto poder computacional dotados de várias funcionalidades e sensores.

No Brasil a popularização do *smartphone* está aumentando gradativamente conforme demonstrado na Figura 16:

Figura 16 – Utilização do smartphone no Brasil entre 2012 e 2018



Fonte: (Statista)

Um *Smartphone* é caracterizado por possuir não somente a função de ligação, mas muitas outras funcionalidades além da qual foi criado. Possuem um sistema operacional, sendo os mais comuns o Android, iOS e Windows Phone, além de contarem com as principais tecnologias de comunicação e disponibilizar serviços

como: mensagens instantâneas, e-mail, internet, GPS, câmera, reprodutor de música e vídeo, jogos, etc. Devido a essa variedade de serviços, vários aplicativos são desenvolvidos diariamente para *smartphones* de acordo com seu sistema operacional.

3.1 Transmissão de dados

Conforme dito anteriormente, um *smartphone* possui as principais tecnologias de comunicação, como o *Bluetooth*, redes 3G/4G e *Wi-Fi*. A seguir segue uma breve descrição sobre cada uma delas.

A rede *Wi-Fi* consiste em um padrão de redes locais sem fios, conhecida pelo padrão IEEE 802.11, e que podem cobrir uma área de centenas de metros (TANENBAUM, 2003). Permite a comunicação entre dispositivos e é muito utilizada por empresas, residências, universidades, aeroportos, shoppings entre outros. No padrão 802.11n sua taxa de transferência pode variar de 65 à 600 Mbps.

O *Bluetooth* é outra tecnologia de comunicação muito utilizada em dispositivos móveis, baseada no padrão IEEE 802.15.1. Tornou-se popular por ser uma tecnologia de baixo custo, e consequentemente passou a estar presente na maioria dos dispositivos. A comunicação pode ser feita entre cliente e servidor, onde um único servidor pode se conectar a vários clientes. É muito utilizado para conectar fones de ouvido, mouse, teclado, dentre outros acessórios.

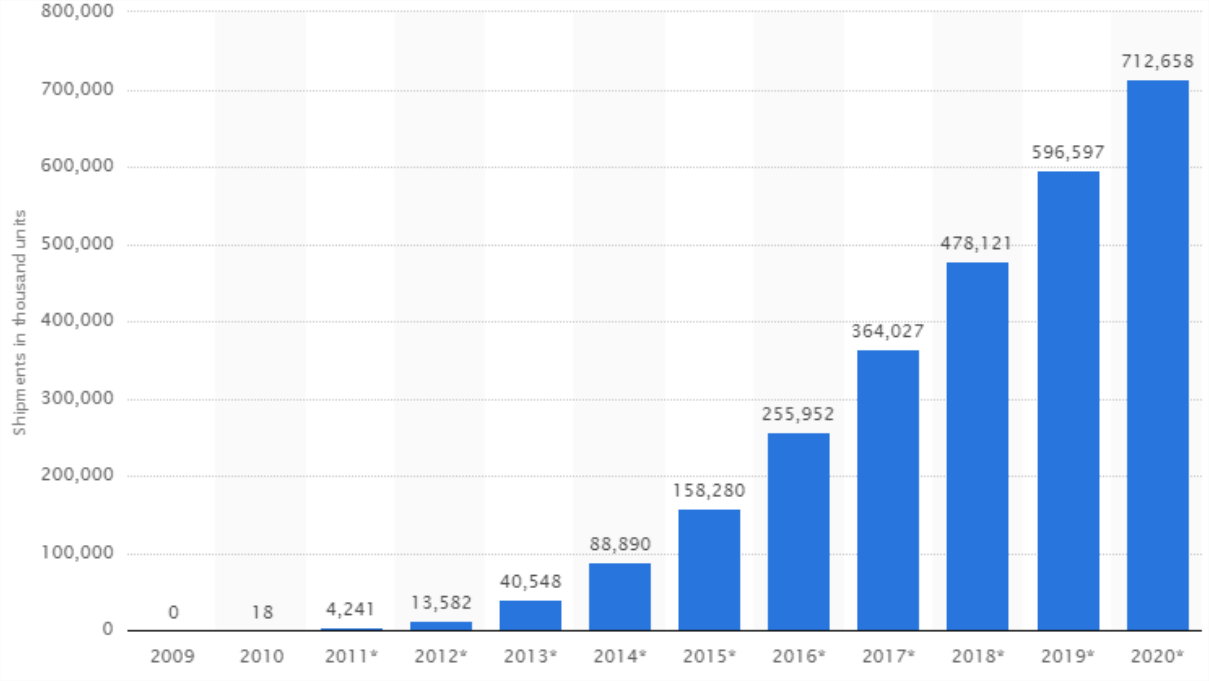
A principal desvantagem do *Bluetooth* é a taxa de transferência, que é baixa quando comparada com a *Wi-Fi*. A taxa de transferência de dados no *Bluetooth* em sua versão 1.2 pode alcançar 1 Mbps (megabit por segundo). Já em sua versão 2.0, a velocidade máxima passou 3 Mbps, porém ainda não era rápida o suficiente para o compartilhamento de multimídia. Buscando maiores velocidades foi então que surgiu a versão 3.0, capaz de atingir taxas de até 24 Mbps. Outra desvantagem é a área de cobertura, que é bastante limitada consistindo num raio de 10 metros.

Já a conexão 3G, baseada no padrão UMTS (*Universal Mobile Telecommunication System*), caracteriza-se pela transmissão de dados em alta velocidade e a longa distância, utilizada para telecomunicações. Uma de suas vantagens está na sua disponibilidade, pois os dados podem ser enviados ou

recebidos imediatamente conforme a necessidade do usuário, sendo que a taxa de transferência pode variar entre 384 kbps à 7,2 Mbps para sistemas móveis.

Recentemente surgiu a rede 4G, onde no Brasil é utilizado o padrão LTE (*Long Term Evolution*), sendo a quarta geração da comunicação wireless. Sua taxa de transferência é muito superior em relação ao 3G, podendo alcançar taxas de até 100 Mbps. Gradativamente a tecnologia está sendo inserida nos novos dispositivos móveis e em breve a tecnologia 3G será definitivamente substituída. Podemos visualizar essa tendência na Figura 17, onde há uma previsão para o aumento da exportação de *smartphones* que já trabalham na rede 4G até o ano de 2020.

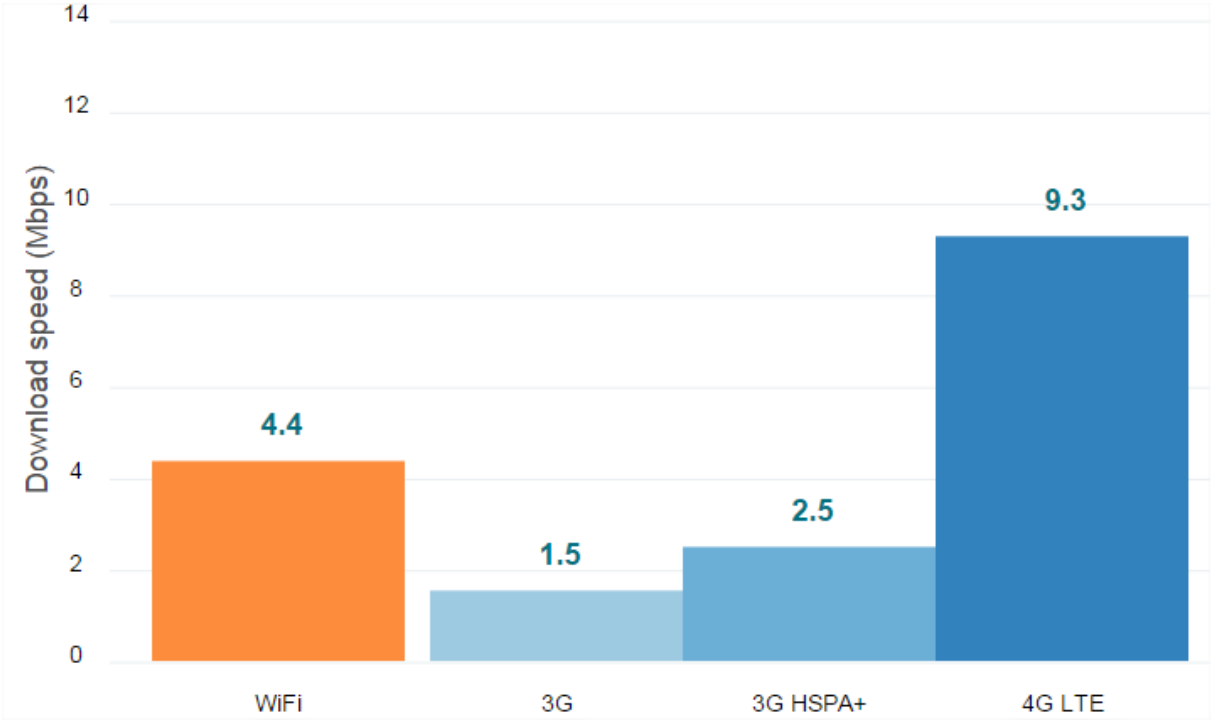
Figura 17 – Estimativa de exportação de smartphones com 4G



Fonte: (Statista)

Conforme estudo realizado pela OpenSignal, onde foram coletados dados de 11 milhões de usuários que têm planos de rede 4G, podemos verificar que a velocidade média de download da rede 4G é muito superior em relação às outras tecnologias (Figura 18). Os dados utilizados foram coletados entre novembro de 2014 a janeiro 2015.

Figura 18 – Velocidade média de download das redes Wireless



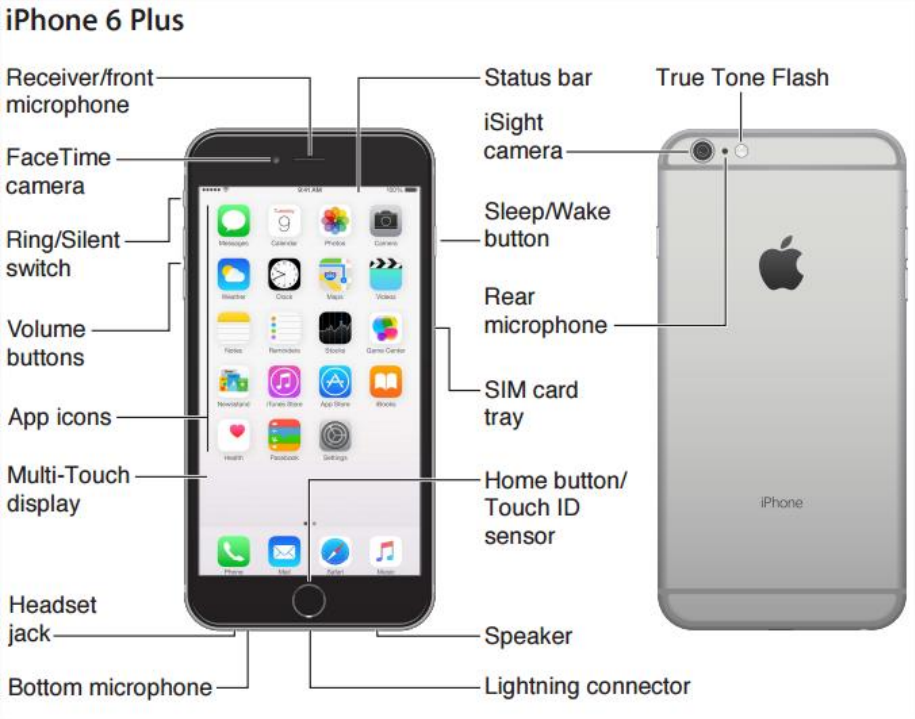
Fonte: (OpenSignal)

3.2 Componentes

Assim como os computadores, os *smartphones* também possuem processador, memória, armazenamento, placa gráfica, etc. Porém possuem o desafio de proporcionar um bom desempenho com um consumo muito baixo de energia, já que utilizam bateria como fonte de alimentação.

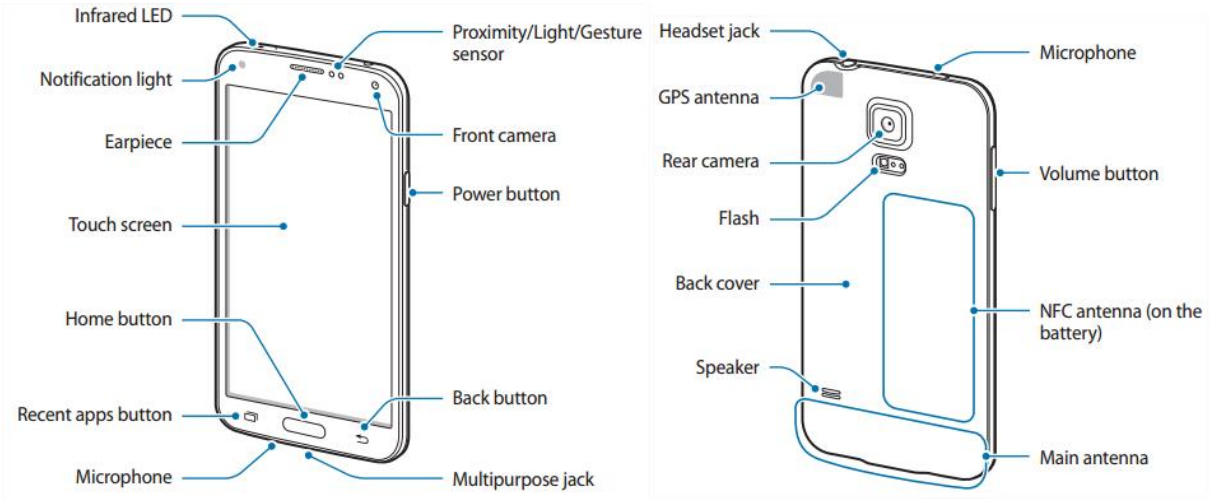
Os *smartphones* são conhecidos por possuírem várias utilidades, com o objetivo de proporcionar uma melhor experiência para o usuário. Quanto mais funcionalidades maior é o seu custo de fabricação, e consequentemente o seu valor de mercado. Com o passar dos anos, novos componentes foram implantados como o *Bluetooth*, GPS, rádio, TV, tela sensível ao toque, infravermelho, câmera traseira e frontal, *flash*, sensores de proximidade, movimento e claridade. Conforme Figuras 19 e 20, podemos verificar que os *smartphones* possuem características semelhantes, mesmo quando produzidos por diferentes marcas.

Figura 19 – Componentes do smartphone iPhone 6 Plus



Fonte: (Apple)

Figura 20 – Componentes do smartphone Galaxy S5



Fonte: (Samsung)

Recentemente os *smartphones* estão recebendo leitores de impressão digital. Como podemos ver nas Figuras 19 e 20, os *smartphones* da Apple e da Samsung possuem o sensor de impressão digital localizado no *Home button*, onde o usuário pode se autenticar ou desbloquear o *smartphone* através de suas digitais.

Conforme novos dispositivos foram surgindo as fábricas de software foram criando novos aplicativos, aproveitando ao máximo os recursos disponíveis. Porém uma das características esperadas em um smartphone é a sua velocidade, o que exige que seu poder de processamento e a velocidade de armazenamento sejam aprimorados.

3.3 Controle de acesso

Um dos temas mais abordados em relação aos *smartphones* é o controle de acesso. Assim como buscamos adotar medidas para protegermos informações armazenadas em computadores, há uma preocupação constante em manter as informações armazenadas nos *smartphones* protegidas de pessoas não autorizadas.

A proteção é feita através de uma autenticação utilizada para desbloquear o *smartphone*. Basicamente a maioria dos *smartphones* possuem várias formas de desbloqueio, como por exemplo: senha, PIN, traçado de um padrão, em que o usuário deve escolher qual será utilizada para desbloqueio do *smartphone*. O destaque vai para a possibilidade de autenticar o usuário baseado em sua biometria, através dos sensores de impressão digital, microfone e câmera, disponíveis em *smartphones*.

Recentemente foram implantados novos recursos relacionados ao controle de acesso, como é o caso do NFC (*Near Field Communication*), solução desenvolvida em uma parceria entre as empresas Sony e Phillips, que permite uma comunicação rápida e segura entre dois dispositivos a poucos centímetros de distância um do outro. Desta forma é possível utilizar uma tarja NFC para desbloquear o *smartphone*, apesar do número de *smartphones* com a tecnologia NFC ainda ser pequeno.

O NFC é uma tecnologia de comunicação de curto alcance, de alta frequência, baixa largura de banda e sem fio, baseada na tecnologia RFID (*Radio Frequency Identification*). Sua referência está padronizada nas normas ISO/IEC 18092 e ECMA- 340. (FRANCISCO; COSTA, 2012).

A comunicação é estabelecida mediante radiofrequência a partir da faixa de 13,56 MHz, a uma distância máxima de 10 cm entre os dois dispositivos, com a velocidade de transmissão de dados variando entre 106, 212 e 424 Kb/s.

Recentemente passou a ser possível também trabalhar com a taxa máxima de 848 Kb/s, embora não oficialmente. (ALECRIM, 2012).

3.4 Pagamentos

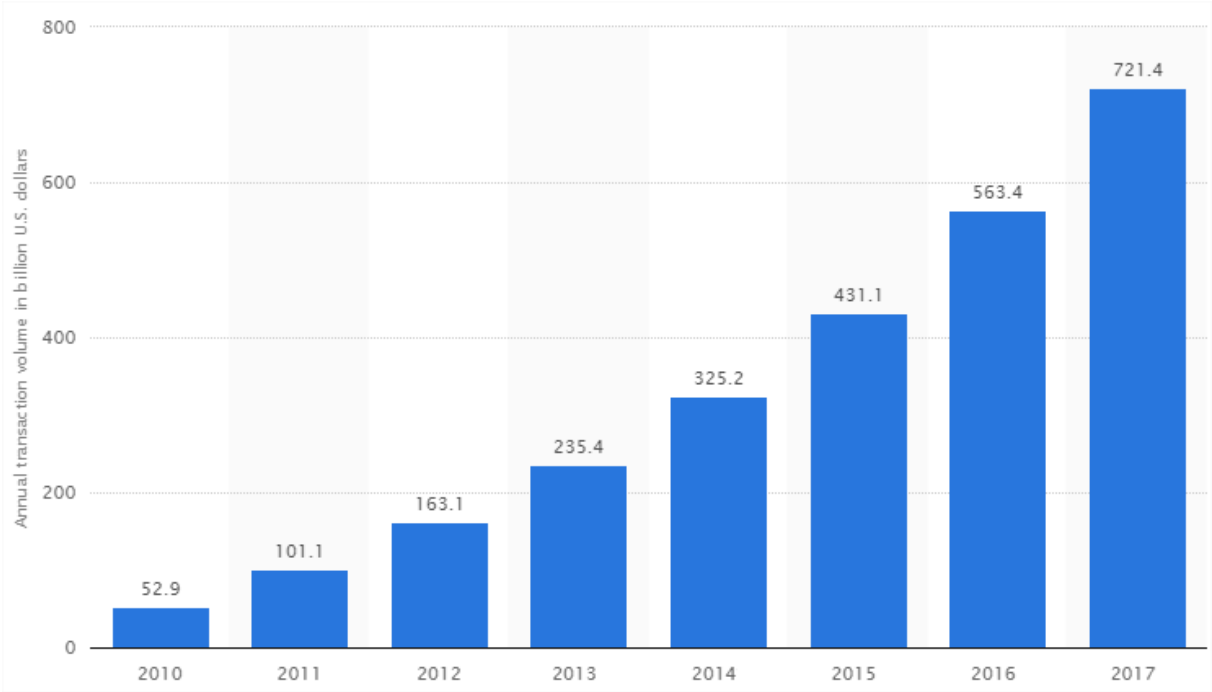
O pagamento em dispositivos móveis é uma das grandes conquistas obtidas através do avanço da tecnologia. Consiste na possibilidade de realizar operações financeiras através de um dispositivo móvel. O correntista deve acessar o aplicativo de sua instituição financeira onde é possível realizar consultas de saldo, extratos, transferências eletrônicas, pagamento de boletos, recarga telefônica, etc.

