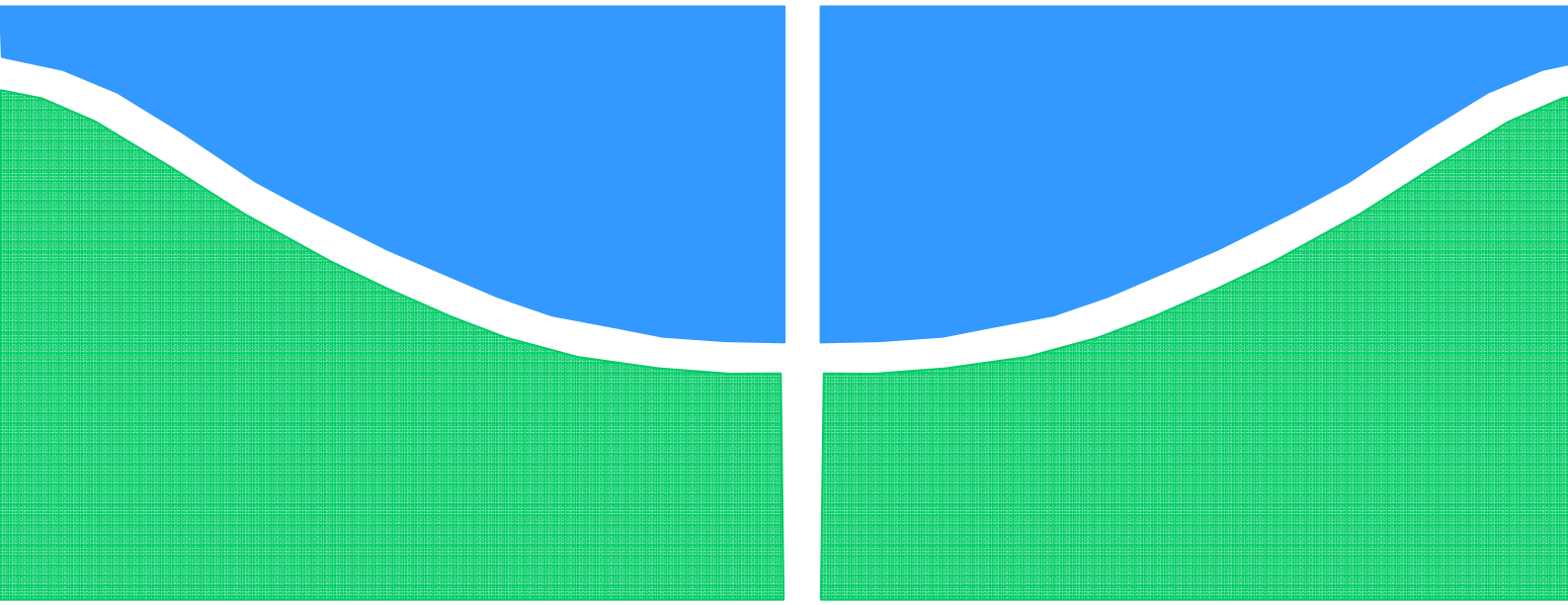


Universidade de Brasília - UnB
Faculdade de Tecnologia - FT
Curso de Engenharia de Redes de Comunicação

Modelo de Classificação de Técnicas Biométricas na Individualização de Pessoas

Autora: Andressa de Andrade Gonçalves
Orientador: Dr. Flávio Elias Gomes de Deus

Brasília, DF
2014

TRABALHO DE GRADUAÇÃO

MODELO DE CLASSIFICAÇÃO DE TÉCNICAS BIOMÉTRICAS NA INDIVIDUALIZAÇÃO DE PESSOAS

Monografia submetida ao curso de graduação em Engenharia de Redes de Comunicação da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Redes de Comunicação.

Orientador: Dr. Flávio Elias Gomes de Deus

Brasília, DF
2014

Gonçalves, Andressa de A.
Modelo de Classificação de Técnicas Biométricas na Individualização de Pessoas / Andressa de Andrade Gonçalves. Brasília: UnB, 2014. 109 p.

Monografia (Graduação) – Universidade de Brasília Faculdade de Tecnologia, Brasília, 2014. Orientação: Flávio Elias Gomes de Deus.

1. Biometria 2. Comparativo 3. Formas de Reconhecimento 4. Multibiometria 5. Custo-Benefício
I. Universidade de Brasília. Faculdade de Tecnologia. Departamento de Elétrica. II. t.

REGULAMENTO E NORMA PARA REDAÇÃO DE RELATÓRIOS DE PROJETOS DE GRADUAÇÃO FACULDADE DE TECNOLOGIA - FT

Andressa Gonçalves

Monografia submetida como requisito parcial para obtenção do Título de Bacharel em Engenharia de Redes de Comunicação da Faculdade de Tecnologia - FT, da Universidade de Brasília, em (data da aprovação 09/07/14) apresentada e aprovada pela banca examinadora abaixo assinada:

Prof. Doutor : Flávio Elias Gomes de Deus, UnB/ FT
Orientador

Pesquisador Associado: Fábio Mesquita Buiati, UnB/ FT
Membro Convidado

Prof. MSc Engenharia de Redes: Valério Aymoré Martins, UnB/ FT
Membro Convidado

Brasília, DF
2014

Esse trabalho é dedicado à minha família, Maria Aparecida, Pedro Paulo, Larissa e Cindy, por estarem sempre comigo.

AGRADECIMENTOS

Agradeço a Deus por ter ouvido minhas preces e apelos, pedindo coragem e determinação ao longo desses 5 anos de curso. Mesmo eu tendo me afastado da Igreja, Ele nunca se afastou de mim.

Obrigada aos meus pais, Maria Aparecida e Pedro Paulo, pela minha criação e incentivo constante à minha formação acadêmica. Por estar viva e com saúde para concretizar os meus sonhos.

Á minha irmã, Larissa, pela amizade, carinho e por ser minha psicóloga em casa.

À Cindy, minha eterna filhota, pela companhia e por me acalmar em meus momentos de estresse.

Ao Carlos Alexandre Griebler, pelo companheirismo, paciência e apoio ao longo da graduação. Por ser meu professor e amigo. Agradeço também a sua família, pela amizade e auxilio.

Ao Valério Martins, pela ajuda, apoio, amizade e incentivo. Não conseguiria concretizar este trabalho sem o seu suporte.

Ao meu orientador, Flávio Elias, por aceitar desenvolver esse trabalho ao do meu último ano de graduação. Por me oferecer um tema em que pude me interessar e ampliar meus horizontes.

Ao Fábio Buiati, por ajudar na orientação, pelas reuniões e auxilio no desenvolvimento deste trabalho.

Aos meus familiares e amigos, por acreditarem no meu potencial, me incentivarem e pela energia positiva.

A todos os meus colegas que tive o prazer de conhecer ao longo dessa jornada, pelos grupos de estudo no GPDS, pelo desespero compartilhado e pela amizade.

Aos meus professores, que participaram da minha formação e evolução.

E, finalmente, obrigada à UnB, por esses 5 anos cheios de desafios, superação e crescimento profissional e pessoal.

RESUMO

A Biometria tem conquistado espaço quanto ao Reconhecimento de Indivíduos. Contudo os estudos em biometria são ainda discretos, quando se comparam às outras áreas de estudo quanto às formas de reconhecimento presentes no mercado. O objetivo é mostrar o quanto a biometria tem a oferecer, quais são seus desafios e quais benefícios seu uso proporciona. Além disso, mostra como a biometria se sobressai quando comparada aos identificadores já habituais, como senhas, cartões e chips. As biometrias também podem complementar outras formas de reconhecimento de forma construtiva, a fim de prover maior segurança contra possíveis fraudes. O aprofundamento teórico é para propiciar o aprendizado a respeito de como os sistemas biométricos funcionam, quais são as biometrias estudadas e quais são as vantagens e desvantagens delas. Assim é possível traçar uma proposta de avaliação de sistemas biométricos, para que os possíveis consumidores possam ver os custos-benefícios das tecnologias biométricas mais utilizadas e qual delas melhor se adapta às suas necessidades. O trabalho também fornece estudos do mercado, fornecendo exemplos de aplicações reais.

Palavras-chave: Biometria. Aprofundamento teórico. Proposta de avaliação.

ABSTRACT

Biometrics has become increasingly more popular as the Recognition of Individuals. However studies on biometric are still discrete when compared to other areas of study as to the forms of recognition in the market. The aim is to show how biometrics has to offer, what your challenges are and what benefits its use provides. Also, shows how biometrics excels when compared to the already standard identifiers such as passwords, cards and chips. The use of biometrics can also complement other forms of recognition in a constructive manner in order to provide greater security against possible fraud. The theoretical study is to provide learning on how biometric systems work, what are some samples studied and what are the advantages and disadvantages of them. So it is possible to draw a proposal for evaluating biometric systems, so that the prospective buyers can see the cost-benefit of biometric technologies most used and which one best suits your needs. The report also provides market research, providing examples of real applications.