Para realizar pagamentos e transferências eletrônicas, as instituições financeiras exigem por segurança que o correntista primeiramente faça um cadastro do dispositivo móvel e efetue sua liberação. Essa medida tem por objetivo evitar que indivíduos mal intencionados, de posse de informações como agência, conta e senha, consigam realizar pagamentos e transferências através de dispositivos não cadastrados ou liberados previamente pelo correntista.

Em caso de perda, furto ou roubo do dispositivo móvel, a instituição financeira a qual o correntista pertence tem o dever de assegurar a privacidade e a proteção de dados pessoais dos usuários, resguardando os seus interesses econômicos.

Nos últimos anos o pagamento através de dispositivos móveis aumentou exponencialmente. Conforme a Figura 21, podemos verificar o volume global de transações de pagamento móveis entre 2010 e 2013 em bilhões de dólares, e a previsão para seu avanço até o ano de 2017.

Figura 21 – Volume global de transações através de dispositivos móveis



Fonte: (Statista)

No Brasil, as transações bancárias através de dispositivos móveis já eram realizadas antes mesmo de uma legislação específica para a modalidade. Somente após a edição da lei nº 12.865, de 9 de outubro de 2013, e da regulamentação infralegal, é que o serviço passou a ser regulamentado e fiscalizado pelo Banco Central.

Recentemente os *smartphones* têm sido utilizados como carteiras virtuais. Em outros países já é possível utilizar serviços como o Google Pay e o Apple Pay. Uma solução semelhante disponível no Brasil é o Ourocard-e, desenvolvida pelo Banco do Brasil. Atualmente disponível apenas para *smartphones* Android, o aplicativo permite o pagamento de compras nas funções débito e crédito por meio de cartões virtuais, disponibilizados via smartphones para uso em lojas físicas que possuem uma máquina com NFC.

Sua utilização é considerada simples e ocorre basicamente em três passos:

1. O cliente informa a opção de pagamento e o lojista seleciona a opção desejada e insere o valor na máquina.

2. O cliente desbloqueia seu telefone, abre o aplicativo Ourocard-e e seleciona o cartão a ser utilizado na opção de pagamento informada anteriormente ao lojista.
3. O cliente aproxima o smartphone da máquina com NFC (Figura 3), digita a senha (desnecessária para compras abaixo de R$50,00) e é só aguardar a emissão do comprovante.

Ao realizar um pagamento, o sistema emitirá para a máquina uma chave de segurança, conforme ilustrado na Figura 22, eliminando qualquer possibilidade de captura do número do cartão do cliente.

Figura 22 – Ilustração de pagamento com o Ourocard-e

Fonte: (Banco do Brasil)

Algumas precauções de configuração e segurança são necessárias para poder usufruir da nova solução (Banco do Brasil):

- Primeiramente o *smartphone* deve possuir a função NFC e não pode ter acesso “root”, procedimento que concede ao usuário acesso a todos os arquivos de aplicações e do sistema em si, bem como permissão para alterar configurações anteriormente bloqueadas por padrão.

- O sistema operacional suportado até o momento é o Android a partir da versão KITKAT 4.4.2.
- O smartphone deve possuir acesso à Internet, seja por *Wi-Fi* ou 3G/4G.
- O usuário deve configurar uma das formas de desbloqueio do *smartphone* Android, como por exemplo: senha, PIN numérico, padrão de toques, padrão de traçado, reconhecimento facial, digital, voz, etc.

O aplicativo ainda possibilita ao cliente criar, alterar e desativar vários cartões virtuais, definir o limite disponível, até mesmo definir a validade do cartão. O cliente também poderá estabelecer um valor limite por transação e definir se ele poderá efetuar transações no exterior. (Banco do Brasil).

3.5 Considerações Finais do Capítulo

Neste capítulo, foram abordados componentes relacionados aos dispositivos móveis. Com sua crescente popularidade, os *smartphones* estão recebendo novas tecnologias gradativamente, conforme apresentado na Seção 3.2. Foram descritas as suas principais tecnologias de transmissão, com foco para a tecnologia 4G, onde foi apresentada uma previsão para o aumento do número de smartphones que já trabalham na rede 4G, e sua velocidade média de transmissão.

Ainda neste capítulo foram apresentadas as principias formas de desbloqueio dos *smartphones*. Na seção 3.4 foi abordado o pagamento através de dispositivos móveis, bem como sua expectativa de crescimento. Foi apresentada uma breve descrição das aplicações de pagamento utilizadas atualmente.

4 MOBILE BANKING

Mobile Banking é o termo em inglês utilizado para o acesso a serviços bancários através de um dispositivo móvel. Começou a ser disponibilizado pelas instituições financeiras a partir de 2008, quando os primeiros *smartphones* surgiram. Assim como o *Internet Banking* acessado por computadores, o *Mobile Banking* utiliza a internet como meio de comunicação.

O medo da fraude ainda é o principal fator limitador do uso da Internet como canal transacional. No entanto, tem sido possível mudar a percepção dos usuários sobre a segurança, por meio da implementação de medidas adicionais e de materiais educativos que informam os usuários sobre como usar essas medidas de maneira eficaz.

A popularidade do banco móvel cresceu em todo o mundo, ganhando espaço entre os canais de atendimento tradicionais, como agências e caixas eletrônicos. No entanto, muitos usuários que se sentem confortáveis em realizar transações a partir de um computador estão apreensivos em adotar o canal móvel. Mais uma vez, a principal razão pela qual não temos mais pessoas realizando operações bancárias em seus dispositivos móveis é o medo de *phishing*.

A precaução dos clientes não é sem motivo. Um estudo realizado pela empresa Arxan Technologies revelou que 95% dos principais aplicativos financeiros para Android (e 70% dos aplicativos para iOS) foram hackeados. Em 2014, a Trend Micro concluiu que 77% dos 50 aplicativos gratuitos mais baixados do Google Play teriam versões falsas, sendo muito difícil para os usuários diferenciar entre aplicativos autênticos e falsificados. Sem uma segurança adequada no canal móvel, muitos usuários irão facilmente deixar a conveniência de lado para se sentirem mais protegidos, realizando suas transações bancárias a partir de seus computadores.

Nesse sentido algumas instituições financeiras costumam negar o uso de suas aplicações em *smartphones* que tenham sido modificados. A referida modificação é chamada de “*root”*, onde o usuário passa a ter acesso a todos os arquivos e configurações sensíveis do sistema operacional do *smartphone*, e consequentemente de outras aplicações.

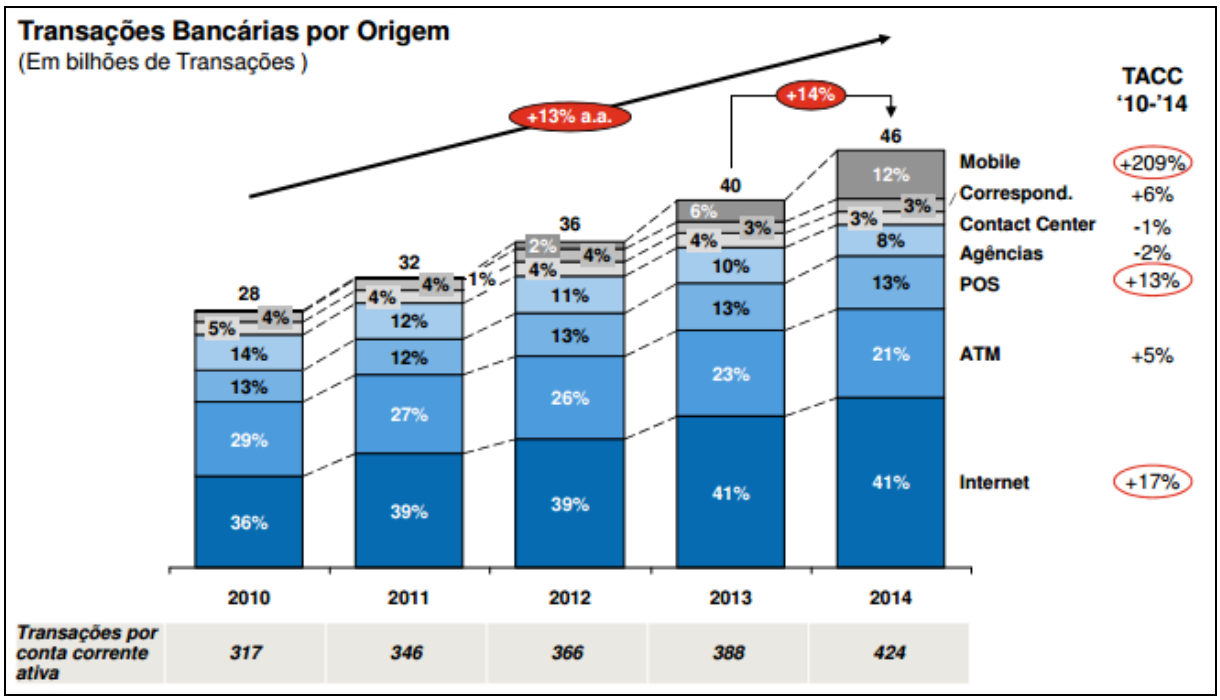
Atualmente, o acesso ao *mobile banking* é feito basicamente em duas camadas de segurança: a primeira é a senha eletrônica e a segunda é utilizando o *Token*. Abaixo são descritos alguns ataques conhecidos direcionados a autenticação:

- **SSL *Proxy*** – Utilizado para espionagem de informações confidenciais. Consiste em interceptar toda a comunicação entre o cliente e o servidor, além da utilização de um certificado digital falso, criando uma “conexão segura” entre o cliente e atacante. Dessa forma, o atacante pode capturar informações como o número da agência, conta corrente, senha eletrônica, senha do cartão de débito e o token. (IDGNOW).
- **SSL *Strip* e *Man-in-the-middle*** – Ataque executado para roubo de informações como senhas, *tokens*, número de agencia, conta corrente, palavras-chave, dentre outras; Mesmo quando as informações estão criptografadas, são utilizadas ferramentas para sequestrar o tráfego de informações entre o aplicativo do *mobile banking* instalado no *smartphone/tablet* e a instituição financeira, onde são monitorados solicitações ao protocolo HTTPS; O SSL é isolado, deixando o cliente do banco em uma conexão não segura, onde o número da agência, conta corrente e senha eletrônica são capturadas pelo atacante através de uma transmissão não segura das credenciais enviadas à Instituição Financeira. (IDGNOW).
- **Certificados digitais falsos -** Ataque baseado em *Man-in-the-middle* onde o atacante emite um certificado digital falso, com o objetivo de interceptar o tráfego em uma conexão HTTPS supostamente segura. (IDGNOW).
- **Engenharia reversa e análise de código –** Ataque baseado na análise do código-fonte de um aplicativo, com o objetivo de explorar vulnerabilidades encontradas, como por exemplo: Implementação de ASLR, *Heartbleed*, *Stack Overflflow*, *Address Reference Counting*, *Memory dump values*, entre outras. (IDGNOW).

Um estudo realizado pela empresa Easy Solutions (Visão dos consumidores latino-americanos sobre fraude eletrônica em 2015), demonstra que os usuários se percebem como um dos principais responsáveis pela segurança das transações eletrônicas, seguidos de perto pelos bancos. Esse dado sugere que os usuários da região não esperam que o banco seja o único a cuidar da segurança das atividades dos clientes. Eles estão conscientes de que devem adotar medidas parte para garantir que as operações sejam realizadas corretamente.

Conforme relatório da Pesquisa FEBRABAN de Tecnologia Bancária 2014, as transações via *Mobile Banking* continuam apresentando um crescimento expressivo, sendo o quarto canal com o maior volume de transações. A Figura 23 mostra que entre os anos de 2010 e 2014 o canal *mobile banking* obteve um crescimento de 209%, correspondendo a 12% das 46 bilhões de transações realizadas em 2014.

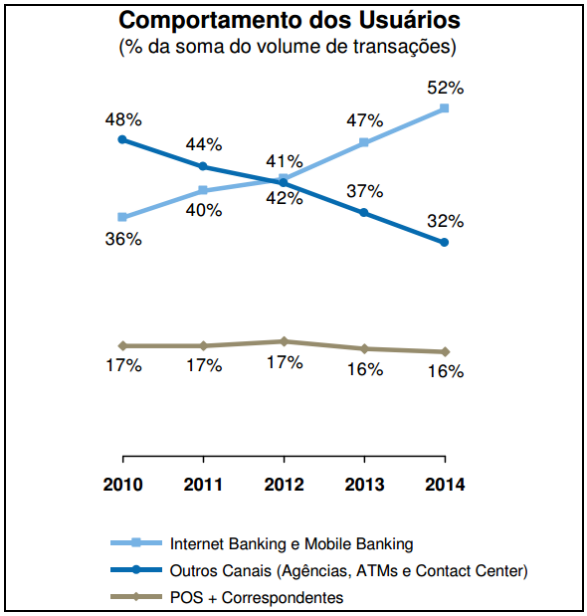
Figura 23 – Distribuição das transações por canal de atendimento



Fonte: (FEBRABAN)

Outra informação importante é que o *Internet* e *Mobile Banking* juntos foram responsáveis por mais de 50% do total de transações do ano de 2014. Esse crescimento pode ser observado na Figura 24.

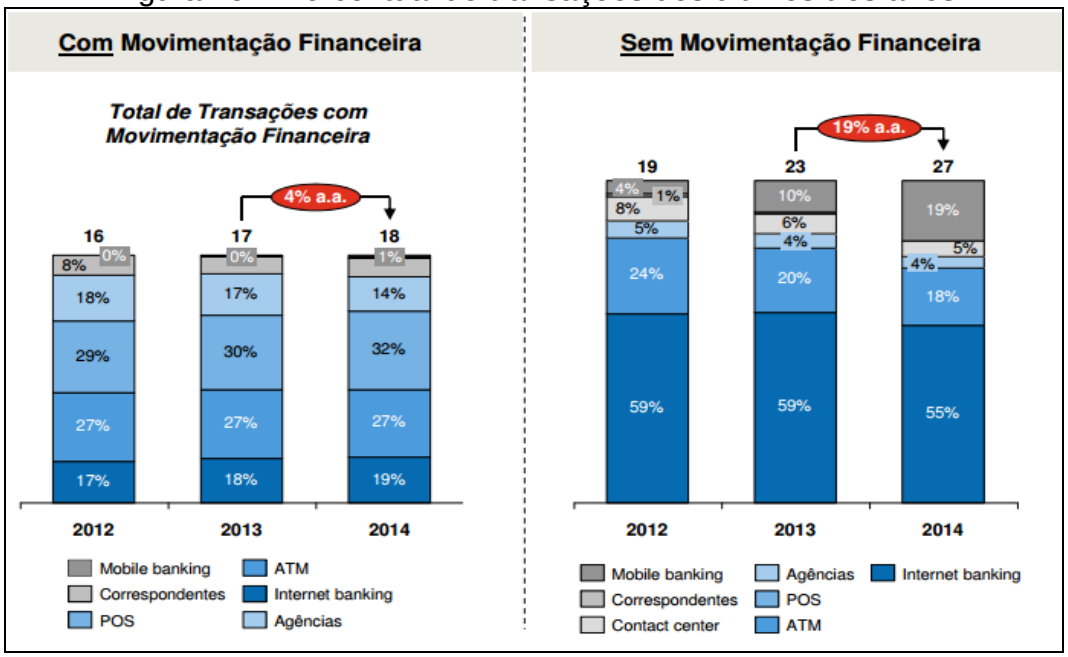
Figura 24 – Preferência dos usuários por canal de atendimento



Fonte: (FEBRABAN)

O número de usuários de *Mobile Banking* cresceu rapidamente, mas ainda está muito distante dos computadores, mesmo com os recordes de vendas de *smartphones* a cada ano. Esse dado sugere que ainda há muito a ser feito para motivar os usuários a utilizar *smartphones* e *tablets* como canal padrão para operações bancárias.

Figura 25 – Percentual de transações dos últimos três anos

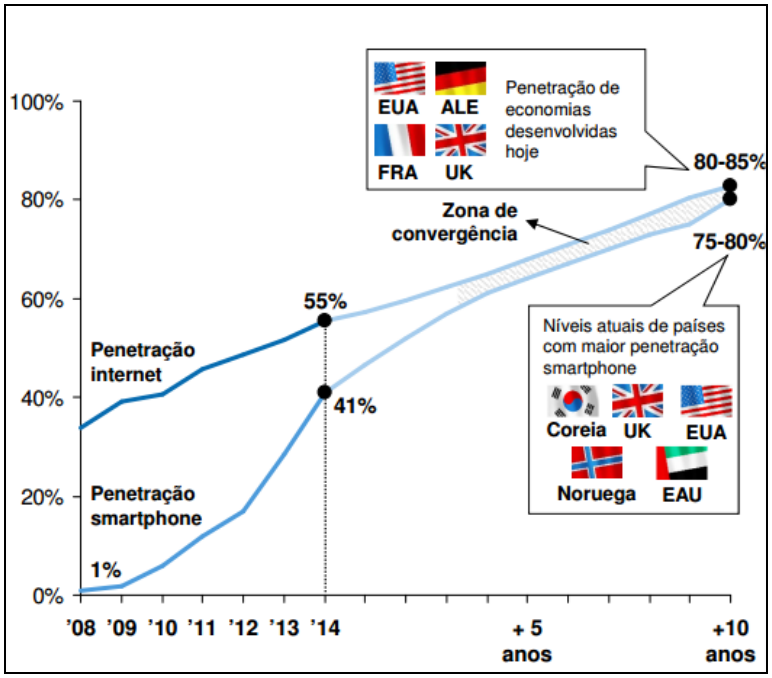


Fonte: (FEBRABAN)

Apesar do aumento do total de transações nos canais *Internet* e *Mobile Banking*, a maioria das transações não são de movimentação financeira. Conforme a Figura 25, o Mobile Banking foi responsável por apenas 1% do total de transações com movimentação financeira em 2014.

Os dados da Figura 26 evidenciam que mais da metade da população (55%) tem acesso à internet, e a penetração de *smartphones* continua apresentando crescimento contínuo, atingindo 41% em 7 anos. Porém estima-se que poderá levar 10 anos para o Brasil atingir níveis de penetração de internet e smartphones que de países desenvolvidos possuem atualmente.

Figura 26 – Penetração de acesso à Internet e Smartphones



Fonte: (FEBRABAN)

O colapso dos canais tradicionais é mais evidente quando se pergunta aos usuários da Internet qual é o seu canal de atendimento favorito para a realização de operações bancárias e pagamentos. O *Internet Banking* é atualmente o canal mais popular, mas a tendência é que nos próximos anos se torne um canal complementar ao *Mobile Banking*.

5 ESTUDO DE VIABILIDADE

Neste capítulo são abordados os parâmetros utilizados no estudo de viabilidade, como análise de desempenho, normas, custo, vantagens e desvantagens do uso da biometria multimodal como meio de autenticação em sistemas *mobile banking*. Também será indicado um modelo teórico acerca de técnicas de fusão biométrica, que tem como objetivo aumentar o nível de segurança e reduzir o número de falsos positivos em *mobile banking*. Ao final do capítulo encontra-se o resultado de uma pesquisa, com o objetivo de observar o conhecimento e a aceitação dos usuários sobre a utilização da biometria como forma de autenticação em *mobile banking*.

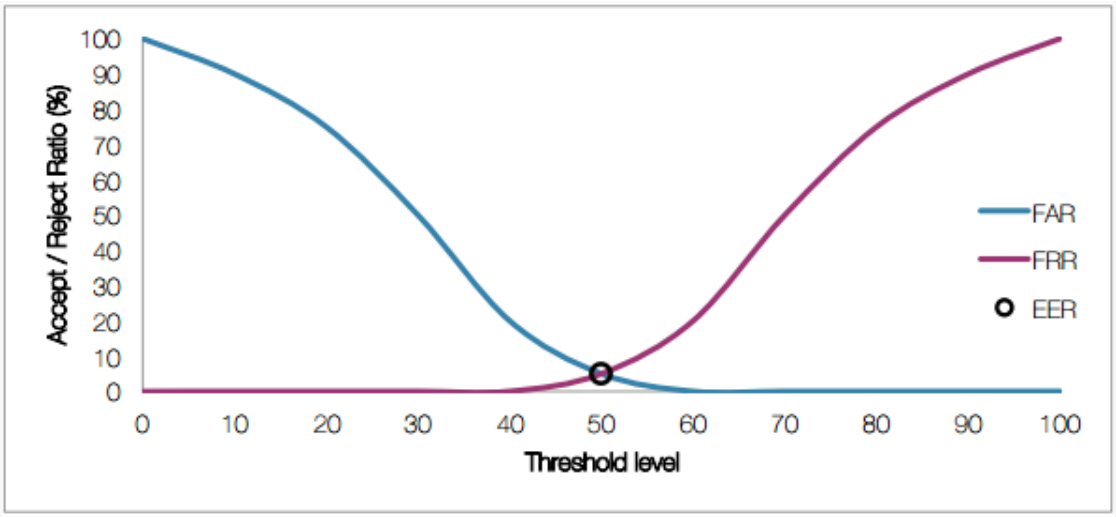
5.1 Análise de Desempenho

Um dos desafios na combinação de características de diferentes modalidades é que as medições das diferentes fontes verificam-se ser, em geral, não homogêneas. Além disso, os sistemas na parte de identificação e cadastro estão sujeitos a variações em função da posição de leitura.

O mais comum dos métodos que pode ser aplicado em uma comparação sobre a verificação e análise de desempenho é o que realiza a comparação dos sistemas multimodais às modalidades individualmente, tanto no que tange à verificação e autenticação, como nos indicadores de taxas de falsos positivos e falsos negativos.

Para aplicações de instituições financeiras que são acessadas por milhares de correntistas, quanto menor for a taxa de erros FAR (*False Acceptance Rate*) ou FRR (*False Rejection Rate*) mais seguro é o sistema. Porém primeiramente é necessário atingir um equilíbrio entre as duas taxas (Figura 27), conhecido pela sigla EER (*Equal Error Rate*).

Figura 27 – Equilíbrio (EER) entre as taxas FRR e FAR



Fonte: (handyman.hu)

A taxa de falsa aceitação FAR (*False Acceptance Rate*) representa o percentual de amostras aceitas que não estão cadastradas no sistema, e não deveriam ter sido aceitas, ou seja, a probabilidade de um impostor ser indevidamente aceito. A FAR pode ser calculada por:

Quadro 2 – Cálculo da Taxa de Falsa Aceitação (FAR)

FAR= NFA / NIIA

Fonte: (PINHEIRO, 2008)

onde, NFA é a quantidade de falsas aceitações e NIIA representa o número de tentativas de identificação de impostor.

Já a taxa de falsa rejeição FRR (*False Rejection Rate*) representa as amostras rejeitadas que estavam cadastradas no sistema, e deveriam ter sido aceitas, ou seja, a probabilidade de um usuário cadastrado ser classificado como um impostor. A FRR pode ser calculada por:

Quadro 3 – Cálculo da Taxa de Falsa Aceitação (FRR)

FRR= NFR / NEIA

Fonte: (PINHEIRO, 2008)

onde, NFR é a quantidade de falsas aceitações e NEIA representa o número de tentativas de identificação de um usuário cadastrado.

Na Tabela 1 são apresentados resultados de FAR (*False Acceptance Rate*) e FRR (*False Rejection Rate*) obtidos na avaliação individual das modalidades impressão digital, face e voz.

Tabela 1 – FAR e FRR

Biometria	**FAR**	**FRR**
Impressão Digital	2%	2%
Face	10%	1%
Voz	10-20%	2-5%

Fonte: (adaptado de: RAHAL; ABOALSAMAH; MUTEB, 2006)

Quanto à evolução dos estudos e pesquisas observamos diferenças nos resultados, dependendo da implementação cada sistema. Observe a Tabela 2 abaixo, que mostra os mesmos parâmetros para as 3 modalidades da Tabela 1, acrescentado a Iris (NANDAKUMAR, 2008). Nota-se que no caso da face e da voz há uma melhoria considerável no desempenho. Os números indicados na coluna de teste indicam a quantidade de testes realizados em cada caso.

Tabela 2 – Resultado de testes biométricos

Biometria	**Teste**	**Condições de Teste**	**Taxa de Falsa Aceitação (FAR)**	**Taxa de Falsa Rejeição (FRR)**
Impressão Digital	FVC 2006 [148]	População heterogênea incluindo trabalhadores manuais e idosos	2.2%	2.2%
	FpVTE 2003 [204]	Dados do governo (E.U.A)	1%	0.1%
Face	FRVT 2006[153]	Controle de iluminação e alta resolução	0.1%	0.8 - 1.6%
Voz	NIST 2004 [156]	Teste independente, várias frases	2 - 50%	5 – 10%
Iris	ICE 2006 [153]	Iluminação controlada, ampla gama de qualidade	0.1%	1.1 – 1.4%

Fonte: (adaptado de: NANDAKUMAR, 2008)

Quando comparamos o desempenho de sistemas unimodais com multimodais, observamos uma melhoria significativa em todos os índices analisados com a biometria multimodal. Na Tabela 3 abaixo, podemos verificar que em uma

comparação do resultado dos testes nos bancos de dados NIST-*Multimodal*, NIST-*Fingerprint*, NIST-*Face* e XM2VTS-*Benchmark*, a biometria multimodal, baseada na regra de fusão *Likelihood Ratio* (razão de verossimilhança), obteve ganhos significativos:

Tabela 3 – Desempenho da Biometria Multimodal

Banco de Dados	Melhor combinador único	Média da Taxa de Aceitação Genuína		Intervalo de confiança de 95% no aumento da GAR
		Melhor combinador único	Fusão baseada em razão de verossimilhança	
NIST-Multimodal	Dedo indicador direito	85.3%	13.5%	[13.5%, 14%]
NIST-Fingerprint	Dedo indicador direito	83.5%	91.4%	[7.6%, 8.2%]
NIST-Face	Combinador 1	71.2%	77.2%	[4.7%, 7.3%]
XM2VTS-Benchmark	DCTb-GMM Combinador de Face	89.5%	98.7%	N/A

Fonte: (adaptado de: NANDAKUMAR, 2008)

Também têm sido utilizadas técnicas baseadas em requisitos que o sistema biométrico deve ter para identificar e reconhecer um indivíduo de forma satisfatória. Os requisitos levam em consideração as características do identificador biométrico, geralmente classificados quanto aos níveis de universalidade, diferenciação, permanência, coletabilidade, desempenho, aceitação e evasão.

A Tabela 4 mostra identificadores avaliados conforme estes critérios, no qual podemos observar que a impressão digital e a face têm um bom desempenho quando usados estes critérios.

Tabela 4 – Características dos identificadores biométricos

Biometria	Universalidade	Diferenciação	Permanência	Coletabilidade	Desempenho	Aceitação	Evasivo
Face	A	B	M	A	B	A	A
Geometria da Mão	M	M	M	A	M	M	M
Impressão Digital	M	A	A	M	A	M	M
Iris	A	A	A	M	A	B	B
Retina	B	B	B	M	B	M	M
Teclado	B	B	B	M	B	M	M
Assinatura	B	B	B	A	B	A	A
Voz	M	B	B	M	B	A	A

B: Baixo M: Médio A: Alto

Fonte: (RAHAL; ABOALSAMAH; MUTEB, 2006)

5.2 Vantagens e Desvantagens

Com o uso da biometria multimodal para autenticação no *Mobile Banking,* o correntista não precisa mais gerenciar senhas difíceis ou estar sempre com seu *token*. Câmeras e microfones já estão presentes em qualquer *smartphone* ou *tablet*, porém os leitores de impressão digital ainda estão presentes apenas em *smartphones* mais modernos.

Os sistemas multimodais podem aliviar muitas das limitações dos sistemas unimodais. Diferentes fontes biométricas normalmente compensam as limitações inerentes às fontes individuais, o que lhes permite oferecer vantagens tais como:

- Combinando as evidências obtidas de diferentes fontes através de esquemas de fusão pode-se melhorar a precisão. A presença de várias fontes melhora o dimensionamento do sistema e reduz o espaço entre as diversas características individuas;
- Reduzem o problema da não-universalidade quanto à aquisição e captura das dos dados. Por exemplo, se uma pessoa não pode ser cadastrada devido a algum problema em sua digital, ela pode se cadastrar com outras modalidades;
- Podem oferecer certo grau de flexibilidade. Por exemplo, se forem cadastradas várias características de um determinado usuário, podem ser selecionadas quais devem ser utilizadas, dependendo da aplicação;
- A disponibilidade de amostras de várias fontes de informação reduz a influência de ruídos na coleta de dados, pois mais amostras a serem comparadas, melhoram a seleção;
- O sistema multibiométrico melhora a capacidade e direcionamento da pesquisa, uma vez que se pode iniciar por determinada característica e ir refinando o processo na medida em que novas características forem incluídas;
- O sistema multibiométrico é mais resistente a ataques, uma vez que o invasor (impostor) precisaria burlar as várias modalidades;

Diferente das senhas e *tokens*, a biometria é pessoal e intransferível, o que impossibilita seu compartilhamento, além de serem muito difíceis de copiar. Ainda assim a infraestrutura de comunicação entre cliente e servidor deve ser continuamente protegida.

Mas como na maioria dos sistemas, não existem apenas vantagens também existem algumas desvantagens das quais destaco a seguir:

- Uma das premissas para utilizar uma biometria como forma de autenticação é a imutabilidade. Porém em caso de doenças na pele, nos olhos, ferimentos, inflamações de garganta, as características biométricas podem sofrer alterações dificultando o processo de autenticação;
- Com o envelhecimento algumas características biométricas são alteradas, o que exige um recadastramento para atualizar as informações biométricas;
- Em caso de cópia ou roubo de alguma característica biométrica, não é possível trocá-la como fazemos com as senhas, ou seja, não há a possibilidade de possível substituir uma íris, voz, face ou outra característica física;
- Como o indivíduo se torna a sua própria senha, casos de sequestro são temidos pela sociedade. O atacante não precisa tentar descobrir ou copiar a sua senha já que a tem em "suas mãos";
- Interferências do ambiente como iluminação são um obstáculo para a biometria facial. Da mesma forma em ambientes barulhentos, o estado emocional do usuário (rouquidão, cansaço, estresse) são fatores de interferência na biometria pela voz. É necessário utilizar outra biometria, como por exemplo, a impressão digital;
- No momento da autenticação, a posição em que o dedo, a mão, o rosto, o olho, dentre outros, interfere no processo de validação do usuário;
- O uso de óculos, barba, bigode, cabelo grades, expressões da face, etc., podem afetar diretamente no reconhecimento do usuário.

- Existem técnicas para tentar burlar a biometria do usuário, como por exemplo, a criação de moldes de silicone das impressões digitais, o uso de uma foto (sistemas 2D) no momento do cadastro, gravações da voz de um usuário já cadastrado, dentre outras.

No Quadro 2 podemos visualizar um comparativo com as vantagens e desvantagens distribuídas por método biométrico:

Quadro 4 – Vantagens e desvantagens por biometria

MÉTODO	VANTAGEM	DESVANTAGEM
Impressão digital	Estável, bom grau de confiabilidade, fácil de implantar, barato.	A digital pode ser copiada em moldes e reutilizada.
Face	Não há necessidade de adquirir equipamento específico.	Fotos podem fraudar alguns sistemas.
Voz	Barato. Higiênico.	Ruídos podem prejudicar a captura da voz.
Íris	Praticamente impossível de fraudar. Não está sujeita ao envelhecimento. Método muito seguro.	Quando o ajuste das câmeras é manual o processo é lento.
Retina	Método muito seguro. Taxa de falsa aceitação próxima de zero.	Quando o ajuste das câmeras é manual o processo é lento. Pode ser afetada por doenças. Difícil aceitação.
Geometria da mão	Fácil aceitação.	Lesões ou variação de peso podem dificultar a identificação. Custo. Pouco higiênico.
Assinatura	Fácil aceitação. Rápido e fácil de utilizar.	Variações na escrita podem dificultar a identificação.
Veias da mão	Quase impossível de falsificar. Método muito seguro. Sem contato (higiênico).	Pode ser afetado por lesões nas mãos. Custo.

Fonte: (adaptado de: VIGLIAZZI, 2006)

O uso de métodos *antispoofing*, que consiste em mascarar o IP de origem por outro IP de redes diferentes, pode evitar uma série de ataques como *man-in-the-middle*, *routing redirect*, *blind spoofing* e SYN *flood*, possibilitando detectar tentativas de fraude na autenticação.

5.3 Metodologia

Segurança é o que todos os indivíduos buscam quando o assunto é finanças, porém atualmente muitas fraudes ocorrem diariamente devido a brechas encontradas na segurança de sistemas bancários. Cada vez mais usuários utilizam a mesma senha para fazer o *login* em sites diferentes. Esse hábito aumenta o risco de acessos não autorizados, uma vez que as credenciais roubadas em um ataque a um site podem ser testadas em outro para tentar obter acesso.

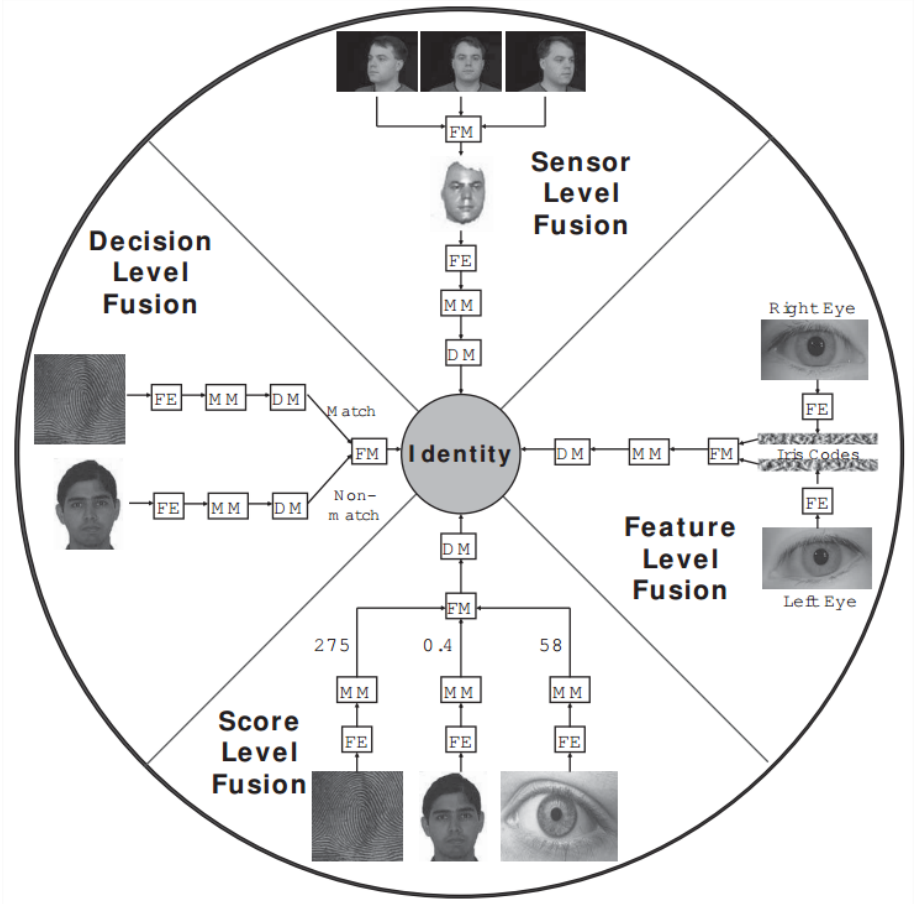
O modelo indicado a seguir busca elevar o nível de segurança para aplicações voltadas a *mobile banking*, que exigem elevado nível de confiabilidade. A seguir descrevo os fatores determinantes para a escolha da aplicação, dispositivo e biometrias:

- O ramo de aplicação foi escolhido por ser promissor e mais utilizado a cada dia pelos correntistas, conforme demonstrado na Figura 23 do Capítulo 4.
- O fator determinante para a escolha da Impressão Digital, a Face e a Voz como forma de autenticação biométrica multimodal, se deve ao fornecimento de índices menores de falsos positivos e falsos negativos durante o reconhecimento do usuário. A utilização de métodos pouco intrusivos proporciona pouca resistência por parte do usuário.
- A escolha do *smartphone* como dispositivo de autenticação se deve ao seu avanço tecnológico e sua crescente popularização, conforme descrito na Figura 16 do Capítulo 3. Atualmente vários modelos de *smartphone* já possuem leitores de impressão digital, como por exemplo: Oppo N3, HTC M9+, Samsung Galaxy S5, Samsung Galaxy S6, Samsung Galaxy Note 4, Huawei Ascend Mate 7, Meizu MX4 Pro, Apple iPhone 5S e Apple iPhone 6.