Keywords: *Biometrics. Theoretical study. Proposal evaluation.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	*Authentication, Authorization and Accounting*
ABIS	*Automated Biometric Identification System*
ADN	*Ácido Desoxirribonucleico*
AFIS	*Automated Fingerprint Identification System*
ASR	*Automatic Speech Recognation*
BAT	*Biometric Automated Tooset*
CHS	*Carolinas Healthcare System*
CMOS	*Complementary Metal-Oxide-Semiconductor*
CODIS	*Combined DNA Index System*
DNA	*Deoxyribonucleic acid*
DoS	*Disk Operating System*
DTW	*Dynamic Time Warping*
EER	*Equal Error Rate*
FA	*False Accept*
FAR	*False Accept Rate*
FBI	*Federal Bureau of Investigation*
FM	*False Match*
FMR	*Rate False Match Rate*
FNM	*False Non-Mach*
FNMR	*False Nonmatch*
FR	*False Reject*
FRR	*False Reject Rate*
FTA	*Failure to Acquire Rate*
FTE	*Failure to Enroll Rate*
FTIR	*Frustrated Total Internal Reflection*

GMM	*Gaussian Mixture Models*
HD	*Normalized Hamming Distance*
HSN	*Home Shopping Network*
IAFIS	*Integrated Automated Fingerprint Identification System*
ICA	*Idenpendent Compoment Analysis*
NIR	*Near Infrared*
NIST	*Nacional Institute of Standards and Technology*
RF	*Radio Frequency*
PCA	*Principal Compoment Analysis*
PIN	*Personal Identification Number*
TI	Tecnologia da Informação
TOWL	*Terrorist on Watch List*
UID	*Unique Identity Number/* Número Único de Identificação
UIDAI	*Unique Identification Authority of India*
US – VISIT	*United States Visitor and Immigrant Status Indicator Technology*
WEB	*World Wide Web*

SUMÁRIO

1. INTRODUÇÃO

O inevitável investimento e aprimoramento na área da Tecnologia da Informação (TI) trazem consigo inúmeros benefícios para a sociedade, como a possibilidade de pessoas de diversas localidades geográficas poderem se comunicar, a comodidade de acessar e executar transações bancárias por via remota, a disponibilização de informações, a viabilização do estudo não presencial, entre outras conquistas. Porém, também cresce proporcionalmente formas de invasão, quebra de sigilo de informações confidenciais, distorção de dados, tudo para que certas pessoas consigam burlar os sistemas de segurança para benefício próprio, sem se importar nas consequências de seus atos.

Assim, com a clara a tendência de se aproximar cada vez mais o mundo virtual do real, portanto novos métodos de segurança são imprescindíveis para proteger os usuários.

Nesse sentido, a identificação de um indivíduo é um fator básico para qualquer tipo de interação, desde uma simples saudação informal até a autorização de ações que interferem na vida de milhares de pessoas. Então, nada mais do que óbvio que as pessoas possuam uma forma de identificação.

Há três formas de técnicas de identificação de indivíduos que são baseadas em:

- Algo que se sabe, como, por exemplo, senhas, PINs, frases secretas;
- Algo que se possui, como, por exemplo, chaves, *tokens*, passaportes, cartões de certificação digital;
- Algo que se é, no caso, os dados biométricos, baseados no reconhecimento de pessoas por meio de características biológicas ou comportamentais do indivíduo.

Os dois primeiros dos métodos citados acima são mais vulneráveis, pois podem ter seus objetos ou caracteres identificadores roubados, modificados ou esquecidos. Ainda, o método de posse tem ainda a possibilidade de extravio. Essas

vulnerabilidades acabam por expor deus donos a muitos riscos, financeiros ou mesmo riscos legais.

Já os métodos de reconhecimento por meio de dados biométricos não podem ser esquecidos ou trocados, assim tecnologias biométricas oferecem um método confiável de reconhecimento e, por isso, melhores técnicas de identificação por meio da biometria surgem a cada dia.

A utilização das tecnologias biométricas já é vista em diversas áreas atualmente. Existem, por exemplo, aplicações na área governamental, na de saúde e em setores financeiros que já se utilizam dessas técnicas, pois a confiabilidade e eficiência dessas tecnologias se mostram cada vez mais necessárias. Por exemplo, alguns Auto Atendimentos suportam aplicações bancárias e fazem uso da biometria para validar de forma mais segura essas transações. Mundo virtual e real está cada dia mais entrelaçado.

Porém, é preciso lembrar que o meio de reconhecimento por biometria não é perfeito, afinal mensurar singularidades humanas é complexo, pois são essas singularidades podem ser instáveis, com variações que muitas vezes não seguem uma explicação previsível. Portanto não se pode fornecer 100% de segurança ou obter uma solução confiável para todos os possíveis problemas [5].

1.1 OBJETIVO

O objetivo deste projeto é introduzir conceitos fundamentais de biometria e compará-las com demais formas de reconhecimento do individuo, a fim de observar e analisar sua relação com aspectos de segurança, viabilidade e abrangência.

A forte motivação deste trabalho está no uso recente e promissor da biometria como técnicas de identificação de indivíduos dada sua menor vulnerabilidade. Nesse sentido, há vários elementos essenciais a serem estudados, que formam o referencial teórico deste trabalho, tais como: a questão da segurança das informações capturadas e armazenadas, a transmissão do local dos dados capturados até o banco de dados do órgão que armazena tais informações, os equipamentos e as instruções necessárias para captura, as formas posteriores de uso desses dados na verificação se um indivíduo é ou não genuíno, quais serão os

custos envolvidos com as tecnologias baseadas em biometria, e qual a necessidade de adaptação dos modelos atuais tendo em vista a tecnologia vigente.

Assim, após o referencial teórico, é traçado um comparativo entre as tecnologias existentes de biometria, construindo um modelo que suporte a avaliação de formas eficientes e eficazes de identificação adaptadas para as necessidades específicas dos consumidores de serviço que necessitem da identificação de um indivíduo de forma menos vulnerável.

1.2 JUSTIFICATIVA

Biometria consiste em padrões físicos ou comportamentais que caracterizam um individuo. Para que uma característica biométrica possa ser aplicada em tecnologias de reconhecimento de seres humanos é preciso que ela possua algumas propriedades [2]:

- **Universalidade:** A característica precisa estar presente em todos os indivíduos que compõem uma população normal;
- **Singularidade:** É necessário que a característica seja relativamente única e diferenciada entre todos os indivíduos da população normal;
- **Coletável:** As amostras devem ser capturadas em tempo real sem que seja interrompido o processo ou sem que haja invasão à privacidade do usuário;
- **Permanente:** Seu tempo de validade deve ser relativamente longo quando à preservação dos padrões da característica;
- **Desempenho:** A característica quando utilizada deve apresentar precisão e consistência para julgamentos em tempo real.

Para fins práticos, as tecnologias biométricas precisam levar em conta algumas considerações complementares para prover um uso satisfatório em um cenário real, tais como:

- **Performance:** Os resultados apresentados em tempo real não devem causar qualquer constrangimento ao usuário nem ocasionar algum impacto negativo à organização que faz uso da tecnologia;

- **Aceitação:** As pessoas que farão uso da tecnologia devem se sentir confortáveis quanto à utilização rotineira da característica;

- **Evasão**: Reflete o qual fácil o sistema pode ser enganado quando se usa métodos fraudulentos [1];

- **Escalabilidade:** O sistema deve ser capaz de lidar com uma quantidade crescente de dados, sem qualquer impacto sobre o desempenho, rendimento e facilidade;

- **Acessibilidade:** O sistema deve preservar a privacidade do usuário e respeitar sua cultura.

Abordando o ponto de vista de segurança, o uso da tecnologia biométrica deve fornecer uma capacidade de detecção de vivacidade para proteger contra ataques *spoofing*. *Spoofing* é o ato de apresentar uma amostra biométrica vinda de um objeto falso modelado com os traços da característica ou um usuário não genuíno ser validado erroneamente por conta de uma falsa amostra biométrica, podendo assim inutilizar a eficácia da segurança do uma tecnologia biométrica.

A partir dos critérios gerais e complementares práticos a serem apresentados, poder-se-á observar que nem todas as tecnologias biométricas são capazes de satisfazer tudo na mesma proporção. Portanto cabe estabelecer critérios de prioridade quanto aos requisitos necessários para que se possa conseguir selecionar uma melhor tecnologia, aonde todos os critérios devem fazer parte da decisão final quanto ao uso de uma tecnologia para uma situação específica.

A Tabela 1 resume tipos de critério de seleção de uma tecnologia a partir de três perspectivas diferentes [5].

Tabela 1. Lista de prioridades em três perspectivas distintas quanto à escolha de uma Tecnologia Biométrica. Modificado de [5].

Prioridades focadas nas características essenciais das tecnologias biométricas	Prioridades focadas no aprimoramento tecnológico	Prioridades focadas no usuário
Universalidade	Detecção de objeto inanimado	Aceitação
Singularidade	Desempenho	Acessibilidade
Coletável	Acessibilidade	Facilidade
Durabilidade	Evasão	Performance
Performance	Escalabilidade	Coletável

1.3 METODOLOGIA DO TRABALHO

Esse trabalho propõe um estudo teórico acerca de vários assuntos relevantes que compõem a biometria. É de interesse este trabalho dar a conhecer as demais técnicas de reconhecimento já consolidadas, saber sobre seu uso e quais vulnerabilidades podem ser supridas quando se substitui por um reconhecimento por dados biométricos. A partir desta busca de conhecimento à respeito e assuntos já explorados na sociedade biométrica, é viável se chegar a reflexões práticas, como a modelagem de uma proposta de avaliação das tecnologias biométricas já em uso, para se obter um *ranking* de avaliação considerando aspectos globais essenciais.

Ao longo da discussão exposta neste trabalho, é apontado o que vem sendo estudado atualmente, os desafios e, quando possível, são expostas considerações de mercado e de valor financeiro, isto é, deve ser investido pelas organizações que aderem às tecnologias biométricas.

1.4 ORGANIZAÇÃO DO TRABALHO

Este projeto se encontra dividido em sete capítulos.

No primeiro capítulo é apresentada uma introdução do que será desenvolvido ao longo do trabalho e qual a importância de se estudar o reconhecimento do indivíduo por características biométricas. O capítulo dois explora fundamentos necessários que permeiam todo o estudo de biometria, fornecendo uma base de compreensão, pela definição dos conceitos correlatos a essa tecnologia. O capítulo três apresenta as técnicas utilizadas pelos sistemas biométricos, apontando valores objetivos que permitem a avaliação de questões como a segurança, precisão entre outros. O capítulo quatro explora cada um dos principais dados biométricos atualmente em uso e estudo, mostrando suas vantagens, desvantagens, como funcionam e seus modos de utilização. O capítulo cinco aborda o uso de dois ou mais dados biométricos, a multibiometria, e o correspondente aumento de potencial de proteção contra possíveis fraudes. O capítulo seis apresenta o resultado deste trabalho: avaliação das tecnologias biométricas, estruturada de forma a dar suporte para que as organizações que desejam utilizar esse tipo de tecnologia possam ter uma noção do que o mercado tem a oferecer e consigam identificar qual tecnologia se adapta melhor as suas prioridades. No capítulo sete se expõe algumas aplicações utilizadas no mundo, desafios e as contribuições que este trabalho fornece.

Nas referências bibliográficas constam quais foram as fontes de estudo do projeto.

2. ESTUDO BIBLIOGRÁFICO – ESTADO DA ARTE

2.1 RECONHECIMENTO DE CARACTERÍSTICAS BIOMÉTRICAS

Um número considerável de características biométricas vem sendo estudadas ao longo dos anos, e crescentes vem sendo os investimentos na área de reconhecimento por uso de técnicas biométricas.

Neste sentido, as tecnologias que envolvem a biometria no reconhecimento de indivíduos são divididas em dois grupos: tecnologias que fazem uso de traços fisiológicos ou também conhecidos como estáticos e tecnologias que fazem uso de traços comportamentais ou também conhecidos como dinâmicos.

Os traços fisiológicos se tratam de peculiaridades do individuo originadas da carga genética, normalmente tem certa durabilidade, pois permanecem intactos ou mantém mesma estrutura por um prazo de tempo considerável. Digital, face, Iris e a geometria das mãos são as principais características fisiológicas usadas no reconhecimento do indivíduo por meio da biometria.

Outras características estáticas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa [6]:

- Impressão Palmar;
- DNA;
- Formato das orelhas;
- Padrão vascular da retina;
- Odor do corpo;
- Padrão da arcada dentária;
- Padrão de calor do corpo ou de partes dele (Termograma).

Os traços comportamentais são características assumidas por influência do ambiente externo, estas características são obtidas através do aprendizado ou desenvolvidas pelo uso frequente, e assim, é suscetível à mutação ao longo do

tempo. Além disso, as características comportamentais podem ser facilmente modificadas e reproduzidas pela vontade ou estado do usuário. Neste sentido duas amostras consecutivas do mesmo indivíduo podem ser bastante diferentes. Voz e a Dinâmica da Assinatura são as principais características comportamentais usadas no reconhecimento do individuo por meio da biometria.

O processo de geração de voz pode ser categorizado tanto na parte comportamental como na parte fisiológica, pois tem influencia da estrutura anatômica da laringe e formação das pregas vocais como também sofre influência regional, cultural e de estado do usuário, como por exemplo, alguém que necessitou de uma traqueostomia. Enquanto a dinâmica de assinatura trata de comportamentos adotados na escrita, não só a caligrafia como também a pressão, ritmo, inclinação, pausa, entre outros.

Outras características dinâmicas também são utilizadas em menor grau ou estão em estágios inicias de pesquisa [6]:

- Dinâmica de digitação;
- Modo de andar;
- Movimento labial;
- Som da assinatura;
- Vídeo da assinatura.

A Tabela 2 relaciona um resumo de tecnologias biométricas existentes.

Tabela 2. Resumo descritivo das Tecnologias Biométricas. Modificado de [5].

Tecnologia de Reconhecimento	Tipo	Interação com o Usuário	Exemplos
Digital	Fisiológico	Necessária	Identificação Criminal, Registro em Rede, Computador, Banco (utilização de ATM), Acesso a Áreas Restritas, Cadastro Eleitoral, Sensor de Identificação de Digitais em Celulares
Face	Fisiológico	Não Necessária	Identificação Criminal, Registro em Rede, Computador, tecnologia de reconhecimento Facial do Facebook
Íris	Fisiológico	Não Necessária	Registro em rede, Controle de Imigração e da Fronteira
Geometria da Mão	Fisiológico	Necessária	Acesso à Área Restrita, Registro de Ponto
DNA	Fisiológico	Necessária	Aplicação da Lei
Orelha	Fisiológico	Não Necessária	Acesso a Área Restrita
Retina	Fisiológico	Não Necessária	Acesso à Área Restrita
Padrão Vascular	Fisiológico	Necessária	Acesso a Área Restrita, Registro em Rede e em Computadores, Verificação de Identidade na Área da Saúde.
Voz	Fisiológico e Comportamental	Não Necessária	Sistema de reconhecimento por Voz em Celulares
Dinâmica de Assinatura	Comportamental	Necessária	Verificação de Identidade nas transações feitas com Cartão de Crédito, Técnicas de Autenticação de Usuários em Sistemas Remotos
Digitação	Comportamental	Necessária	Complementa a Autenticação de Senhas, Sistema de Segurança aplicado a um ambiente WEB
Modo de Andar	Comportamental	Não Necessária	Aplicações na Área de Vigilância

Embora sejam traços fisiológicos ou comportamentais, todas essas características pessoais de um indivíduo podem ser dispostas em uma linha contínua, como pode ser visto na Figura 1.