Os sistemas multibiométricos utilizam técnicas orientadas de acordo com as etapas dos processos de coleta de amostras, transmissão, processamento, extração de características, armazenamento e tomada de decisão. Elas influenciam no desempenho. Assim, temos:

- Uso de multi-sensoriamento com os respectivos algoritmos que tratam de múltiplas amostras em múltiplas instâncias. Os algoritmos precisam decidir quais das múltiplas amostras serão usadas;
- Escolha da sequência em que os múltiplos sensores devem realizar a aquisição: em cascata ou em paralelo;
- Tipos de decisão a Nível de Fusão (Figura 28): nível de sensoriamento, nível de recursos, nível de pontuação e nível de decisão.
    - **Fusão a nível de sensor:** uma fusão entre as amostras coletadas é realizada no dispositivo sensor, e apenas uma amostra é processada. Possui a desvantagem de que não é possível fazer uma fusão em amostras biométricas que tenham diferentes representações, como por exemplo, imagens de impressões digitais e amostras de voz.
    - **Fusão a nível de recurso:** o subsistema de processamento de sinal extrai as características de interesse a partir do sinal com o objetivo de armazenar e comparar. Este nível de fusão combina vários conjuntos de características e cria um único *template*. Muito utilizado em sistemas multibiométricos onde as amostras coletadas não são independentes.
    - **Fusão a nível de pontuação:** a pontuação da compatibilidade é calculada baseada no nível de similaridade entre duas ou mais amostras biométricas. As pontuações de várias fontes são integradas para gerar um único escore de compatibilidade.
    - **Fusão a nível de decisão:** a fusão pelo nível de decisão pode trabalhar de três formas: com o operador “E” (aceita apenas se ambas as amostras forem compatíveis), “Ou” (aceita se uma das amostras for compatível) ou “Decisão pela maioria” (aceita se a maioria das amostras forem compatíveis).

Figura 28 – Tipos de Níveis de Fusão



Fonte: (NANDAKUMAR, 2008)

5.4 Arquitetura da Metodologia

A autenticação multimodal indicada utiliza a fusão por nível de pontuação das biometrias: impressão digital, face e a voz. Na impressão digital são analisadas as cristas, vales e sulcos existentes, que são diferentes para cada indivíduo. Na face são analisadas características como a localização da boca, olhos, nariz, cor de pele, contorno da face, sobrancelhas, dentes, etc. Já na voz são analisados padrões harmônicos e a pronúncia de textos, levando-se em consideração a forma dos intervalos vocais, que modificam o índice espectral de uma onda acústica.

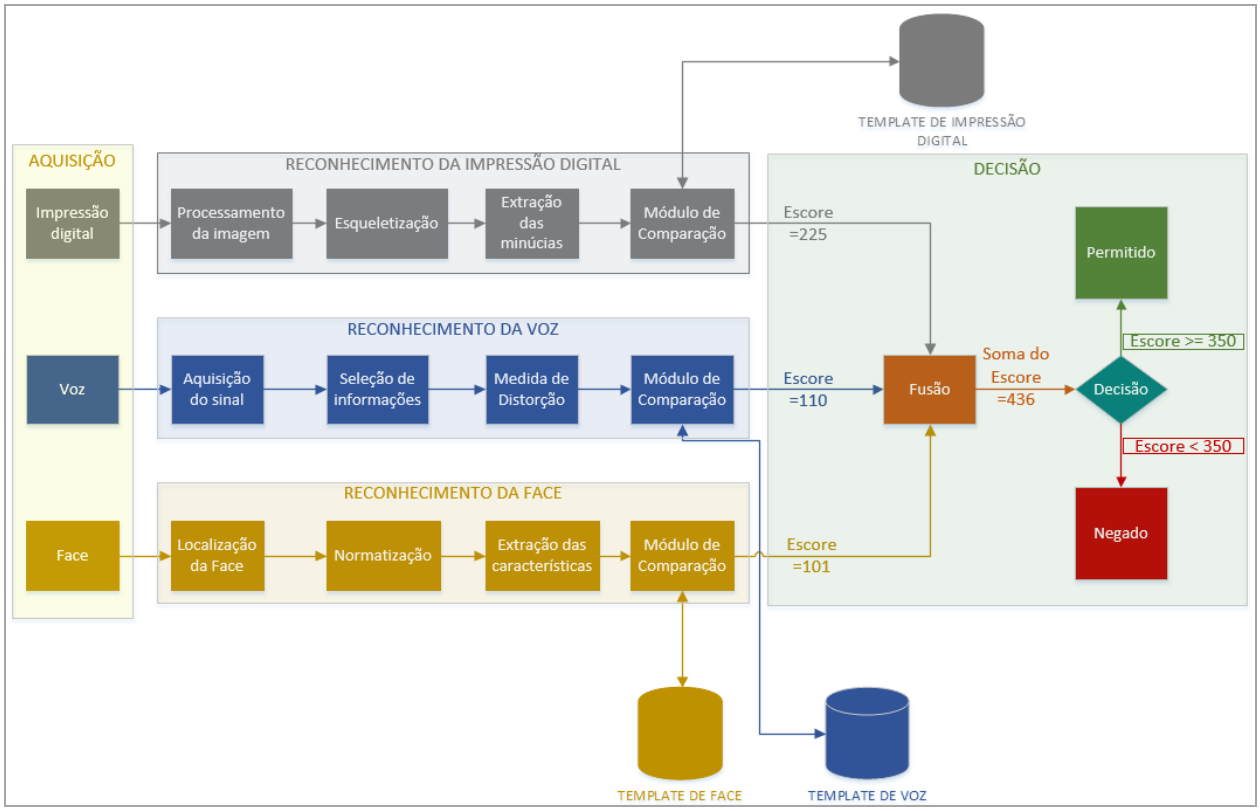
Após a análise das amostras ocorre o processo de comparação com o *template* previamente cadastrado e armazenado. No caso de sistemas como *mobile banking*, assim que o correntista insere as informações de agência e número da conta, o sistema fará uma comparação de escala 1:N. Já que o sistema possui a

informação do número da conta, só fará a comparação com os *templates* relacionados a esse número de conta.

Na Figura 29 é ilustrada a arquitetura do modelo indicado, que é dividido basicamente em três etapas:

1) **Aquisição**: o sistema coleta amostras da impressão digital, da voz e da face do usuário;
2) **Reconhecimento**: o sistema fará a análise, refinação e extração das características de cada amostra, e em seguida as compara com os *templates* previamente cadastrados. Após a comparação uma pontuação é dada baseada na de similaridade da amostra;
3) **Decisão**: o módulo de Fusão analisa as pontuações informadas pelos módulos de Comparação e repassa para o módulo de Decisão, que permite ou não o acesso ao indivíduo, com base no escore previamente definido para permitir o acesso.

Figura 29 – Arquitetura do modelo indicado com Biometria Multimodal



Fonte: (PERETTI, 2015)

A descrição do funcionamento dos segmentos: Aquisição, Reconhecimento da Impressão Digital, Reconhecimento da Voz e Reconhecimento da Face, estão disponíveis no Capítulo 1.

O módulo de comparação tem a função de receber as informações extraídas das amostras adquiridas e compará-las com a base de *templates* biométricos. Esta base de dados deve estar sob segurança e responsabilidade da instituição responsável pelo fornecimento do serviço a ser acessado.

O modulo de Fusão possui um papel fundamental no processo de reconhecimento biométrico. Após o processo de comparação entre a amostra biométrica e o *template* armazenado em um banco de dados, uma pontuação é dada baseada no nível de similaridade entre as características dos itens analisados. De posse dessa pontuação, o modulo de Fusão tem o papel de calcular o escore obtido fazendo uma simples operação de soma e aplicação de um peso para cada tipo de biometria, e em seguida repassar o resultado para o módulo de Decisão. A combinação do escore (S) pode ser obtida através da regra abaixo:

Quadro 5 – Cálculo do Escore

S = (a1p1−b1) + (a2p2−b2) + (a3p3−b3)

Fonte: (JAIN; NANDAKUMARA; ROSS, 2005)

onde p1, p2, e p3 correspondem as pontuações correspondentes obtidas da impressão digital, face e voz, respectivamente. O efeito das diferentes técnicas de normalização é determinar os pesos a1, a2 e a3, e propensão b1, b2, e b3. (JAIN; NANDAKUMARA; ROSS, 2005).

O modulo de Decisão tem a função de decidir se aceita ou não o indivíduo, baseado na comparação do escore obtido com escore previamente definido. É no módulo de Decisão é que podemos regular as taxas de FAR (*False Acceptance Rate*) e FRR (*False Rejection Rate*), baseado no escore definido para aceitar ou rejeitar um indivíduo.

Para ilustrar o módulo de Decisão, a seguir podemos visualizar um estudo realizado por Nandakumar, onde é descrito o funcionamento do módulo de decisão

baseado no teorema de Neyman–Pearson, onde é realizado o teste *likelihood ratio* (razão de verossimilhança).

Seja *S* uma variável aleatória que representa uma pontuação dada por um comparador. Seja a função de distribuição para os escores genuínos indicada por *Fgen*(*s*) (i.e.,P(*S* ≤ *s*|*S* is genuine) = *Fgen*(*s*)), com a correspondente função de densidade *fgen*(*s*). Da mesma forma, a função de distribuição para os escores de impostores ser representada por *Fimp*(*s*), com a correspondente função de densidade *fimp*(*s*). Suponha que temos de decidir entre as classes genuíno e impostor (para verificar uma identidade alegada) com base na pontuação observada *s*. Seja Ψ um teste estatístico para testar a hipótese nula *H*0: escore *S* corresponde a um impostor, e a hipótese alternativa *H*1: score *S* corresponde a um usuário genuíno. Seja Ψ(*s*) = *i* implica que decidimos em favor da *H*i, onde *i* = 0,1. A probabilidade de aceitar um impostor *H*0 é conhecida como a taxa de Falsa Aceitação (FAR). A probabilidade de corretamente rejeitar *H*0 quando *H*1 é verdadeiro é conhecida como a taxa Genuína de Aceitação (GAR). O teorema de Neyman - Pearson afirma que:

- Para testar *H*0 contra *H*1, existe um teste Ψ e uma constante *η* de tal modo que

$$P(\Psi(S) = 1|H_0) = \alpha$$

e

$$\Psi(s) = \begin{cases} 1, & \text{when } \dfrac{f_{gen}(s)}{f_{imp}(s)} > \eta, \\ 0, & \text{when } \dfrac{f_{gen}(s)}{f_{imp}(s)} < \eta. \end{cases}$$

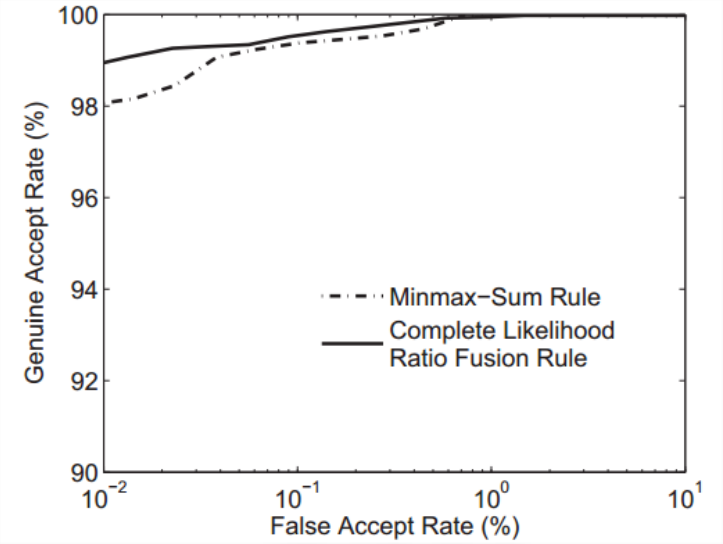
Quando *fgen*(*s*)/*fimp*(*s*) é igual a *η,* Ψ(*s*) é zero com a probabilidade *γ* e um com a probabilidade 1- *γ*. Desta forma, *γ* é escolhido de tal modo que o nível do teste é exatamente igual a *α.* (NANDAKUMAR, 2008).

- Se um teste satisfaz as duas equações para um determinado *η,* então esse é o teste mais poderoso para testar *H*0 contra *H*1 no nível *α*. (NANDAKUMAR, 2008).

De acordo com o teorema de Neyman - Pearson, dado a taxa de falsa aceitação (FAR) α, o teste adequado para decidir se a pontuação *S* corresponde a um usuário legítimo ou a um impostor é o *likelihood ratio* (razão de verossimilhança), dada pela equação Ψ(*s*). Para uma taxa de falsa aceitação (FAR) fixa, podemos selecionar um limiar *η,* de forma que o teste *likelihood ratio* (razão de verossimilhança) maximiza a taxa de aceitação genuína (GAR) e não há qualquer outra regra de decisão com uma maior GAR. (NANDAKUMAR, 2008).

Na Figura 30, podemos verificar uma comparação entre o desempenho da fusão pela regra de Soma e pela *Likelihood Ratio* (razão de verossimilhança), utilizando a base de dados NIST-Multimodal. Como podemos observar, o desempenho de ambas é praticamente igual, onde o teste com a regra *Likelihood Ratio* não fornecer qualquer melhoria significativa sobre a regra da soma. (NANDAKUMAR, 2008).

Figura 30 – Desempenho entre a Regra de Soma e a Likehood Ratio



Fonte: (NANDAKUMAR, 2008)

No entanto, essa otimização do teste *likelihood ratio* só é garantida quando as densidades subjacentes são conhecidas. Na prática, só temos um conjunto finito de pontuação genuína e de impostor, por isso precisamos estimar as densidades *fgen*(*s*) e *fimp*(*s*) antes da aplicação do teste *likelihood ratio*.

No Quadro 3, podemos observar que vários outros métodos de combinação e classificação utilizam ou não probabilidade, parametros de compatibilidade e escores:

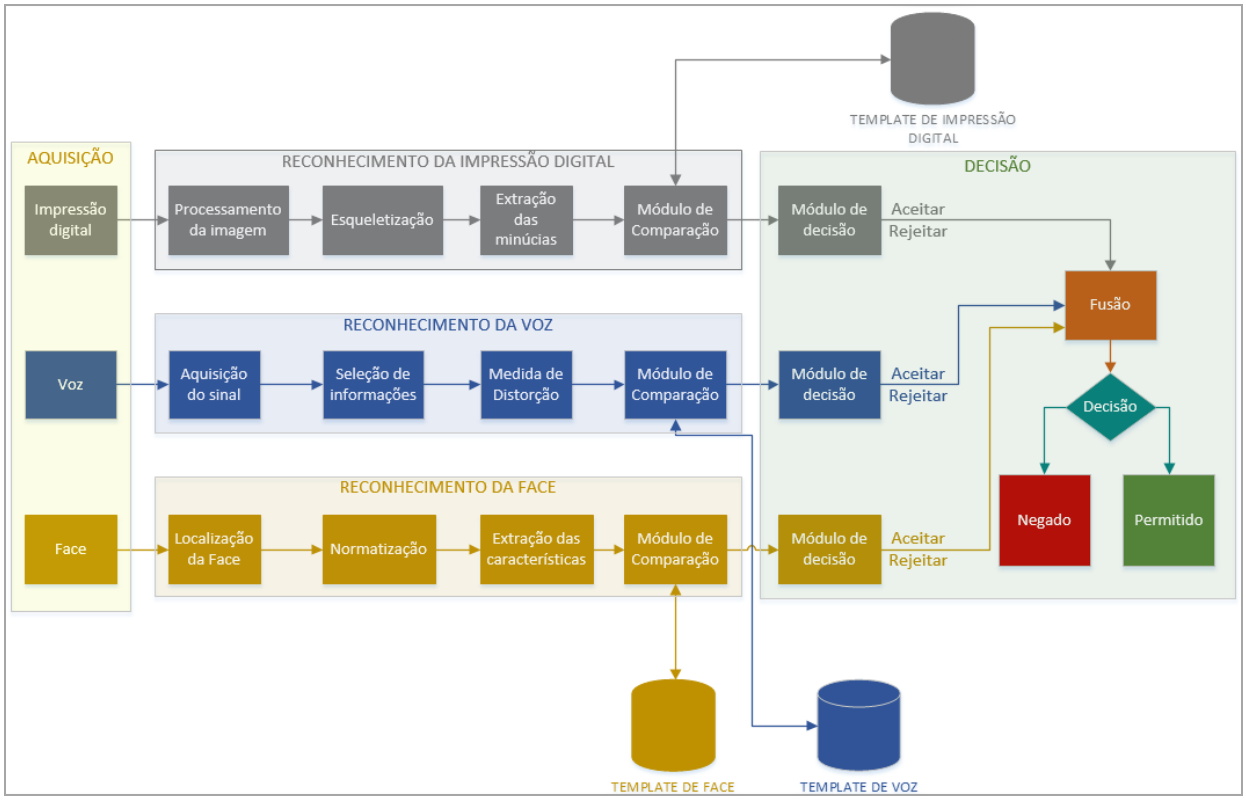
Quadro 6 – Técnicas de fusão por escore

Método	**Descrição**
Abordagens de combinação	
Soma simples	Não requer parâmetros de distribuição de probabilidade ou correspondência
Pontuação mínima	Não requer parâmetros de distribuição de probabilidade ou correspondência
Pontuação máxima	Não requer parâmetros de distribuição de probabilidade ou correspondência
Ponderação de correspondênci	Distribuições de probabilidade genuína e de impostor
Ponderação do usuário	Parâmetros de performance individual
Soma das probabilidades	Distribuições de probabilidade genuína e de impostor
Produto de probabilidades	Distribuições de probabilidade genuína e de impostor
Razão de verossimilhança	Distribuições de probabilidade genuína e de impostor
Abordagens de classificação	
K-vizinho mais próximo	Correspondencia por pontuação genuína e de impostor
Árvores de decisão	Correspondencia por pontuação genuína e de impostor
SVM	Correspondencia por pontuação genuína e de impostor
Rede neural	Correspondencia por pontuação genuína e de impostor
Análise discriminante	Correspondencia por pontuação genuína e de impostor

Fonte: (adaptado de: MODI, 2011)

A escolha do método utilizado na seção de “Decisão” deve ser observado qual o objetivo que se quer alcançar. A seguir descrevo brevemente outra abordagem na seção de decisão, onde é possível definir até oito combinações diferentes para aceitar ou rejeitar uma autenticação baseado na “Decisão pelo voto da maioria”. Na Figura 31 é possível visualizar a arquitetura de um sistema multimodal com base na Fusão a nível de decisão.