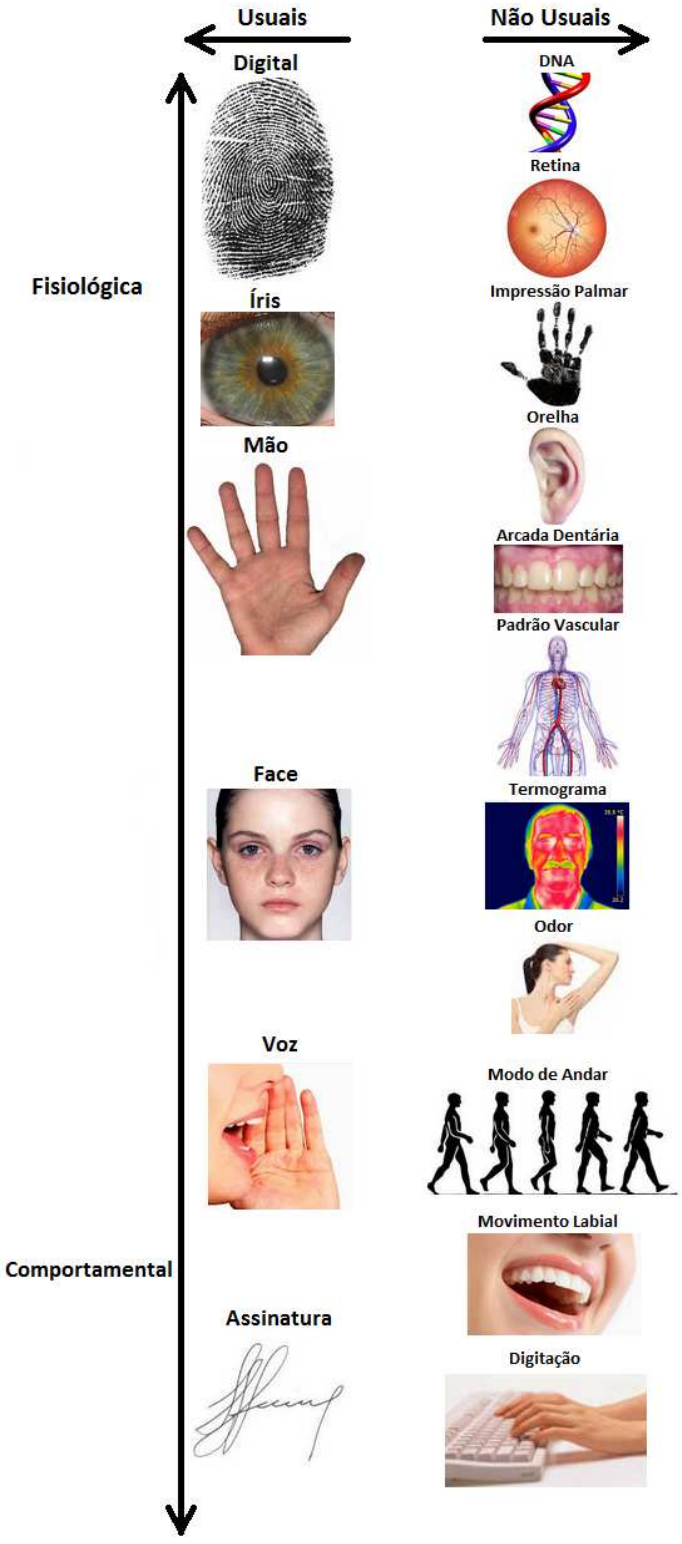


Figura 1. Linha Contínua contendo as Características Biométricas Usuais e não Usuais.

As tecnologias que fazem uso da biometria utilizam algum tipo de dispositivo de captura, neste sentido, a aquisição de amostras depende de como o usuário interage com o sensor, quando é necessária a sua interação física, ou como o usuário se encontra quando a amostra for capturada. Mesmo que uma característica seja inteiramente fisiológica, como uma digital, o processo de captura tem impacto por conta da interação entre o usuário e o dispositivo, sendo que esta interação tem certo nível de influência comportamental.

Assim, um sistema biométrico é essencialmente um mecanismo de reconhecimento de padrão que usa uma representação das características humanas como sua entrada.

Um sistema biométrico genérico pode ser visto como uma combinação funcional dos seguintes subsistemas [4]:

- Aquisição: Captura de amostras, o mais limpa (por exemplo, sem ranhuras) possível, do usuário. Normalmente a aquisição é feita por meio de um sensor que necessita de uma interação física com o usuário;

- Processamento de Sinal: Extração de particularidades que representam a singularidade de uma amostra. Este módulo de pré-processamento da amostra para o aprimoramento realiza avaliação da qualidade, e cria uma representação recursos para posterior utilização em armazenamento ou comparação;

- Armazenamento de Dados: Guarda a representação característica produzido pelo subsistema do processamento de sinal;

- Comparação: Realiza a comparação entre duas características e produz um *score* de similaridades. Um *score* de similaridades é o grau de confiança que duas amostras originais de um mesmo indivíduo têm entre si. Este subsistema é baseado em dados probabilísticos, pois duas amostras de um mesmo usuário nunca fornecem uma perfeita correspondência;

- Tomada de Decisão: Esse subsistema utiliza o *score* de similaridade gerado pelo subsistema de comparação e realiza comparações com um limiar gerado com base em decisões de sucesso e de fracasso.

A partir desses subsistemas, se devem traçar estratégias de proteção contra possíveis ataques ao sistema Biométrico. A Tabela 3 retrata alguns ataques em cada subsistema ou parte específica de um dos subsistemas e traz soluções para essas ameaças.

Tabela 3. Ataques nos diferentes subsistemas. Adaptado de [5].

Subsistema	Ameaça	Estratégia de Proteção
Aquisição	*Spoofing*/ biometria falsa	Detecção se o indivíduo está vivo
Aquisição	Instabilidade	Prover baixa resposta de granularidade
Aquisição	Inserção de sensor fraudulento	Verificar se existe identificação no Dispositivo
Aquisição	Utilização de Resíduo	Limpeza do Sensor/ Detecção se o indivíduo está vivo
Processamento de Sinal	Substituição	Verificação de Integridade/ Uso de *hash*
Processamento de Sinal	Instabilidade	Prover baixa resposta de granularidade
Processamento de Sinal	DoS	Monitoramento de desempenho do sistema
Processamento de Sinal	Controle de Qualidade	Verificação de Integridade/ Uso de *hash*
Armazenamento de Dados	Inserir *templates* não autorizados	Segurança do banco de dados
Armazenamento de Dados	Roubo de *templates* genuínos	Criptografia
Comparação	Inserção de subsistema Fraudulento	Verificação de Integridade/ Uso de *hash*
Tomada de Decisão	Inserção de subsistema Fraudulento	Verificação de Integridade/ Uso de *hash*
Transmissão	*Man-in-middle*/ Reprodução	Criptografia, assinatura digital, identificação de períodos de tempo
Processo Operacional	Cadastro Fraudado	Criação de políticas de retirada de habilitação e procedimentos
Processo Operacional	Instabilidade na verificação/ Identificação	Permissão de um número pré-definido de falhas

2.2 CADASTRO, VERIFICAÇÃO E IDENTIFICAÇÃO BIOMÉTRICA

A base de funcionamento de um sistema biométrico consiste na criação de um modelo padrão de minúcias de características biométricas específicas a fim de fornecer informações suficientes para comparar com amostras armazenadas na base de dados de um sistema, de forma à efetuar a validação de um indivíduo.

Os processos feitos pelo sistema podem ser separados em:

- Cadastro

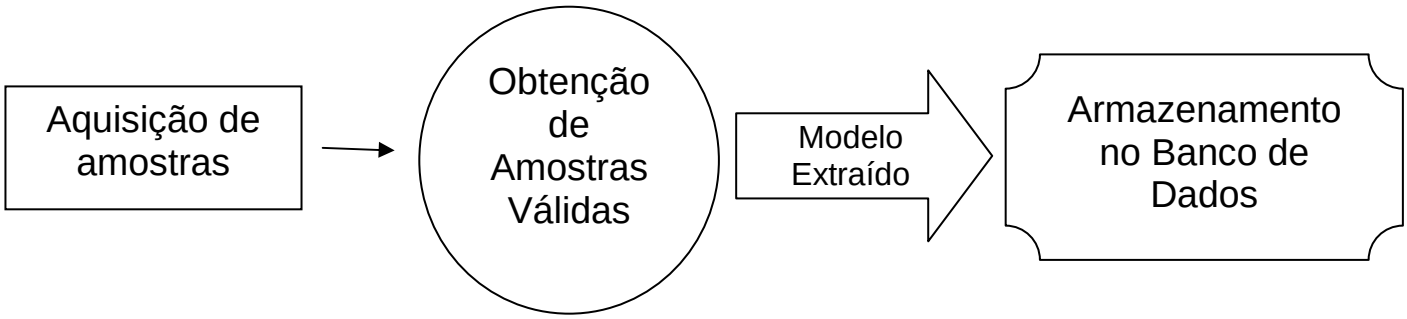


Figura 2. Processo de Cadastramento de um Usuário.

- Verificação

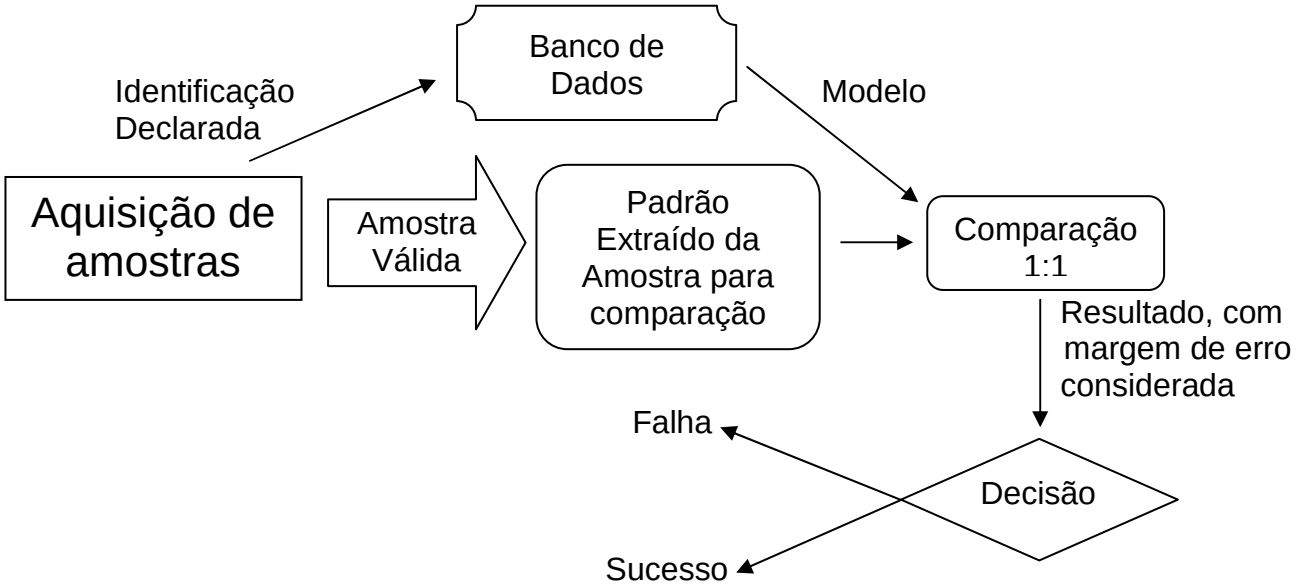


Figura 3. Processo de Verificação de um Usuário.