Figura 31 – Arquitetura baseada na Fusão a nível de decisão



Fonte: (PERETTI, 2015)

Neste tipo de sistema de decisão, o módulo de Fusão pode trabalhar de três formas distintas:

1) Fusão pelo operador (E):

A decisão só será “Permitido” se após a análise de todos os Módulos de decisão a resposta for “Aceitar”. Partindo dessa premissa, uma falsa aceitação ocorrerá apenas se o resultado de cada teste for uma falsa aceitação. A probabilidade de falsa aceitação P (FA) é, portanto, o produto das probabilidades obtidas em cada teste P1, P2 e P3.

Quadro 7 – Cálculo da probabilidade de Falsa Aceitação (E)

P (FA) = P1 (FA)*P2 (FA)*P3 (FA)

Fonte: (adaptado de: SAMIR et al., 2011)

Já a falsa rejeição, que consiste em negar acesso ao indivíduo cadastrado, a probabilidade pode ser obtida conforme abaixo:

Quadro 8 – Cálculo da probabilidade de Falsa Rejeição (E)

P (FR) = P1 (FR) + P2 (FR) + P3 (FR) - P1 (FR)*P2 (FR)*P3 (FR)

Fonte: (adaptado de: SAMIR et al., 2011)

2) Fusão pelo operador (OU)

A decisão só será “Permitido” se após análise de todos os Módulos de decisão a resposta de pelo menos um deles for “Aceitar”. Ou seja, usuário é aceito se pelos menos uma de suas biometrias for reconhecida. A probabilidade de falsa aceitação P (FA) pode ser obtida conforme segue abaixo:

Quadro 9 – Cálculo da probabilidade de Falsa Aceitação (OU)

P (FA) = P1 (FA) + P2 (FA) + P3 (FA) - P1 (FA)*P2 (FA)*P3 (FA)

Fonte: (adaptado de: SAMIR et al., 2011)

Com essa configuração, uma falsa rejeição pode existir somente se os três testes produzirem uma falsa rejeição. A probabilidade de falsa rejeição P (FR) é o produto das três probabilidades de falsa rejeição:

Quadro 10 – Cálculo da probabilidade de Falsa Rejeição (OU)

P (FR) = P1 (FR)*P2 (FR)*P3 (FR)

Fonte: (adaptado de: SAMIR et al., 2011)

3) Fusão pelo voto da maioria

Já neste modo, a decisão só será “Permitido” se após análise de todos os Módulos de decisão a resposta da maioria for “Aceitar”. Conforme demonstrado na Tabela 5, basicamente ocorre um processo de votação, onde cada Módulo de decisão fornece sua escolha e a decisão é tomada com base na regra da maioria.

Tabela 5 – Decisão pelo voto da maioria

SITUAÇÃO	DIGITAL	FACE	VOZ	RESULTADO
1	A	A	A	PERMITIDO
2	A	A	R	PERMITIDO
3	A	R	A	PERMITIDO
4	R	A	A	PERMITIDO
5	A	R	R	NEGADO
6	R	A	R	NEGADO
7	R	R	A	NEGADO
8	R	R	R	NEGADO

A: Aceitar R: Rejeitar

Fonte: (PERETTI, 2015)

A decisão “Negado” será tomada se a maioria das respostas dos Módulos de decisão for de “Rejeitar”.

Analisando o primeiro método de decisão através da fusão pelo operador (E), tomando como exemplo um sistema multibiométrico baseado em impressão digital, face e voz, a chance do acesso ao sistema ser negado é muito maior, pois quanto maior o número de verificações, maior é a taxa de FRR. Já a taxa de FAR é reduzida, tendo em vista que para o módulo de fusão autorizar o acesso ao sistema, todas as biometrias do usuário devem ser aceitas pelos módulos de decisão.

No segundo método de decisão baseado na fusão pelo operador (OU), a taxa de FAR aumenta, tendo em vista que se apenas uma das três biometrias for reconhecida, o sistema permitirá o acesso. Com essa situação a taxa de FAR é reduzida, e consequentemente o sistema estará mais vulnerável, chegando a se equiparar com a sistemas unimodais.

Concluímos que à medida que se reduz uma das taxas de erros, FAR ou FRR, a outra pode acabar aumentando (Figura 27). A opção mais indicada é a fusão pelo voto da maioria, onde o módulo de fusão permitirá o acesso ao usuário caso

pelos menos duas de suas biometrias forem aceitas pelos módulos de decisão, que são baseadas no nível de similaridade entre as características da amostra coletada e as armazenadas no *template*.

5.5 Normas

Atualmente o grupo que define as normas ISO/IEC adotadas para a padronização da biometria, dentro do comitê técnico de tecnologia da informação é o JTC 1/SC37.

Para quem pretende apresentar soluções relacionadas a reconhecimento biométrico multimodal, seus sistemas devem atentar para as diretrizes dispostas nas principais normas dispostas abaixo:

- **ISO/IEC TR 24722:2007 –** "*Information technology — Biometrics– Multimodal and other multibiometric fusion*". É um Relatório Técnico que contém descrições e análises e das práticas atuais em fusão multimoldal e outras fusões multibiométricas, incluindo referências a descrições mais detalhadas. Também discute a necessidade e as possíveis formas de padronização para dar suporte a sistemas multibiométricos. Contém descrições e explicações de conceitos de alto nível multibiométrico para auxiliar na explicação de fusão multibiométrica, incluindo abordagem multimodal, multi-instância, multissensorial, multi-algorítima, lógica do nível de decisão e do nível de pontuação.
- **ISO/IEC 29159-1:2010 – "***Information technology -- Biometric calibration, augmentation and fusion data -- Part 1: Fusion information format*". Esta norma aborda o método mais comum e mais facilmente implementado de fusão: a fusão por nível de pontuação. Define os componentes para a distribuição de informação da contagem a partir de um subsistema de comparação. Também auxilia na interoperabilidade e o intercâmbio de dados entre aplicações biométrica e o sistema.
- I**SO/IEC 19795-2:2007/Amd 1:2015 – "**Testing of multimodal biometric implementations". Esta norma descreve métodos para realizar testes em sistemas biométricos. Os métodos de teste descritos na ISO / IEC 19795

primeiramente eram destinados a sistemas unimodais, porém esses métodos podem ser inadequados para a execução de avaliações de desempenho em sistemas biométricos multimodais. Várias configurações são propostas para sistemas biométricos multimodais, conforme descrito na norma ISO / IEC TR 24722. É necessário identificar claramente os métodos e requisitos para avaliar sistemas biométricos multimodais, tais como variação dos parâmetros e fatores externos dependendo do ambiente.

- **ISO/IEC PRF 30107 –** "*Information technology -- Biometric presentation attack detection -- Part 1: Framework – Part 2: Data formats – Part 3: Testing and reporting*". A norma ainda está em fase de desenvolvimento, com previsão de publicação para Setembro de 2016. Na primeira parte da norma contém termos e definições que são úteis na especificação, caracterização e avaliação de métodos de detecção de ataques. A segunda parte possui a definição de um formato de dados comum para transmissão. Já na terceira são descritos os princípios e métodos de avaliação de desempenho.

Várias normas já foram publicadas a respeito de biometria. Para empresas que pretendem participar de licitações, e que queiram se basear nos padrões ISO/IEC para especificar suas soluções, essas normas são de conhecimento obrigatório.

5.6 Vulnerabilidades

Ao longo dos anos, a tecnologia biométrica tem se mostrado uma tendência no âmbito dos sistemas de autenticação. Este caminho de evolução tecnológica nos conduz a uma questão crítica que recentemente começa a ser abordada por organizações e entidades normativas, que é a resistência desta tecnologia emergente a ataques externos e, em particular, para *spoofing*, que refere-se à capacidade de fraudar um sistema biométrico reconhecendo um usuário ilegítimo como um legítimo, utilizando material forjado com características biométricas originais.

No Quadro 4, podemos observar uma série de formas e situações conhecidas em fraudes de sistemas biométricos. São classificadas em Artificiais e Humanas:

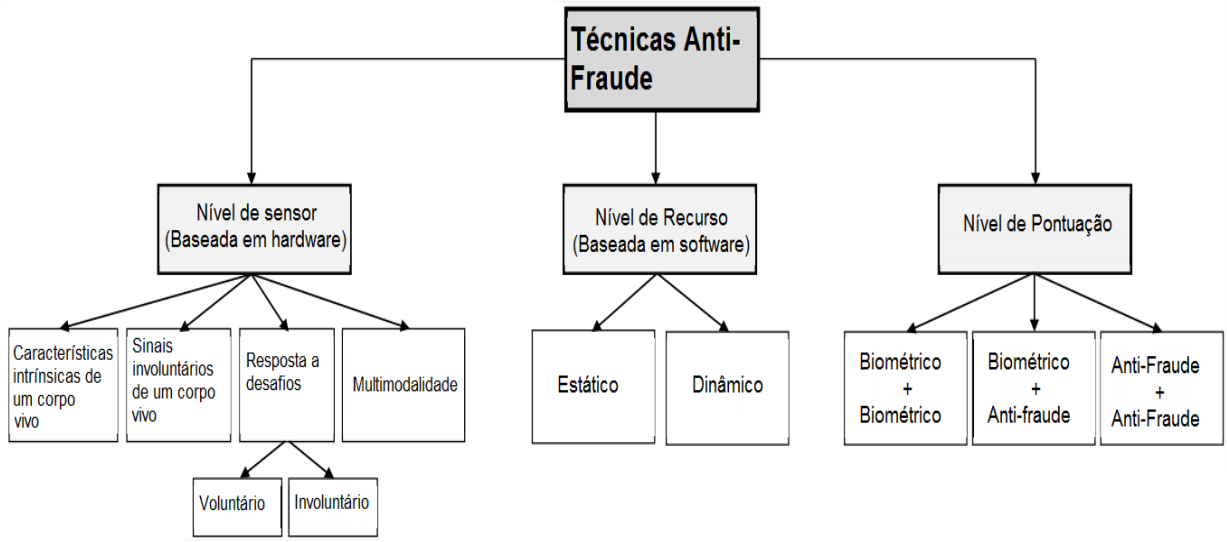
Quadro 11 – Exemplos de meios utilizados em fraudes

ARTIFICIAL	**Completa**	Dedo de goma ou látex, foto da cara ou da Iris, gravação de voz, vídeo do rosto, mão artificial, lente de contato personalizada, lente de contato personalizada artificialmente, máscara facial,
	Parcial	Cola no dedo, pelos faciais falsos, cosméticos, implantes removíveis, Óculos de Sol
HUMANA	**Inanimada**	Parte de um cadáver, dedo ou mão cortada
	Alterada	Cirurgia plástica, amputação, mutilação, transplante cirúrgico das digitais das mãos e / ou dos pés
	Não conformidade	Mimetismo, Controle de Forma da mão, assinatura forjada, Expressão Facial/Extrema, ponta ou lateral do dedo, Falsete de voz
	Conformidade	Tentativa impostora sem esforço
	Coagido	Inconsciente, sob pressão, Drogado

Fonte: (adaptado de: NEWTON, 2012)

Com o objetivo de combater essas vulnerabilidades, técnicas *anti-spoofing* podem ser aplicadas em várias etapas de um sistema de reconhecimento biométrico. Entre as técnicas citadas a biometria multimodal se destaca no nível sensorial e no de pontuação. As técnicas são distribuídas a nível de hardware e software (Figura 32).

Figura 32 – Técnicas Anti-spoofing distribuídas por níveis

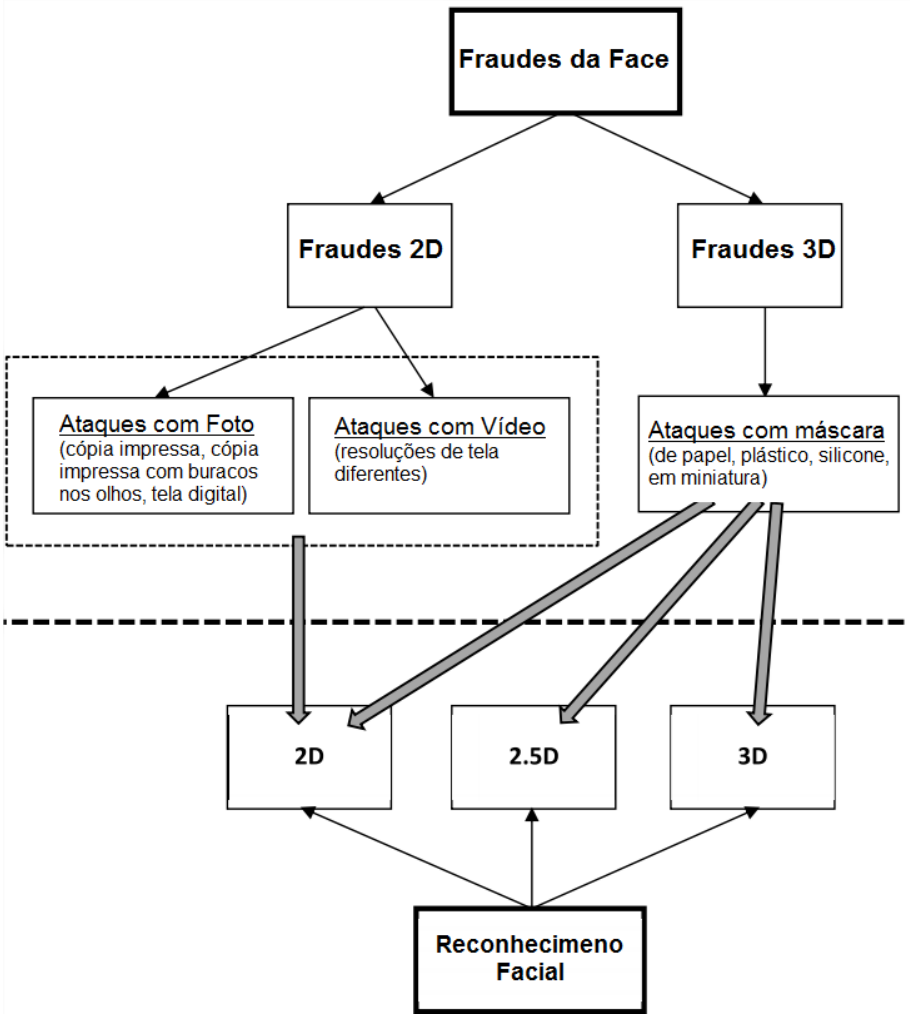


Fonte: (adaptado de: GALBALLY; MARCEL; FIERREZ, 2014)

5.6.1 Face

Vários tipos de ataques já foram mapeados, e soluções de contorno também foram apresentadas e testadas. A seguir temos uma breve descrição das principais formas de ataque a biometria facial. Na Figura 33 podemos observar a natureza da fraude, divididas entre sistemas de reconhecimento com duas dimensões, e também sistemas mais modernos que utilizam sensores tridimensionais:

Figura 33 – Esquema de fraude em Biometria Facial



Fonte: (adaptado de: GALBALLY; MARCEL; FIERREZ, 2014)

- **Ataques de imagens:** Neste tipo de ataque uma fotografia de um usuário legítimo é utilizada para tentar burlar o sistema de reconhecimento. A fotografia pode ser obtida com uma câmera digital ou internet, onde na maioria das redes sociais as pessoas carregam fotos e podem ser visualizadas publicamente. A foto pode ser impressa em um papel ou pode

ser exibida na tela de um dispositivo digital, como *smartphone* ou *tablet*. Outro tipo de ataque é o uso de uma máscara fotográfica, obtidas a partir de imagens de alta resolução. Depois de impressa, os olhos e a boca são cortados com o objetivo de simular movimentos e o piscar dos olhos. (GALBALLY; MARCEL; FIERREZ, 2014).

- **Ataques de vídeo:** Conhecido como ataque de repetição, este ataque consiste em reproduzir um vídeo de um usuário para o dispositivo de reconhecimento. O vídeo com a face do usuário atacado pode ser obtido através da internet, invasão de sua webcam ou câmera frontal de seu *smartphone*, dentre outras. (GALBALLY; MARCEL; FIERREZ, 2014).
- **Ataques máscara:** Neste tipo de ataque, é utilizada uma máscara 3D da face de um usuário legítimo, com a intensão de burlar o sistema de reconhecimento. Ainda não há muitos estudos sobre esse tipo de ataque, devido ao pequeno número de bancos de dados com máscaras reais. (GALBALLY; MARCEL; FIERREZ, 2014).

Algumas técnicas *anti-spoofing* a nível sensorial, voltadas para biometria facial, apresentaram uma melhoria significante na redução do percentual de erros, como é o caso da biometria multimodal. Na Tabela 6 também podemos visualizar bons resultados obtidos a partir de técnicas *anti-spoofing* a nível de recurso.

Tabela 6 – Técnicas anti-spoofing a nível sensorial

Técnicas anti-fraude Facial: Visão Geral					
Técnicas a nível de sensor					
Referência	**Tipo**	**Recurso e metodologia**	**Ataque**	**Base de Dados**	**Erro**
2005, Chetty and Wagner	Multibiométrica	Face + voz	Vídeo	Público, VixTIMIT DB (43 identidades, 500 amostras) e UCBN DB (30 identidades, 30 amostras)	2%
2008, Kollreider et al.	Resposta a desafio	Detecção de movimento	Foto, Vídeo	Proprietário, 15 identidades 390 amostras	3.5%
2011, Zhang et al.	Propriedade intrínseca	Reflexão utilizando iluminação multiespectrais em imagens 2D	Foto, Vídeo, Máscara	Proprietário, 40 identidades, 1.000 amostras	7%
2013, Kose and Dugelay	Propriedade intrínseca	Reflexão em varreduras 3D	Máscara	Proprietário, 20 identidades, 400 amostras	5.5%
2013, Dhamecha et al.	Sinal corporal involuntário	Imagens térmicas	Máscara	Público, 75 identidades, 1.362 amostras	13%

Fonte: (adaptado de: GALBALLY; MARCEL; FIERREZ, 2014)

5.6.2 Impressão digital

Empresas e acadêmicos do mundo todo se reúnem para organizar competições, como a LivDet. Nestas competições cada equipe apresenta seus algoritmos de detecção de amostras biométricas falsas, que posteriormente são testados e avaliados.