- Identificação

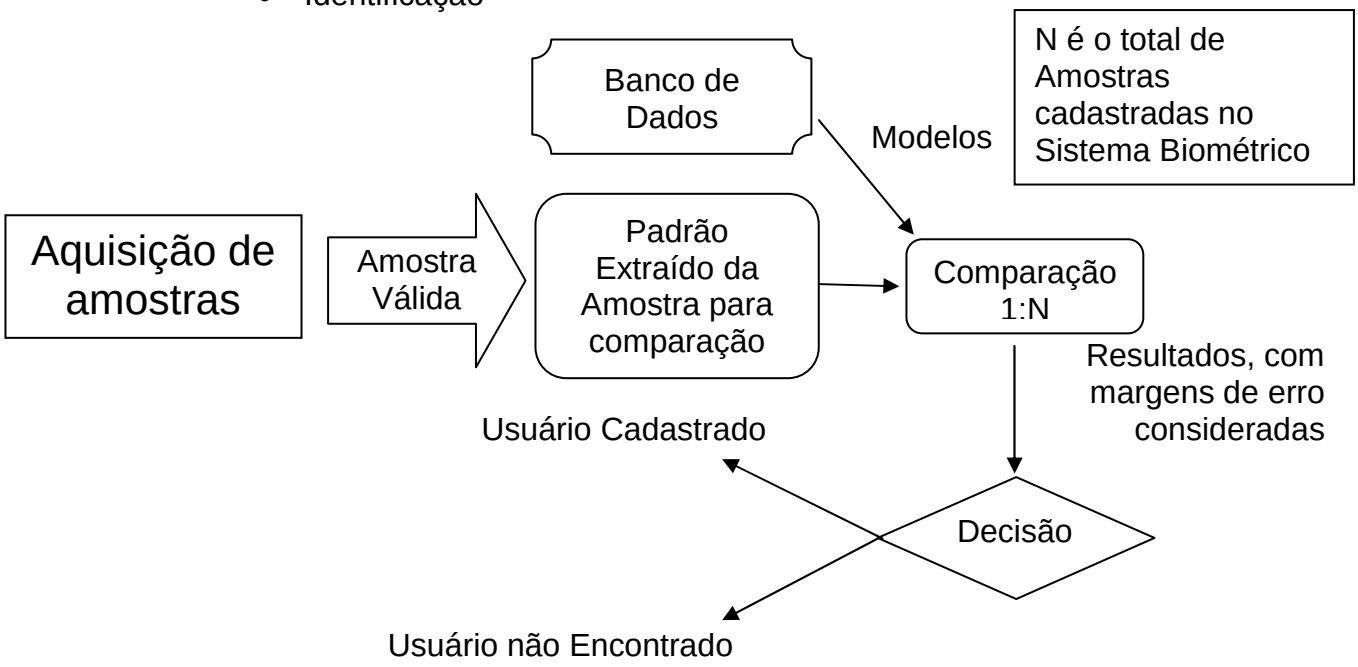


Figura 4. Processo de Identificação de um Usuário.

2.2.1 Cadastro

Nesse processo, o indivíduo fornece ao sistema biométrico amostras do dado a qual o sistema trabalha, para que a partir de amostras válidas (com resolução suficiente) sejam extraídas minúcias únicas da melhor das amostras para a diferenciação de se usuário dos demais, efetuando assim o registro de um modelo (*template*) gerado desse usuário no banco de dados do Sistema, juntamente com o identificador (caso esse tipo complementar de reconhecimento seja utilizado).

2.2.2 Verificação

Na Verificação se faz a validação da autenticidade do indivíduo por meio da apresentação de uma identificação feita por senha, cartão ou algo do tipo e o fornecimento de uma ou mais amostras em um sensor de captura do Sistema. O uso das outras técnicas de reconhecimento de um indivíduo é necessário no processo de verificação, pois se precisa de informação extra para ter continuidade esse processo.

Com a senha, o sistema biométrico percorre o seu banco de dados e verifica, por meio da comparação 1:1, se a característica capturada pelo dispositivo é genuína ou não.

2.2.3 Identificação

A identificação de usuário não exige uma informação adicional, o uso de outras técnicas de reconhecimento, pois é de responsabilidade do Sistema Biométrico estabelecer a identidade do usuário. Assim, com o fornecimento da amostra no dispositivo, o sistema varre todo o seu banco de dados, executando comparações de 1:N (sendo N o total de amostras registradas no banco de dados do sistema).

Em algumas aplicações, é possível que o sistema peça por uma lista de possíveis candidatos em vez de um único melhor resultado de comparação. Esse tipo lista é bem comum em sistemas que necessitam de intervenção humana, como o processo de comparação de uma digital desconhecida com uma base de dados de criminosos já catalogados. O sistema traz uma lista de possíveis candidatos para que um especialista possa fazer a perícia final [5].

2.3 BIOMETRIA X AUTENTICAÇÃO

Autenticação trata-se da verificação e/ou determinação de uma identidade de um indivíduo, possibilitando aos membros acesso aos sistemas protegidos.

Dados biométricos estão entre os fatores de autenticação, pois a maioria dos sistemas de segurança da área de Tecnologia da Informação necessita de altos níveis de segurança e eles conseguem ser alcançados por meio de vários fatores.

Genericamente, os fatores de autenticação podem ser divididos pelas três técnicas de reconhecimento já apresentadas anteriormente: O que você sabe, o você possui e o que você é.

Tabela 4. Diferentes classificações das três técnicas de Autenticação Básica. Adaptado de [3].

	Possibilidade de cópia	**Perda ou Danificação**	**Possibilidade de Roubo**	**Divulgação**	**Mudanças**
O que você sabe	Reprodução por escrita ou fala	Pode ser esquecida	Engenharia Social	Reprodução por escrita ou fala	Fácil
O que você possui	Fácil reprodução de cópia do atributo	Fácil perda ou danificação	Possível	Distribuição física	Distribuição física
O que você é	Difícil reprodução. Possui ata complexidade quando se trata de falsificações eficientes	Quase impossível	Difícil	Dependendo do atributo, pode ser fácil pra difícil	Limitada

A Autenticação Biométrica usa dados biométricos como identificador dos membros. Este processo pode ser dividido em dois passos:

- Cadastro: Aquisição de *template* do usuário por meio da analise de amostra ou amostras válidas capturadas por um dispositivo do sistema. Este *template* fica armazenado no banco de dados do sistema e serve como identificador do usuário cadastrado;

- Utilização: Quando o usuário interage com o sistema, à espera de sua autenticação. Deve-se fornecer uma amostra, a fim de criar um *template* para que ele seja comparado com o *template* armazenado. Um usuário é autenticado por meio da taxa de acerto (*match score*).

A Figura 5 ilustra os passos de cadastro e verificação ou identificação, em que estes dois últimos funcionam como o processo de autenticação de um sistema biométrico.

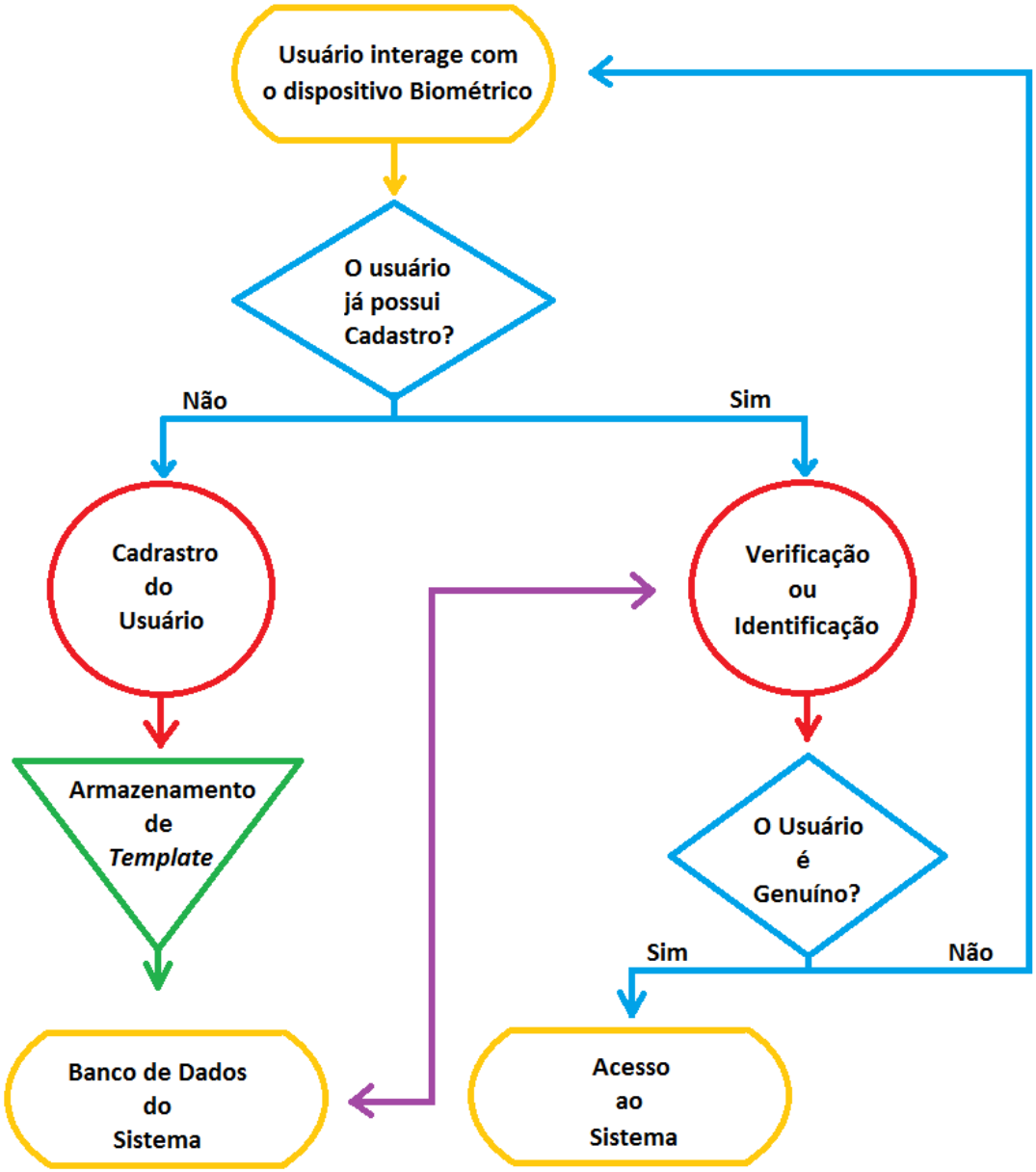


Figura 5. Fluxograma da Autenticação Biométrica.

Como se pode ver, a autenticação não é tão simples, pois ela se baseia em um *score* obtido pelas comparações entre o *template* formado pela amostra fornecida pelo usuário e o *template* armazenado no banco de dados. Este processo precisa levar em conta um limiar (quantidade de características idênticas, que varia de acordo com o sistema usado), pois nunca uma mesma mostra será 100% idêntica a outra, mesmo partindo do usuário genuíno. Por isso o sistema biométrico trabalha com a taxa de acerto (*match score*).

Ainda assim, há duas possíveis situações de falha, que serão vistas posteriormente:

- Falso positivo: Também conhecido como FA (*False Accept*), em que o sistema autentica um usuário errado;
- Falso negativo: Também conhecido como FR (*False Reject*), em que o sistema não autentica o usuário genuíno.

Os sistemas de autenticação, após o processo de verificação ou identificação validada, geralmente entram em cena os processos de autorização e auditoria.

A autenticação, a autorização e a auditoria são conhecidas como Soluções AAA (*Authentication, Authorization and Accounting*), em que estas definem a capacidade do sistema de coordenar políticas e efetuar o gerenciamento da configuração e do acesso a diversos dispositivos da rede e da segurança.

Em essência, uma solução AAA deve conter uma base de dados que tenha arquivos com os dados dos membros, seus perfis e suas configurações, em que haja a comunicação com os roteadores, servidores de acesso remoto entre outros dispositivos que fazem parte da comunicação do sistema [6].

A autorização, segundo A da Solução AAA, consiste em apontar quais áreas do sistema que o usuário genuíno tem direito ao acesso. Já a auditoria, terceiro A da Solução AAA, está relacionada ao consumo dos recursos feito pelos usuários e, principalmente, é essencial para a segurança do sistema, pois descobre quais infrações foram cometidas por cada usuário. O banco de dados gera *logs* de auditoria, que catalogam as ações ocorridas no sistema.

Estas soluções têm aplicabilidade em diversas áreas da Tecnologia da Informação [6].

3. FUNDAMENTOS DAS AVALIAÇÕES TÉCNICAS

Como já exposto, nenhum Sistema Biométrico é perfeito, afinal o reconhecimento dos usuários é baseado em estimativas estatísticas.

Nesse sentido, há várias formas de se avaliar o desempenho de um sistema biométrico, como taxas de erro de incompatibilidade (*Mismatch Error Rates*), taxas de transferência, confiabilidade, consistência, custo, população alvo entre outros [5].

Para se obter resultados viáveis para se avaliar com certo grau de exatidão um sistema biométrico, foram desenvolvidos métodos aceitos pela comunidade biométrica, baseados em taxas e percentagens construídas a partir dos resultados das avaliações quanto aos erros de autenticação cometidos pelo próprio sistema.

3.1 COMPORTAMENTO DE UM SISTEMA BIOMÉTRICO

Um sistema Biométrico é capaz de executar os seguintes processos de: cadastro, verificação e identificação. Cada um desses processos tem a necessidade do usuário interagir com o dispositivo de captura do sistema, para que assim seja recolhida uma ou mais amostras, isto é, apresenta-se uma amostra ou mais amostras ao sistema. Esse tipo de operação resulta no cadastro de novos membros ou no desenvolvimento de um *score* baseado na comparação entre *templates* que é conhecido como tentativa. A Transação seria o uso da tentativa para fins de cadastro, verificação ou identificação do usuário.

3.2 TIPOS DE ERROS EM SISTEMAS BIOMÉTRICOS

A avaliação do desempenho de um sistema biométrico tem forte relação com os tipos de erros gerados em um ou mais subsistemas que compõem qualquer sistema biométrico. Os subsistemas são: aquisição, processamento de sinal, armazenamento de dados, comparação e tomada de decisão.

3.2.1 Erro na Aquisição

Seria quando o subsistema de aquisição é incapaz de obter uma amostra com resolução suficiente para que o sistema possa extrair características essenciais do dado biométrico para a identificação do usuário ou quando o erro vem do próprio processo de extração, subsistema de processamento de sinal, das características da amostra.

Alguns fatores que influenciam esse tipo de erro são:

- Habilidade do usuário quanto ao uso do dispositivo de captura;
- Orientação quanto ao correto uso do dispositivo de captura;
- Estado de conservação do dispositivo de captura;
- Estado da amostra capturada;
- Estado emocional do usuário;
- Estado físico do dado biométrico;
- Condições do ambiente;
- Limite de qualidade da amostra;
- Tempo necessário para a captura da amostra;
- Quantidade de ruído.

3.2.2 Erro na Comparação

O subsistema de comparação serve para comparar duas amostras, a fim de verificar o grau de similaridade das características extraídas da amostra fornecida pelo usuário e a amostra armazenada no banco de dados. A partir disso gera-se um *score* que representa as similaridades entre os dados biométricos. Este *score* é então comparado a um limiar para assim poder se tomar a decisão de autenticação.

Logo, há dois possíveis erros nesse tipo de operação:

- Validar erroneamente um falso usuário
- Invalidar um usuário genuíno

Os erros de comparação podem ser gerados em diversos cenários, alguns inclusive podem vir junto com erros cometidos na aquisição [5].

3.3 FORMAS DE AVALIAÇÃO DO DESEMPENHO

Como foi exposta anteriormente, a avaliação de sistemas biométricos é baseada em estimativas estatísticas e percentagens, pois qualquer sistema biométrico comete erros e as taxas desses erros não podem ser estabelecidas teoricamente, por meio de um cálculo ou fórmula padrão.

Existem dois tipos de erros que podem ser obtidos da comparação (URL 1) :

- *False Match* (FM): Os exemplares comparados são similares no cenário virtual, porém no cenário real as amostras pertencem a pessoas diferentes. A frequência que esse tipo de erro ocorre é denominada *False Match Rate* (FMR).
- *False Non-Mach* (FNM): As Os exemplares comparados são diferentes no cenário virtual, no entanto, no cenário real, pertencem à mesma pessoa. A frequência que esse tipo de erro ocorre é *denominada False Non-Match Rate* (FNMR).