Além das detecções de fraude através de métodos aplicados aos Sistemas Biométricos, políticas de segurança podem ser utilizadas para elevar de forma significativa a prevenção contra a fraude, como é o caso da detecção de várias tentativas de autenticação sem sucesso, e a localização geográfica e temporal do usuário. No Quadro 5 podemos verificar os tipos de detecção descritos na terceira fase da norma ISO/IEC PRF 30107 ainda em desenvolvimento.

Quadro 12 – Tipos de detecção de fraude

Através de um sistema biométrico	Detecção de artefato
	Detecção de animação
	Resposta a desafio
	Detecção de alteração
	Detecção de não conformidade
	Detecção de coerção
	Detecção de escurecimento
Através de política de segurança do sistema	Detecção de tentativas falhas
	Geográfica
	Temporal

Fonte: (adaptado de: NEWTON, 2012)

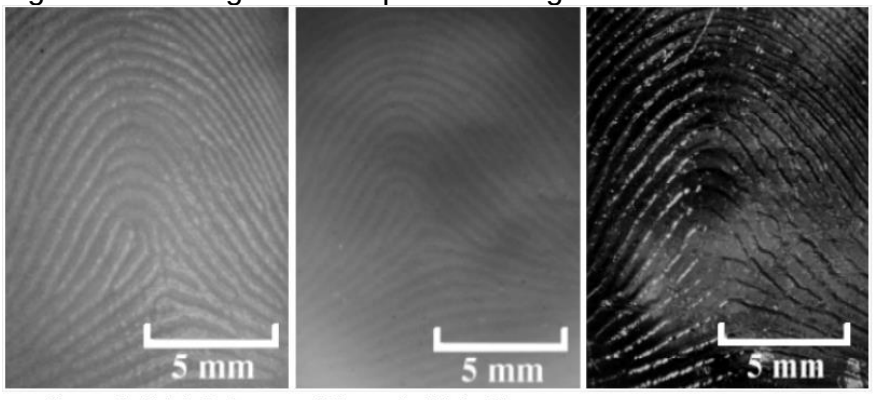
No caso da impressão digital, várias características dos artefatos biométricos sintéticos podem ser facilmente detectadas a nível sensorial. A seguir são descritas algumas dessas características em impressões digitais:

- **Variações de umidade**: cristas mais escuras correspondem a regiões úmidas do dedo, enquanto as mais claras estão associadas a regiões mais secas. Como biometrias sintéticas não possuem transpiração, as imagens de impressões digitais sintéticas devem apresentar pouca variabilidade de níveis de cinza. (PEREIRA, 2013).

- **Distribuição dos poros de suor**: através do processo de transpiração, é possível observar regiões secas no intervalo entre os poros. Em imagens de impressões digitais autênticas, a periodicidade desses pontos coincide com o intervalo entre os poros ao longo das cristas. (PEREIRA, 2013).
- **Continuidade das cristas papilares**: imperfeições na superfície de uma impressão digital sintética surgem ainda no seu processo de fabricação devido, por exemplo, interrupção das cristas papilares, e dependendo do material utilizado, podem surgir até bolhas de ar. (PEREIRA, 2013).
- **Rugosidade da superfície**: materiais sintéticos utilizados na confecção das falsificações, como por exemplo cola e gelatina, são compostos por moléculas orgânicas que tendem a se aglomerar durante o processo de fabricação. Isso aumenta o nível de rugosidade da superior da pele, divergindo da encontrada nos dedos vivos. (PEREIRA, 2013).

Diversos tipos de artefatos de impressões digitais já foram utilizados para tentar fraudar os sistemas biométricos. Sua fabricação consiste basicamente em obter a impressão digital a ser copiada, gerar o molde da forma, e finalmente a criação do artefato com o tipo de material desejado. Em sua maioria são utilizados moldes de silicone, mas podem ser criados látex transparente ou líquido, silicone, gelatina, goma, fita adesiva, borracha, entre outros. Na Figura 34 podemos visualizar alguns exemplos:

Figura 34 – Imagens de impressões digitais reais e fraudadas



Fonte: (adaptado de: MATSUMOTO et al., 2002)

Técnicas *anti-spoofing* buscam avaliar a nível sensorial, através de sensor capacitivo, as características eletrostáticas no momento do reconhecimento. Conforme Tabela 7, os moldes de silicone ou gelatina não possuem a mesma humidade e resistência elétrica que o dedo real. Dessa forma não irá acionar a captura do sensor capacitivo.

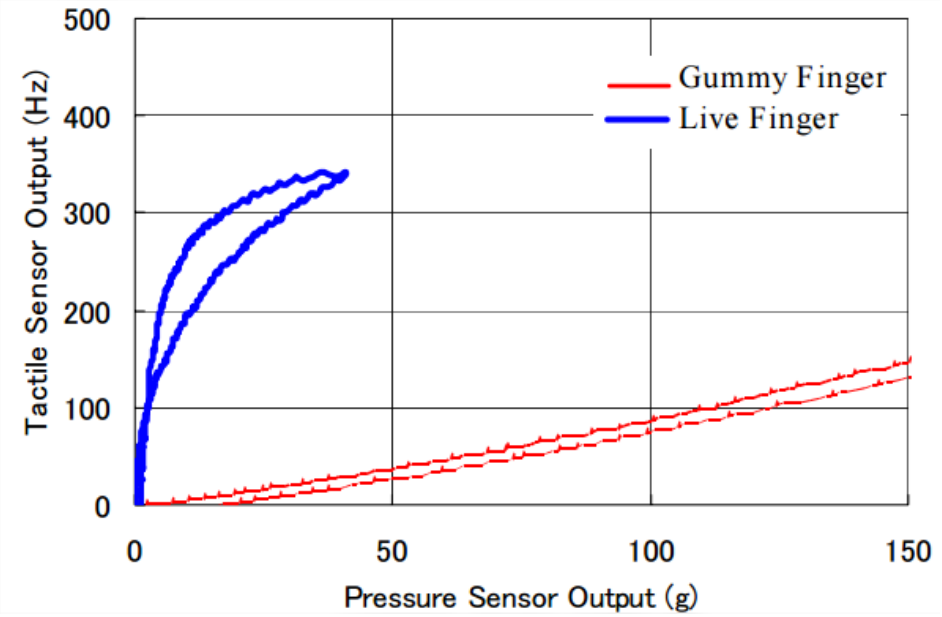
Tabela 7 – Características dos dedos

	Humidade	**Resistência elétrica**
Dedo real	16%	16 Mohms/cm
Dedo de gelatina	23%	20 Mohms/cm

Fonte: (adaptado de: MATSUMOTO et al., 2002)

Outra diferença encontrada a nível sensorial é a pressão aplicada no sensor biométrico. Conforme a Figura 35, a superfície do dedo real possui uma frequência de contato maior e com pouca pressão, já a superfície de um dedo falso feito com goma por exemplo, é necessário aplicar uma maior pressão para que frequência de contato aumente.

Figura 35 – Pressão por superfície de contato



Fonte: (MATSUMOTO et al., 2002)

Mesmo que se consiga de alguma forma acionar o sensor capacitivo, com a luz infravermelha é possível identificar a composição do material através da frequência de reflexão da luz. Nos sensores mais modernos, o padrão de veias do dedo é analisado. Por fim ainda há controles definidos em algoritmos de processamento, que identificam se há alguma distorção na imagem capturada pelo sensor.

5.6.3 Voz

Na autenticação biométrica pela voz, os ataques são distribuídos basicamente em quatro tipos: Imitação, repetição, síntese e conversão. Abaixo temos uma breve descrição de cada um.

- **Imitação**: a imitação se refere a ataques de *spoofing* em que um atacante tenta imitar a fala de outro indivíduo. Esta é uma das formas mais evidentes de falsificação e mais antiga estudada. O ASV (*Automatic Speaker Verification*) pode ser enganado apenas por imitadores que possuem a voz naturalmente igual à do indivíduo alvo (LAU; WAGNER; TRAN, 2004). Em HAUTAMÄKI et al. (2015) não foi observado tal efeito sistematicamente. Isto poderia ser porque, apesar da multiplicidade de técnicas de normalização aplicada, características MFCC (*Mel frequency Cepstral Coefficients*) são sensíveis não só a mudanças na qualidade de voz, mas também a mudanças de canal (devido a diferentes condições de gravação). (EVANS et al., 2014).
- **Repetição**: utilização de um discurso previamente gravado a partir de um usuário verdadeiro sob a forma de gravações de fala contínua, ou amostras resultantes à concatenação de segmentos mais curtos. Repetição é um ataque de relativamente baixa tecnologia ao alcance de qualquer invasor em potencial, mesmo sem conhecimento especializado em processamento de fala. A disponibilidade de dispositivos de gravação em alta qualidade e softwares de edição de áudio digital, pode sugerir que a repetição é eficaz e difícil de detectar. Em (ZHI-FENG; GANG; HE, 2011) duas contramedidas são

comparadas, ambas baseadas na detecção de diferenças de características do canal de espera entre tentativas verdadeiras e falsas. O desempenho de um sistema baseado em modelos de misturas Gaussianas GMM com UBM (*Universal Background Model*) com uma linha de base EER de 40% sob o ataque *spoofing* cai para 29%, e com a segunda contramedida a EER cai para 10%. (EVANS et al., 2014).

- **Síntese de voz**: síntese de voz, comumente conhecida como texto para fala (TTS), é uma técnica para a geração compreensível de uma pronúncia artificial para qualquer texto. É amplamente utilizada em várias aplicações, incluindo sistemas de navegação, e-books, funções de voz para deficientes visuais. Apenas um pequeno número de tentativas para diferenciar a voz sintética da fala natural tem sido investigado, e atualmente não existe qualquer solução geral que é independente a partir de métodos de síntese de voz específicos. (EVANS et al., 2014).
- **Conversão de voz**: conversão de voz é um sub-domínio de transformação de voz, que visa converter a voz de um indivíduo para a de outro. Duas abordagens para a detecção do sinal artificial são abordadas em (ALEGRE; VIPPERLA; EVANS, 2012). Experimentos mostram que os classificadores SVM baseados em vetores são naturalmente robustos para tais ataques, tanto que todos os ataques de *spoofing* podem ser detectados usando um recurso de variabilidade de nível de locução, que detecta a ausência de natural, característica variável dinâmica da fala legítima. Uma abordagem alternativa baseada na análise da qualidade da voz é menos dependente do conhecimento explícito do ataque, mas menos eficaz na sua detecção. (EVANS et al., 2014).

Na Tabela 8 podemos visualizar um pequeno resumo das quatro técnicas de *spoofing*, onde são avaliados o nível de dificuldade de exploração da técnica, e sua efetividade em sistemas dependentes ou não de texto.

Tabela 8 – Dificuldade e riscos de técnicas contra ASV

Técnica de *Spoofing*	**Descrição**	**Acessibilidade**	**Efetividade (Risco)**	
			Independente de Texto	**Dependente de Texto**
Imitação	Imitação da voz humana	Baixa	Baixa	Baixa
Repetição	Repetição de uma locução pré-gravada	Alta	Alta	Baixa
Síntese de Voz	Geração de voz a partir de texto	Média	Alta	Alta
Conversão de voz	Conversão de voz de um indivíduo para outro	Média	Alta	Alta

Fonte: (adaptado de: EVANS et al., 2014)

5.7 Custo

Outro fator decisivo para implantação de novas tecnologias é o custo. A menos de dois anos, muitas grandes instituições bancárias foram se afastando da possibilidade de adoção da tecnologia biométrica devido ao custo e a complexidade de integrá-la em sua infraestrutura de TI. No entanto, os recentes desenvolvimentos na área, bem como mudanças nos padrões de comportamento do consumidor têm ajudado o sector bancário a visualizar a adoção biométrica não apenas como possível, mas também como favorável.

O custo da implantação de um sistema de reconhecimento biométrico está diretamente relacionado com a quantidade de usuário, frequência de autenticação e a natureza da aplicação. Qualquer instituição que pretenda adotar a autenticação biométrica deve se atentar a custos relacionados a treinamento, campanhas de divulgação, aumento de velocidade nos links de comunicação, infraestrutura de processamento, segurança, armazenamento e backup. No caso do *mobile banking*, o custo relacionado aos sensores, que a pouco tempo eram considerados como a maior barreira para a adoção da tecnologia, agora é repassado para o usuário final, que necessita possuir um dispositivo móvel compatível, seja um *smartphone* ou *tablet*.

A razão pelo qual mais bancos estão investindo em biometria é o seu potencial para reduzir a frequência de fraudes que afetam seus clientes. Através da utilização da autenticação multimodal (Ex: impressão digital, reconhecimento de voz, face, olho) ao invés de senhas digitadas, os bancos podem reduzir significativamente o número de casos de comprometimento de contas de clientes.

Isso está se tornando uma questão cada vez relacionada com o roubo de dados on-line em ascensão. Um relatório recente do provedor de software de segurança Kaspersky Lab revela que os bancos e credores quase sempre tem de compensar seus clientes por cobranças fraudulentas. No entanto, mais de metade (52%) o fazem sem a realização de qualquer tipo de investigação antes de conceder a compensação. Isso ocorre devido ao aumento dos custos de tais esforços. Cerca de 47 % das empresas financeiras pensam que a perda de credibilidade ou danos à reputação como resultado de uma violação de dados é a pior consequência para a empresa (Kaspersky Lab).

Nuance, uma empresa multinacional de softwares, afirma que seus clientes sofreram uma redução de até 10 vezes na fraude, migrando para voz biometria. Este tipo de redução de fraudes representa uma enorme economia de custos para o banco em questão, uma vez que cada tentativa de fraude impedida evita a necessidade de uma investigação sobre o incidente, bem como qualquer recuperação ou reembolso de bens perdidos. (NUANCE).

5.8 Aceitação

O fator mais importante da adoção de um sistema de reconhecimento biométrico é a aceitação por parte de seus usuários. Sem sua aceitação, não é possível colher os benefícios oriundos da segurança proporcionada pela autenticação biométrica, e o projeto torna-se fracassado. A escolha do fator biométrico a ser utilizado para reconhecimento é um item determinante para a aceitação dos usuários. Falhas de reconhecimento em um determinado fator biométrico diminuem a aceitação do usuário. Geralmente métodos não intrusivos costumam ter maior aceitação, porém não se descarta a necessidade de campanhas de divulgação e instrução para o usuário final.

Em uma pesquisa realizada em Abril de 2015 com cerca de 2 mil adultos do Reino Unido conduzida pela YouGov, em nome da agência de crédito Equifax verificou-se que 31% dos consumidores prefeririam ser reconhecidos através de impressões digitais para ter acesso a serviços bancários on-line. Dois bancos no Reino Unido, o Royal Bank of Scotland e NatWest, já implementaram a tecnologia de impressão digital como forma de autenticação, devido à demanda do cliente para o serviço. Apenas 21% dos entrevistados para Equifax disseram que preferem responder perguntas de segurança e apenas 3% eram a favor da tecnologia de reconhecimento de voz. (Equifax).

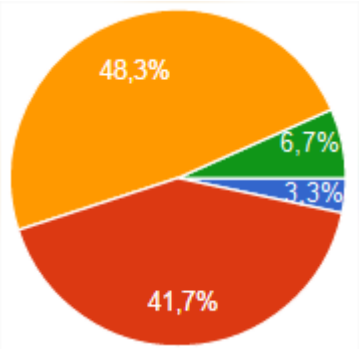
Em outro estudo realizado pela empresa Gigya, foi constatado uma crescente aceitação de métodos de autenticação biométrica. A pesquisa foi realizada em 2015 com 4 mil indivíduos, sendo 2 mil norte-americanos e outros 2 mil britânicos. Um dos resultados obtidos foi que 32% dos entrevistados do Reino Unido e 41% dos EUA dizer que eles aceitariam serem autenticados em um site ou aplicativo móvel usando sua impressão digital, rosto ou olho.

Já no Brasil, um estudo realizado pela empresa Easy Solutions (Visão dos consumidores latino-americanos sobre fraude eletrônica em 2015), mostra que “67% dos usuários estariam mais dispostos a fazer transações eletrônicas se para realizar essas operações tivessem de usar mais uma senha, por exemplo”, diz Silvia Lopez, diretora de Marketing da Easy Solutions. Acrescenta ainda que isso demonstra a disposição para utilizarem uma autenticação mais forte no sentido de aumentar a segurança, mesmo que isso implique em algum trabalho adicional para eles. Outro dado relevante é que 84% dos brasileiros acreditam que os bancos devem aplicar medidas de segurança mais fortes, além de um nome de usuário e senha para identificar os clientes e permitir-lhes o acesso a serviços eletrônicos”, finaliza a executiva.

Com o objetivo de identificar a aceitação pela sociedade acerca do uso da biometria como forma de autenticação, foi realizada uma breve pesquisa de campo com 60 colaboradores de uma instituição financeira, sendo 48 homens e 12 mulheres, onde 90% dos entrevistados tem entre 20 e 40 anos de idade. Foram realizadas perguntas acerca do conhecimento e utilização da biometria como forma de autenticação. O formulário de pesquisa está disponível no APÊNDICE desse trabalho. A seguir temos alguns resultados relevantes.

Qual a sua faixa etária?

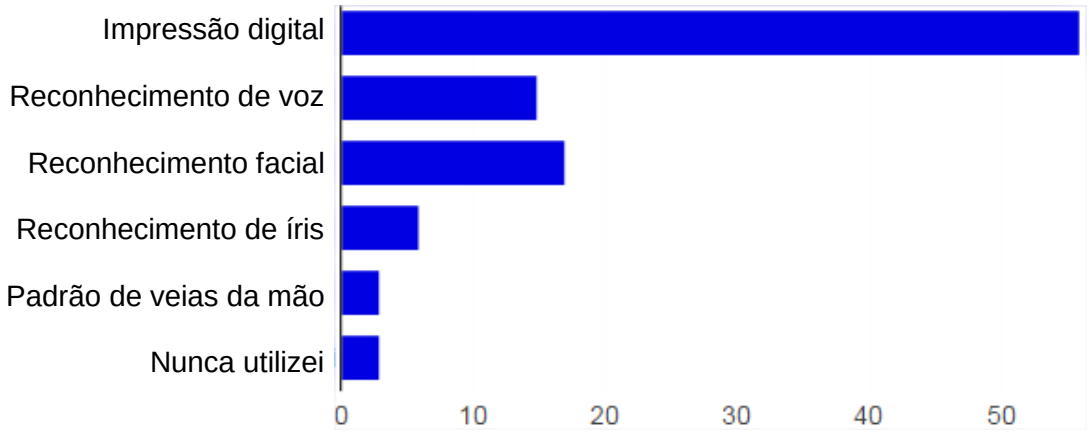
Abaixo de 20 anos:	2	**3.3%**
20 a 30 anos:	25	**41.7%**
30 a 40 anos:	29	**48.3%**
Acima de 40 anos:	4	**6.7%**



Sexo:

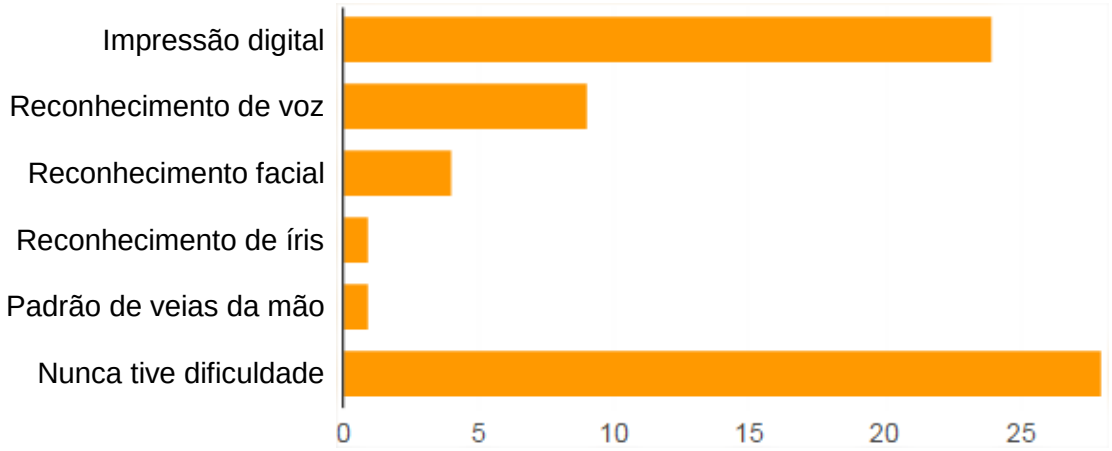
Masculino:	48	**80%**
Feminino:	12	**20%**

Você já utilizou algum dos seguintes métodos de autenticação biométrica?



Impressão digital	56	**93.3%**
Reconhecimento de voz	15	**25%**
Reconhecimento facial	17	**28.3%**
Reconhecimento de íris	6	**10%**
Padrão de veias da mão	3	**5%**
Nunca utilizei	3	**5%**

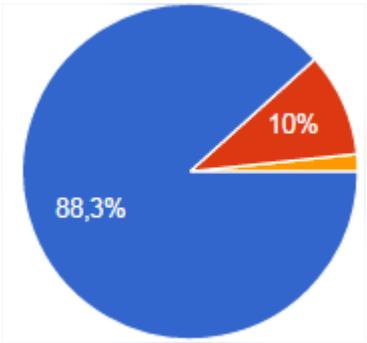
Você já teve dificuldade em utilizar algum sistema de reconhecimento biométrico? Em caso afirmativo, qual?



Impressão digital	24	**40.7%**
Reconhecimento de voz	9	**15.3%**
Reconhecimento facial	4	**6.8%**
Reconhecimento de íris	1	**1.7%**
Padrão de veias da mão	1	**1.7%**
Nunca tive dificuldade	28	**47.5%**

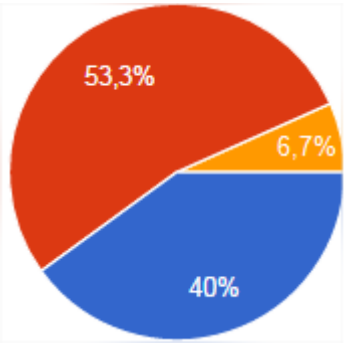
Você realiza pagamentos/transferências através do Mobile Banking?

Sim	53	**88.3%**
Não	6	**10%**
Não acha seguro	1	**1.7%**



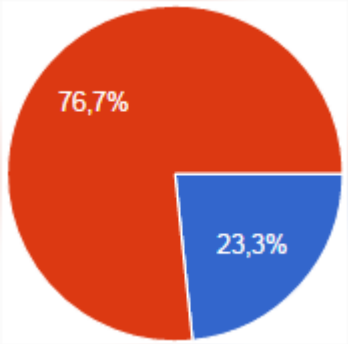
Seu smartphone possui leitor de impressão digital ou Touch ID?

Sim	24	**40%**
Não	32	**53.3%**
Não sabe	4	**6.7%**



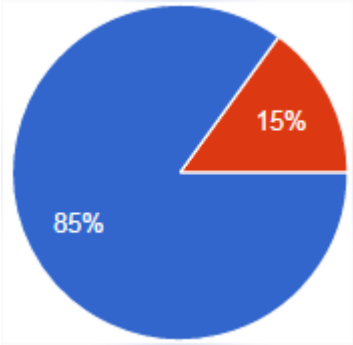
Você utiliza o leitor de impressões digitais para validar compras ou acessar sua conta bancária?

Sim	14	**23.3%**
Não	46	**76.7%**



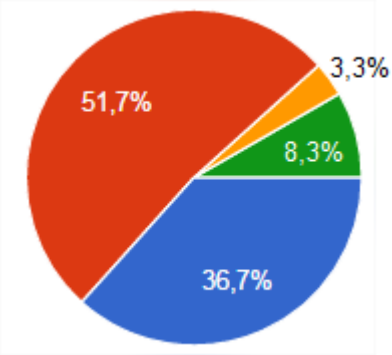
Supondo que seu smartphone possua leitor de impressão digital, câmera frontal e microfone. Com o objetivo de elevar o nível de segurança no processo de autenticação, você aceitaria ser reconhecido por sua impressão digital, face e voz ao invés da atual senha de acesso ao Banco?

Sim	51	**85%**
Não	9	**15%**



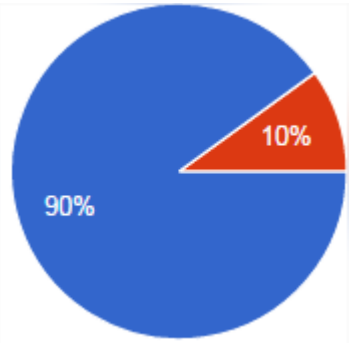
Pensando na fraude eletrônica em Mobile Banking, quem você acha que tem a maior responsabilidade pela segurança?

Usuário	22	**36.7%**
Bancos	31	**51.7%**
Governo	2	**3.3%**
Fabricantes de smartphones/tablets	5	**8.3%**



Você considera possível reduzir o número de fraudes eletrônicas adotando a biometria como forma de autenticação?

Sim	54	**90%**
Não	6	**10%**



Através da pesquisa realizada, observamos que a autenticação biométrica entre os entrevistados está significativamente popularizada, onde 95% já utilizaram alguma forma de reconhecimento biométrico. Em primeiro lugar está a impressão digital (93,3%), em segundo o reconhecimento facial (28,3%), em terceiro o reconhecimento pela voz (25%), seguido da íris (10%) e o padrão de veias da mão (5%). Porém 52,5% dos entrevistados declaram ter tido dificuldades em algum sistema de reconhecimento biométrico.

Em relação ao *mobile banking*, 88,3% dos entrevistados realizam pagamentos/transferências. Outro fator relevante é que 40% dos entrevistados possuem um *smartphone* com leitor biométrico, porém apenas 23,3% o utilizam para validar compras ou acessar a conta bancária. Esse número sugere que ainda falta

conhecimento por parte dos usuários acerca do uso da tecnologia, o que demanda campanhas educativas por parte das instituições.

Quando questionados se aceitariam serem reconhecidos por sua impressão digital, face e voz ao invés da atual senha de acesso ao Banco, 85% dos entrevistados foram favoráveis ao reconhecimento biométrico, e 90% acreditam que é possível reduzir o número de fraudes eletrônicas. Esse número é extremamente favorável para instituições que pretendem adotar um método de autenticação mais seguro, já que mais da metade dos entrevistados (51,7%) acreditam que os Bancos são os principais responsáveis pela segurança do *mobile banking*. Apenas 36,7% dos entrevistados sentem-se responsáveis por se prevenir contra fraudes eletrônicas.

CONSIDERAÇÕES FINAIS

É muito importante lembrar que o reconhecimento biométrico não é cem por cento preciso, é apenas o meio mais confiável de identificar indivíduos a partir de suas características através de um sistema. Os principais pontos fortes do reconhecimento através da biometria são: as características biométricas estão diretamente ligadas a uma única identidade; através do reconhecimento biométrico não é necessário armazenar nenhuma informação por parte do usuário, e consequentemente não pode ser esquecida ou compartilhada.

Do contrário da famosa senha de acesso que nos preocupamos em mantê-la em sigilo, a nossa biometria não é um segredo. A imagem da nossa face e o som de nossa voz podem ser obtidos por pessoas mal intencionadas sem que percebamos. Diariamente deixamos nossas digitais em toda parte, sem falar nas imagens armazenadas em alguns sistemas de controle de acesso ou em “relógios de ponto eletrônico” nas instituições de trabalho. Diversas pesquisas e normas têm sido utilizadas como contramedida aos pontos fracos.

Outras questões que devemos nos preocupar são as consequências da implantação de um sistema de reconhecimento biométrico. Ao reforçar a segurança de um sistema, a tendência é que os indivíduos mal intencionados ataquem a parte mais vulnerável, que nesse caso passa a ser o usuário. Conforme súmula 479 do STJ, a instituição financeira não se responsabiliza por prejuízos oriundos de sequestro relâmpago, devido à natureza externa do fato, que é classificado como imprevisível ou inevitável, com exceção de crimes ocorridos dentro de uma agência bancária, por exemplo. O cliente pode ser sequestrado e usado para cometer fraudes já que suas biometrias são parte do processo de autenticação. Por esse motivo se faz necessário utilizar os princípios de uma autenticação multifator, que deve ser baseada no que se sabe, no que possui e no que é. A biometria por si só não garante a segurança de acesso aos sistemas, ela é um forte aliado para elevar o nível de segurança. No caso do *mobile banking,* também se faz necessário fornecer informações que o cliente sabe, como perguntas de segurança sobre o titular da conta (Nome da Mãe, Local ou Data de Nascimento, etc.). Já para o que se

possui, é utilizado o próprio dispositivo móvel (*tablet/smartphone*), que deve ser devidamente cadastrado e liberado pelo próprio cliente.

Através da pesquisa realizada, podemos inferir que a autenticação biométrica está bastante popularizada. Apenas três entrevistados nunca utilizaram o reconhecimento biométrico. Também é possível verificar que o *mobile banking* é utilizado por mais de 80% dos entrevistados para realizar transações de pagamentos/transferências, o que indica um elevado nível de confiança depositado nesse canal de atendimento e reforça a necessidade de aprimorar a segurança atual. O mecanismo de autenticação baseado em biometria multimodal (impressão digital, face e voz) proposto na pesquisa, obteve uma aceitação de 85% dos entrevistados, contra 15% que ainda preferem serem autenticados por uma senha. Estes comparativos demonstram que a biometria multimodal é considerada adequada para *mobile banking*, já que as biometrias utilizadas não são invasivas, e consequentemente possuem maior aceitação por parte dos usuários, além do fato do avanço tecnológico dos dispositivos móveis possibilitarem a implantação dos sensores biométricos.

Atualmente o meio de reconhecimento biométrico mais utilizado é a impressão digital, porém caso o usuário tenha alguma alergia ou lesão nos dedos, o reconhecimento pode ser prejudicado. A biometria multimodal veio para solucionar esse problema, pois mesmo que o usuário possua alguma deficiência em uma de suas biometrias, ainda assim será possível autenticá-lo com outra característica biométrica.

Os principais fatores que tornam viável o uso da biometria multimodal conforme modelo indicado no capítulo 5, são: alto índice de aceitação por parte dos entrevistados; é pessoal e intransferível; não pode ser esquecida; apresenta elevado desempenho e alto nível de confiabilidade em verificar a identidade de um usuário previamente cadastrado, podendo alcançar taxas de erros consideravelmente menores do que em sistemas unimodais. Este é um dos maiores desafios da tecnologia moderna, principalmente em aplicações como o *mobile banking,* que envolve tanto informações sigilosas quanto o patrimônio dos clientes.

Não podemos nos esquecer da segurança. Vimos que várias técnicas de *spoofing* estão surgindo, fazendo com que novos dispositivos *antispoofing* sejam implantados a nível de hardware e software. O sistema multibiométrico por si só é

mais resistente a ataques do que sistemas unimodais, uma vez que o invasor (impostor) precisaria burlar as várias modalidades. Diferente das senhas e tokens, a biometria é pessoal e intransferível, o que impossibilita seu compartilhamento, além de serem muito difíceis de copiar. Ainda assim a infraestrutura de comunicação entre cliente e servidor deve ser continuamente protegida. O ideal é que o *template* dos usuários seja armazenado em uma base de dados sob responsabilidade da instituição que mantém os dados do usuário. Algumas instituições confiam tal segurança a tecnologia do dispositivo utilizado pelo usuário, onde seu *template* fica armazenado no próprio dispositivo. Em caso de comprometimento da segurança do dispositivo o *template* do usuário pode ser obtido por pessoas/aplicações não autorizadas.

A tendência do mercado é a adoção do reconhecimento biométrico. A divulgação e as campanhas de conscientização serão pontos chave para o sucesso do uso da biometria. Conforme estudo realizado em 2015 pela empresa de consultoria norte-americana Tractica, o uso da biometria deve crescer mais de 25% ao ano até 2024. Conforme relatório divulgado em Janeiro de 2015 pela empresa Juniper, mais de 770 milhões de aplicativos de autenticação biométrica deverão ser baixados anualmente até 2019.

O banco norte-americano Wells Fargo lançou recentemente uma nova versão de seu *mobile banking* utilizando biometria multimodal, que utiliza biometrias de voz e face capturadas simultaneamente pelo *smartphone* para autenticação de seus clientes. Com a fusão de duas biometrias é possível aumentar a precisão e reduzir os efeitos de interferências do ambiente (ruído, iluminação) durante a captura biométrica.

Em relação à adoção da biometria em *mobile banking,* várias instituições financeiras do Brasil já utilizam a impressão digital como complemento na autenticação. O Sicoob foi pioneiro em atualizar seu aplicativo para o iOS 8 com suporte ao Touch ID. Basicamente a autenticação ocorre através da integração entre o *mobile banking* da instituição e o Touch ID (Apple) ou Fingerprint (Samsung), que previamente deve ser configurado pelo próprio usuário.

O reconhecimento biométrico do *mobile banking* do Sicoob é compatível com os *smartphones* da Apple (iPhone 5s, 6 e 6 Plus), e com os *smartphones* da Samsung (Galaxy S5, S6, S6 Edge, Note 4 e Alpha). Conforme dados divulgados

pelo Sicoob, 22% do total de transações executadas em Outubro de 2015, que equivalem a 31,5 milhões de operações, foram feitas por meio de dispositivos móveis. Nesse mês, as transações efetuadas pelos canais móveis foi 148% superior ao mesmo período de 2014. Esse valor reafirma a aceitação desse canal de atendimento por parte dos usuários.

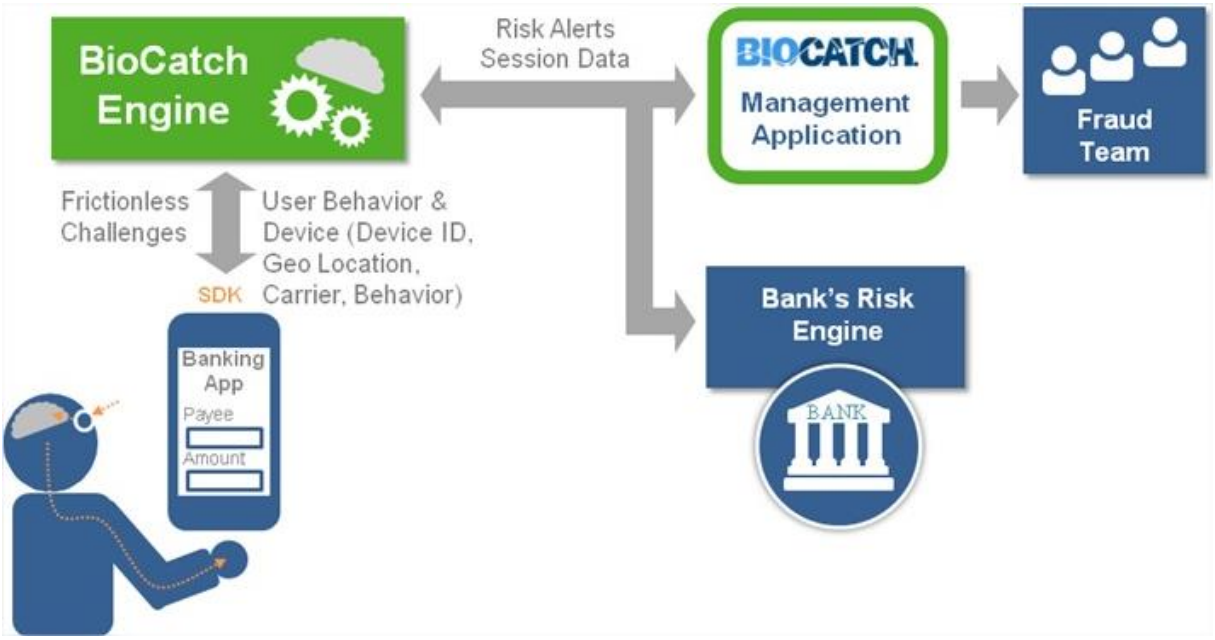
Com o uso do reconhecimento biométrico multimodal, é possível reduzir o problema da não-universalidade, e consequentemente atingir uma parcela maior de usuários. Espera-se obter uma boa aceitação por parte dos usuários, tendo em vista que as biometrias utilizadas variam de um indivíduo para o outro. Um dia chegaremos ao ponto em que não precisaremos mais de cartões de crédito ou senha de acesso. O objetivo é se apresentar e ser reconhecido, não sendo mais necessário guardar ou gerenciar senhas.