Na prática, em sistemas biométricos, trabalha-se com as seguintes terminologias:

- *False Accept* (FA): A identidade legitimada na realidade é falsa. A frequência de ocorrências desses tipos de erros é denominada False Accept Rate (FAR).
- *False Reject* (FR): A identidade alegada é tida como falsa, no entanto ela é legítima. A frequência de ocorrências desses tipos de erros é chamada de *False Reject Rate* (FRR).

3.3.1 *Failure to Enroll Rate* (FTE)

Esta taxa está relacionada a falha no cadastramento de novos usuários, em que o processo de cadastro não cumpre com os requisitos exigidos pelo sistema. O erro pode ser introduzido por qualquer tipo de adversidade citado em 3.2.1.

A probabilidade FTE(n) de não se obter sucesso no cadastro de um dado usuário (n) é:

$$FTE(n) = \frac{Número\ de\ tentativas\ de\ cadastro\ sem\ sucesso\ do\ usuário\ n}{Número\ total\ de\ tentativas\ de\ cadastro\ do\ usuário\ n}$$

O FTE geral para N participantes é obtido pela seguinte média:

$$FTE = \frac{1}{N} \times \sum_{i=1}^{N} FTE(i)$$

Quanto maior o número de participantes (N), melhor será a precisão da taxa.

3.3.2 *False Accept Rate* (FAR)

A Taxa de Falsa Aceitação consiste na frequência que um falso usuário é autorizado pelo sistema biométrico como um usuário legítimo. Isso traz inúmeros riscos à segurança das informações contidas no sistema e/ou da empresa que faz uso da tecnologia para restringir o acesso de pessoas em determinados ambientes (físicos ou virtuais). Pode causar até danos físicos ao sistema, dependendo da autonomia autorizada.

Como esta e as demais taxas, a FAR é de natureza estatística. Assim é necessário executar inúmeras tentativas de fraude para se obter resultados confiáveis.

A probabilidade de sucesso FAR (n) para um dado usuário n não-cadastrado é:

$$FAR(n) = \frac{Nº\ de\ tentativas\ de\ fraude\ com\ sucesso\ realizadas\ pelo\ usuário\ n}{Número\ total\ de\ tentativas\ de\ fraude\ do\ usuário\ n}$$

O FAR geral para N participantes é obtido pela seguinte média:

$$FAR = \frac{1}{N} \times \sum_{i=1}^{N} FAR(i)$$

Quanto maior o número de participantes (N), melhor será a precisão da taxa.

O FAR não depende exclusivamente do sistema, também depende da interação do usuário. Esta taxa é elevada caso o sistema biométrico possua imagens de baixa qualidade, pois isso gera *templates* com baixa qualidade.

3.3.3 *False Reject Rate* (FRR)

Do mesmo jeito que o FAR, a Taxa de Falsa rejeição não depende somente do sistema, também depende dos usuários. Muitos sistemas biométricos acabam invalidando erroneamente membros genuínos por conta de imagens de baixa qualidade. Quando o erro acontece por conta da qualidade da imagem e não pela falha na operação se tem uma falsa rejeição [6].

A probabilidade de rejeição FRR (n) para um dado usuário n cadastrado é:

$$FRR\ (n) = \frac{Nº\ de\ tentativas\ de\ verificação\ rejeitadas\ para\ um\ membro\ válido\ n}{Nº\ total\ de\ tentativas\ \ de\ verificação\ rejeitadas\ para\ \ um\ membro\ válido\ n}$$

O FRR geral para N participantes é obtido pela seguinte média:

$$FRR = \frac{1}{N} \times \sum_{i=1}^{N} FRR(i)$$

Quanto maior o N, número de participantes, melhor será a precisão da taxa.

3.3.4 *Equal Error Rate (*EER)

Esta taxa, também conhecida como *Crossover Error Rate*, é calculada como o ponto em que o FAR e o FRR têm valores iguais.

Um ERR baixo indica que o sistema apresenta um bom desempenho quanto à comparação de *templates*, observando uma perspectiva global de atuação do sistema.

Normalmente essa taxa é usada para se fazer comparações entre sistemas biométricos [5].

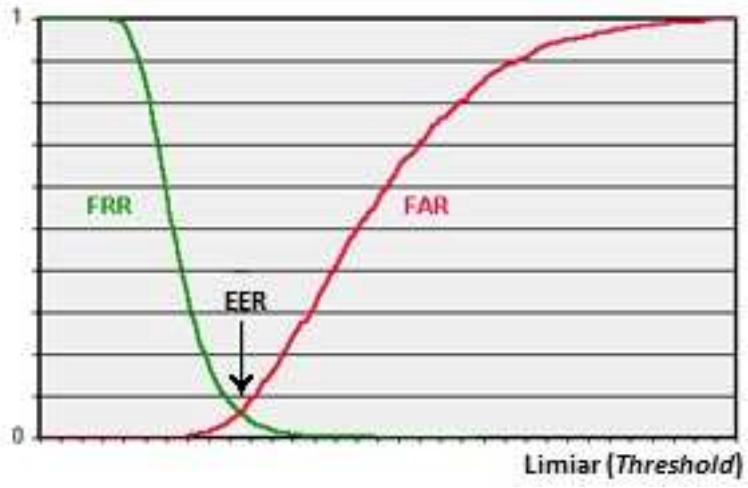


Figura 6. Diagrama FRR – FAR. Adaptado de (URL2).

3.3.5 Erros Tipo I e II

Com relação à comparação entre duas amostras, podem-se obter dois tipos de erro:

- Tipo I: o erro é originado da comparação de *templates* criados de duas amostras fornecidas pelo mesmo indivíduo. O *score* obtido da comparação foi insuficiente quando comparado ao limiar proposto pelo sistema para autenticar um usuário genuíno. *False Reject* (FR) ou *False Non-Match* (FNM) são erros relacionados ao Tipo I.

- Tipo II: o erro é originado da comparação de *templates* criados de amostras fornecidas por indivíduos diferentes. O *score* obtido da comparação foi suficiente quando comparado ao limiar proposto pelo sistema, assim autenticando erroneamente o usuário falso. *False Accept* (FA) ou *False Match* (FM) são erros relacionados ao Tipo II.

Na Figura 6 é possível visualizar duas Distribuições Normais, A e B, em que a Distribuição A representa a Taxa de Acerto (*Match Score*) quando o usuário é caracterizado como genuíno e a Distribuição B a Taxa de Acerto quando o usuário é caracterizado impostor. A sobreposição dessas duas curvas indica a área que representa os erros produzidos pelo sistema biométrico. A posição do limiar é quem decide qual será a proporção de erros introduzida ao sistema. Quanto mais à direita estiver o limiar, maior será a segurança para o sistema, todavia haverá uma maior rejeição de usuários genuínos. Colocando o limiar mais à esquerda significa que aumentará a conveniência do sistema, mas será maior a probabilidade de acesso de falsos usuários no sistema.

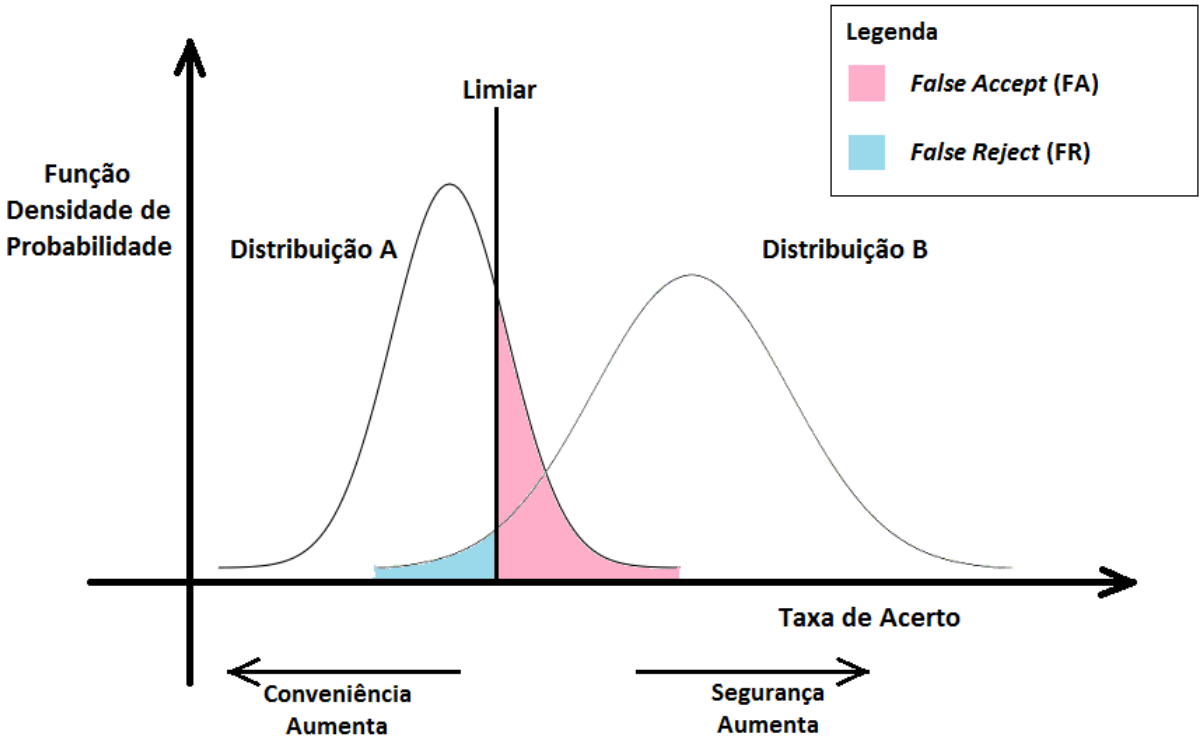


Figura 7. Diagrama das distribuições de Taxa de Acerto do Sistema Biométrico.