TRABALHOS FUTUROS

Como sugestão de trabalho futuro, indico o estudo relacionado a fusão da biometria física com a biometria cognitiva. Um assunto “recém-nascido” no âmbito do reconhecimento biométrico utilizando *smartphones* com sensores de movimento, localização, análise sonora do ambiente, e até a força aplicada no toque de tela. Trata-se da criação de uma “identidade” do usuário constantemente, onde seu comportamento está sempre sendo analisado e sua identidade atualizada.

Na edição de 2014 do CIAB FEBRABAN (Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras), a Order Soluções em TI apresentou tecnologias de biometria cognitiva, voz e face e suas diversas aplicações no combate a fraudes e autenticação forte por múltiplos fatores. Uma das soluções apresentadas foi a BioCatch (Figura 36), tecnologia baseada em autenticação contínua, coletando de dados biométricos do comportamento do usuário a partir da tela sensível ao toque e o sensor de acelerômetro.

Figura 36 – Arquitetura da Solução BioCatch



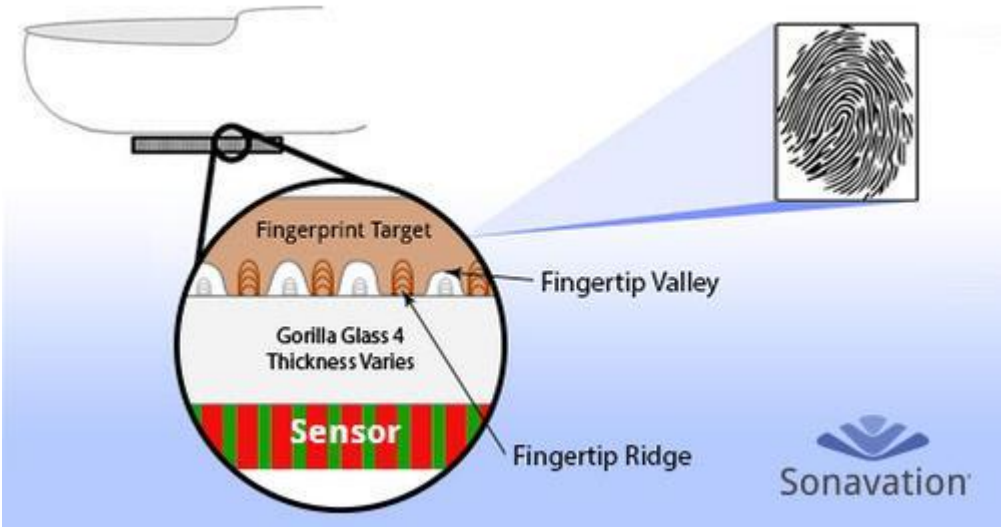
Fonte: (Order Soluções em TI)

São levados em conta como o usuário segura o dispositivo, a força aplicada no toque da tela, o tamanho da área da superfície quando o dedo pressiona a tela, entre outros. A taxa de falso positivo alcançada é de 0,5%, sendo possível detectar mais de 90% de intrusos.

A BioCatch é um fornecedor líder de biometria cognitiva, soluções de autenticação e detecção de *malware* para aplicações mobile e web. Disponível como uma solução baseada em nuvem, a BioCatch recolhe e analisa mais de 400 parâmetros cognitivos para gerar um perfil de usuário único. (CIAB FEBRABAN).

Em relação a tecnologias para sensores em dispositivos móveis, destaco a solução apresentada pela Sonovation. Consiste na identificação da impressão digital através de sensores abaixo da tela de vidro do dispositivo móvel. Com o sensor é possível capturar imagens de impressões digitais através 400UM e 750UM do Gorilla Glass 4 (Figura 37). A tecnologia baseada em ultrassom constrói um modelo 3D detalhado de sua impressão digital, possibilitando a detecção de sulcos e poros do dedo.

Figura 37 – Sensor de impressão digital com Gorilla Glass 4



Fonte: (Sonovation)

Como podemos notar, o reconhecimento baseado no que somos está apenas começando. Várias iniciativas e soluções nesse setor ainda estão por vir, onde provavelmente não usaremos mais a “velha” senha.

REFERÊNCIAS

ALECRIM, Emerson. *O que é NFC (Near Field Communication)?*. 2012. Disponível em <http://www.infowester.com/nfc.php>. Acesso em: 06 out. 2015.

ALECRIM, Emerson. *Introdução à Biometria*. 2005. Disponível em: <http://www.infowester.com/biometria.php>. Acesso em: 01 mar. 2015.

ALEGRE, Federico; VIPPERLA, Ravichander; EVANS, Nicholas. *Spoofing countermeasures for the protection of automatic speaker recognition systems against attacks with artificial signals*. 2012. Disponível em: <https://hal.archives-ouvertes.fr/hal-00783789/document>. Acesso em: 30 nov. 2015.

Apple. *iPhone User Guide For iOS 8.4 Software*. Disponível em: <https://manuals.info.apple.com/>. Acesso em: 13 out. 2015.

ARAÚJO, Marcos Elias Cláudio de; PASQUALI, Luiz. *Histórico dos Processos de Identificação.* Brasília: UNB, 2004. Disponível em: <http://www.institutodeidentificacao.pr.gov.br/arquivos/File/forum/historico_processos.pdf>. Acesso em: 14 ago. 2015.

Banco do Brasil <http://www.bb.com.br/>. Acesso em: 30 out. 2015.

BASTOS, José Mário Parrot; GAGNO, Vinicius; CAVALCANTI, Tatiana; MARTINS, Felipe; TORRES, Frederico. *Biometria Impressões Digitais*. 2008. Disponível em: <http://jpconsultoria.com.br/Seguranca/Biometria_ImpressoesDigitais.html>. Acesso em: 24 Ago. 2015.

Benefix Sistemas. *Certificados Digitais utilizados no Sistema NF-e Security V2*. Disponível em: <www2.ibam.org.br/webiss/download/PL009-Certificados_Digitais.pdf>. Acesso em: 22 set. 2015.

BRASIL. *Decreto nº 4.764, de 5 de Fevereiro de 1903*. Dá novo regulamento á Secretaria da Policia do Districto Federal. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1900-1909/decreto-4764-5-fevereiro-1903-506801-publicacaooriginal-1-pe.html>. Acesso em: 14 ago. 2015.

BUBECK, Uwe M.. *Multibiometric Authentication - An Overview of Recent Developments*. San Diego State University, 2003.

CardWerk Technologies <http://www.cardwerk.com/>. Acesso em: 16 set. 2015.

CASTRO, Thiago da Silva. *Identificação de Impressões Digitais Baseada na Extração de Minúcias*. 2008. Dissertação (Mestrado) - Universidade Federal de Juiz de Fora, 2008.

Consultores Biométricos <http://www.consultoresbiometricos.com.br/>. Acesso em: 17 ago. 2015.

COSTA, R.; OBELHEIRO, R.R.; FRAGA, J.S.. *Introdução à biometria*. In: VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Livro-texto dos minicursos, pp. 103-151, 2006. Disponível em: <http://www.advancedsourcecode.com/minicurso_biometria.pdf> Acesso em: 24 Ago. 2015.

Easy Solutions. *Perspectiva dos Consumidores da Latino-Americanos sobre a Fraude Eletrônica*. Disponível em: <http://www.easysol.net/pt/research-report-por>. Acessado em: 10 nov. 2015.

Equifax. *An extract from Perspective: The fraud and identity issue.* Disponível em: <http://www.equifax.com/assets/unitedkingdom/web_of_deceit.pdf>. Acessado em: 12 dez. 2015.

EVANS, Nicholas; KINNUNEN, Tomi; YAMAGISHI, Junichi; WU, Zhizheng; ALEGRE, Federico; DE LEON, Phillip. *Speaker Recognition Anti-spoofing*. In: MARCEL, Sébastien; NIXON, Mark S.; LI, Stan Z.. Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks, p. 125-146, Springer, 2014.

FEBRABAN. *Pesquisa FEBRABAN de Tecnologia Bancária 2014*. Disponível em: <http://www.febraban.org.br/Febraban.asp>. Acesso em: 07 nov. 2015.

FERNANDES, Daniel. *Biometria - Reconhecimento Facial*. 2011. Disponível em: <http://informaticabiometria.blogspot.com.br> Acesso em: 23 Ago. 2015.

FRANCISCO, Hélder; COSTA, Marco. *NFC: Near Field Communication - Pagamentos móveis por proximidade*. 2012. Faculdade de Ciências da Economia e da Empresa, 2012.

Fujitsu. *PalmSecure - A new level of Biometric Technology Solutions*. Disponível em <http://www.fujitsu.com/pt/Images/Palm_Secure_tcm72-630557.pdf>. Acesso em: 26 ago. 2015.

GALBALLY, Javier; MARCEL, Sébastien; FIERREZ, Julian. *Biometric Antispoofing Methods: A Survey in Face Recognition*. 2014. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6990726>. Acesso em: 23 nov. 2015.

GASPAR, Miguel Alexandre de Campos. *Sintetização de Imagens de Íris Com Ruído*. 2009. Tese (Mestrado) - Universidade da Beira Interior. 2009.
Grand Rapids Historical Commission <http://www.historygrandrapids.org/>. Acesso em: 13 ago. 2015.

GIGYA. *The 2015 State of Consumer Privacy & Personalization*. Disponível em: <http://www.gigya.com/resource/whitepaper/the-2015-state-of-consumer-privacy-personalization/>. Acessado em: 12 dez. 2015.

GTA - Grupo de Teleinformática e Automação <http://www.gta.ufrj.br/>. Acesso em 29 ago. 2015.

HANDYMAN.HU. *A geometria da mão e impressão digital*. Disponível em: <http://handyman.hu/tanulmanyok/kezgeometria-es-ujjlenyomat-azonositas-osszehasonlitasa/>. Acesso em: 08 nov. 2015.

HAUTAMÄKI, Rosa González; KINNUNEN, Tomi; HAUTAMÄKI, Ville; LAUKKANEN, Anne-Maria. *Automatic versus Human Speaker Verification: The Case of Voice Mimicry*. 2015. Disponível em: <http://cs.joensuu.fi/pages/tkinnu/webpage/pdf/imitation_machine_vs_human_SPCOM2015.pdf>. Acesso em: 30 nov. 2015.

IDGNOW. *Anatomia dos ataques em aplicativos para mobile banking*. Disponível em: <http://idgnow.com.br/blog/mente-hacker/2014/07/28/anatomia-dos-ataques-em-aplicativos-para-mobile-banking/>. Acesso em: 16 nov. 2015.

JAIN, Anil; NANDAKUMARA, Karthik; ROSS, Arun. *Score normalization in multimodal biometric systems*. Pattern Recognition Letters, Volume 38, Issue 12, p. 2270-2285, dez. 2005. Disponível em: <http://www.cse.msu.edu/~rossarun/pubs/RossScoreNormalization_PR05.pdf>. Acesso em: 22 nov. 2015.

KAMAROSKI, Abner Kloss; BARDELLI, Luiz Antonio. *Protótipo de sistema de catracas biométricas para estádio de futebol*. 2013. Monografia de Graduação do Curso de Engenharia Eletrônica. Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

Kaspersky Lab. *Kaspersky Lab Survey: 93% of Financial Services Organizations Experienced Cyberthreats in the Past Year*. Disponível em: <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-survey-93-financial-services-organizations-experi>. Acessado em: 11 dez. 2015.

LAU, Yee Wah; WAGNER, M.; TRAN, D.. *Vulnerability of speaker verification to voice mimicking*. In: Proceedings of 2004 international symposium on Intelligent multimedia video and speech processing, p. 145-148, 2004.

LEÒNCIO, Henrique Cezar Martins. *O Uso de Certificados Digitais ICP Brasil, Padrão A3, Como Tecnologia de Acesso a Conta-Cottente em Canal de Auto-Atendimento Internet*. 2006. Monografia de Graduação do Curso de Engenharia da Computação. Centro Universitário de Brasília, 2006.

LOURENÇO, Gonçalo Filipe da Fonseca. *Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída*. 2009. Dissertação (Mestrado) - Instituto Superior Técnico da Universidade de Lisboa. 2009.

MATSUMOTO, Tsutomu; MATSUMOTO, Hiroyuki; YAMADA, Koji; HOSHINO, Satoshi. *Impact of Artificial Gummy Fingers on Fingerprint Systems*. 2002. Disponível em: <https://cryptome.org/gummy.htm>. Acesso em: 28 nov. 2015.

MESSIAS, Andre Luis dos Santos. *Biometria no Auto Atendimento Bancário*. Monografia de Graduação do Curso de Gestão de Sistemas da Informação. Faculdade Impacta De Tecnologia, 2007.

MODI, Shimon. *Biometrics in Identity Management: Concepts to Applications*. Artech House, 2011.

MÜLLER, Eduardo Maikel. *Estudo e Implementação de Autenticação no Acesso para o Portal do HUSM*. 2007. Monografia de Graduação do Curso de Ciência da Computação. Universidade Federal de Santa Maria, 2007.

NAKAMOTO, Rafael Ghezzi. *Estudo de Viabilidade do Reconhecimento da Íris por meio de Dispositivos Móveis*. 2012. Monografia de Graduação do Curso de Sistemas de Informação. Centro Universitário Eurípides de Marília, 2012.

NANDAKUMAR, Karthik. *Multibiometric Systems: Fusion Strategies and Template Security*. 2008. Dissertação (Doutorado em Filosofia) - Michigan State University, 2008.

NEWTON, Elaine. *NIST - Overview of the ISO/IEC 30107 Project: Anti-spoofing and Liveness Detection Techniques*. 2012. Disponível em: <http://biometrics.nist.gov/cs_links/ibpc2012/presentations/Day2/228_Newton.pdf>. Acesso em: 26 nov. 2015.

NUANCE. *Automatic Speech Recognition*. Disponível em: <http://www.nuance.com/for-business/automatic-speech-recognition/index.htm>. Acessado em: 11 dez. 2015.

Open AuTHentication. *HOTP: An HMAC-Based One-Time Password Algorithm*. Disponível em: <http://openauthentication.org/>. Acesso em: 19 set. 2015.

OpenSignal. *The State of LTE*. Disponível em: <http://pt.opensignal.com/reports/2015/02/state-of-lte-q1-2015/>. Acesso em: 07 out. 2015.

PEREIRA, Luis Filipe Alves. *Detecção de impressões digitais falsas usando informações extraídas da rugosidade da pele*. 2013. Dissertação (Mestrado) - Universidade Federal de Pernambuco, 2013.

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

RAHAL, S.M.; ABOALSAMAH, H.A.; MUTEB, K.N.. *Multimodal Biometric Authentication System – MBAS*. In: Information and Communication Technologies, ICTTA 06. 2nd , vol.1, p.1026-1030, 2006.

SAMIR, Akrouf, et al. *A Multi-Modal Recognition System Using Face and Speech*. International Journal of Computer Science Issues, 2011, 8 (3), pp.1694-0814.

Samsung. *User Manual SM-G900F*. Disponível em: <http://www.samsung.com/>. Acesso em 13/10/2015.

SILVA, Jonas Guedes Borges. *Aplicação da Análise de Componentes Principais (PCA) no Diagnóstico de Defeitos em Rolamentos através da Assinatura Elétrica de Motores de Indução*. 2008. Dissertação (Mestrado) - Universidade Federal de Itajubá, 2008.

SILVA, Luis Gustavo Cordeiro, et al. *Certificação Digital - Conceitos e Aplicações*. Ciência Moderna, 2008.

Smartcard News. *Smart Card Tutorial*. Disponível em: <http://www.smartcard.co.uk/tutorials/sct-itsc.pdf>. Acesso em: 16 mai. 2015.

Sonovation. *Touch Sensor Under Glass Technology*. Disponível em: <http://www.sonavation.com/touch-under-glass/>. Acesso em: 11 dez. 2015.

SOUZA, Jones Mendonça. *Métodos para Reconhecimento de Íris em Ambiente não Cooperativo*. 2012. Dissertação (Mestrado) - Universidade Federal de São Carlos, 2012.

Statista <http://www.statista.com/>. Acesso em: 27 set. 2015.

TANENBAUM, A. S. *Redes de Computadores*. Rio de Janeiro. Campus. 4ª edição. 2003.

Tecnologia Radiológica. *O que é radiologia digital?*. Disponível em: <http://www.tecnologiaradiologica.com/digital.htm>. Acesso em: 23 Ago. 2015.
Tranjan Hospital de Olhos <http://tranjan.com.br/problemas-de-visao/anatomia-do-olho/>. Acesso em: 27 ago. 2015.

VIGLIAZZI, Douglas. *Biometria: Medidas de Segurança* – 2ª Edição. Florianópolis: Visual Books, 2006.

ZHI-FENG, Wang; GANG, Wei; HE, Qian-Hua. *Channel pattern noise based playback attack detection algorithm for speaker recognition*. In: Machine Learning and Cybernetics (ICMLC), 2011 International Conference on , vol.4, p.1708-1713, Guilin, 2011.

APÊNDICE – PESQUISA DE ACEITAÇÃO

Pesquisa de aceitação do uso da autenticação biométrica multimodal em *Mobile Banking*.

1- Qual a sua faixa etária?

Abaixo de 20 anos
20 a 30 anos
30 a 40 anos
Acima de 40 anos

2- Sexo:

Masculino
Feminino

3- Você já utilizou algum dos seguintes métodos de autenticação biométrica?

Impressão digital
Reconhecimento de voz
Reconhecimento facial
Reconhecimento de íris
Padrão de veias da mão
Nunca utilizei

4- Você já teve dificuldade em utilizar algum sistema de reconhecimento biométrico? Em caso afirmativo, qual?

Impressão digital
Reconhecimento de voz
Reconhecimento facial
Reconhecimento de íris
Padrão de veias da mão
Nunca tive dificuldade

5- Você realiza pagamentos/transferências através do *Mobile Banking*?

Sim

Não

Não acha seguro

6- Seu *smartphone* possui leitor de impressão digital?

Sim

Não

Não sabe

7- Você utiliza o leitor de impressões digitais para validar compras ou acessar sua conta bancária?

Sim

Não

8- Supondo que seu *smartphone* possua leitor de impressão digital, câmera frontal e microfone. Com o objetivo de elevar o nível de segurança no processo de autenticação, você gostaria de ser autenticado por sua impressão digital, face e voz ao invés da atual senha de acesso ao Banco?

Sim

Não

9- Pensando na fraude eletrônica em *Mobile Banking*, quem você acha que tem a maior responsabilidade pela segurança?

Usuário

Bancos

Governo

Fabricantes de *smartphones/tablets*

10- Você considera possível reduzir o número de fraudes eletrônicas adotando a biometria como forma de autenticação?

Sim

Não