4. BIOMETRIAS

São apresentados os tipos de uso da Biometria como forma de reconhecimento de indivíduos.

O objetivo deste Capítulo é observar de forma mais detalhada os universos das tecnologias biométricas apontados no Capítulo 2, de forma a permitir selecionar os dados de maior interesse no resultado final deste trabalho. Para cada uma das tecnologias biométricas analisadas é discutido como são extraídas, armazenadas e utilizadas e como, a partir de cada captura, se faz os *templates* para fins de comparação/ armazenamento. Há algumas tecnologias listadas que não serão tratadas, por serem biometrias não usuais e que ainda não possuem informações suficientes para sanar as possíveis dificuldades que surgem nos cenários reais.

4.1 DIGITAL

Reconhecimento da digital é a modalidade que mais se utiliza atualmente. Se olhar de perto para a superfície de seus dedos e palma da mão, podem-se observar diversos traços, pontos e relevos, por isso esse tipo de reconhecimento também é conhecido como Dermatoglifia.

As pesquisas realizadas à respeito da digital declaram que este tipo de reconhecimento é único,e que por isso, torna-se um método extremamente eficiente de reconhecimento.

Algumas aplicações [5]:

- *Integrated Automated Fingerprint Identification System* (IAFIS): Começou em 1999 e consiste uma base de dados de histórico criminal operado pelo FBI que assiste agentes federais na identificação de terroristas e criminosos. Além das digitais, são armazenadas informações como tatuagens, peso, cicatrizes, entre outros;

- *Personal Identity Verification* (PIV): Cartões que armazenam templates de face e digital para a identificação de federais e terceirizados;

- *United States Visitor and Immigrant Status Indicator Technology* (US – VISIT): Capturam digitais e imagens da face de visitantes que entram nos Estados Unidos.

4.1.1 Anatomia

A pele da palma da mão e dedos é composta por cristas e vales, em que as cristas, conhecidas como cristas papilares, são os que aparecem pintados na figura 8, e os vales ou sulcos interpapilares não são capturados. Não há uma continuidade respeitada pelas cristas, estes podem acabar abruptamente ou se bifurcar. Algumas formas assumidas pelas cristas são listadas na Tabela 4.

O padrão aleatório formado em cada impressão digital tem sua conclusão no sétimo mês de gestação e permanece o mesmo durante toda a vida da pessoa [5]. Nem mesmo gêmeos monozigóticos possuem padrões iguais.

Mesmo que a epiderme, camada que contêm as cristas papilares, for danificada, a recuperação conserva os traços originais da pele. Isso faz com que a digital seja um ótimo candidato para o reconhecimento [5].

Figura 8. Impressão Digital (URL3).

Tabela 5. Algumas Formas assumidas pelas Cristas Papilares.

Nome	Forma
Ponto	
Ilhota ou Traço Curto	
Cortada ou Traço Longo	
Desvio	
Ponta de Linha	
Arpão	
Travessão	
Bifurcação	
Encerro	
Delta	
Núcleo	

Edward Henry, um policial indiano, foi que começou a usar impressões digitais para identificação de criminosos. Em 1900 ele publicou seu sistema de reconhecimento por meio da digital em seu livro “ *The Classification and Uses of Finger Prints*”.

Segundo o sistema proposto por Henry, mesmo depois de o reconhecimento ter sido automatizado, a base de avaliação de minúcias permanece. A Figura 9 mostra as cinco principais classes das impressões digitais usadas na Classificação de Henry.

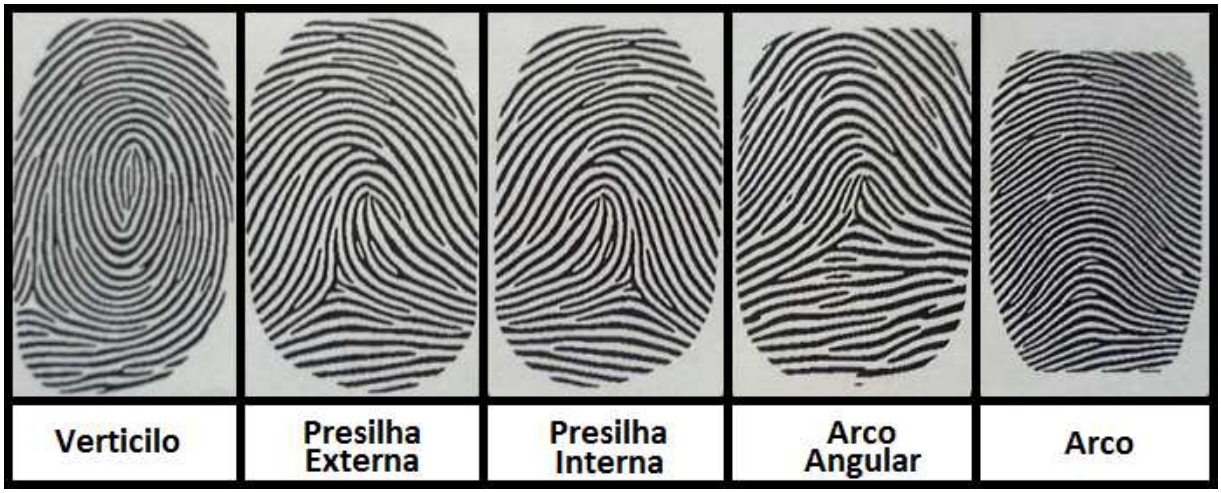


Figura 9. Classificação de Henry. Modificado de [5].

4.1.2 Aquisição da Impressão Digital

Há várias formas de aquisição de uma Digital. Todavia, serão explicitadas somente três formas, a fim de mostrar resumidamente como as tecnologias trabalham com a impressão digital e como ela é utilizada.

Basicamente, um sistema de captura da impressão digital baseado em sistema "*live scan*" é composto de [5]:

- Resolução da Captura
- Área de Captura
- Contraste de Imagem
- Nível de Profundidade de Bits
- Distorção Geométrica

4.1.2.1 Captura por Tinta

A forma mais antiga quanto à aquisição de uma impressão digital. A tinta é aplicada na pele do dedo e a impressão da digital é capturada por um substrato físico [5].

A qualidade da amostra capturada tem influência da quantidade de tinta aplicada na pele ou a pressão feita quando de comprime o dedo no substrato. Isso pode fazer com que a impressão seja clara ou escura demais para se conseguir identificar as minúcias, dificultando a extração delas e posterior comparação.

4.1.2.2 Sensores Ópticos

Estes tipos de dispositivo têm sido os vem acompanhado a mais tempo a forma de aquisição automática da digital [5].

Um dos primeiros métodos consistia em tirar fotos diretamente da Impressão Digital. Dispositivos de captura mais modernos fazem uso do *Frustrated Total Internal Reflection* (FTIR). Esse método consiste em colocar o dedo em um vidro pelo qual um feixe de luz passará, capturando os cristais papilares do dedo.

Esses dispositivos têm um custo elevado e a qualidade de captura está sujeita à condições do ambiente como sujeira e inabilidade do usuário.

4.1.2.3 Sistemas Capacitivos

Estes sistemas detectam o campo elétrico em volta da impressão digital, pois os sensores capacitivos são compostos uma matriz bidimensional de placas condutoras.

São a partir das diferenças dos campos elétricos que se geram e capturam as impressões digitais.

A principal vantagem do sensor capacitivo é que ele precisa de uma impressão digital real. Portanto dedos de gelatina ou feitos de outros materiais não são detectados pelo sensor [6].

Os sensores apresentam problemas quanto à questão de umidade dos dedos. Dedos muito úmidos tentem a escurecer a imagem capturada enquanto dedos secos tendem a obter imagens muito claras e opacas.

4.1.2.4 Outras tecnologias

- Impressões Digitais Latentes: captura resquícios do que foi deixado na superfície que a digital entrou em contato.

- Sensor RF: A captura é feita por sinais RF que medem os contornos dos cristais e vales da pele do dedo.

- Sensor Térmico: Usa o fluxo de energia térmica para capturar impressões digitais.

- Sensor Eletro – óptico: A digital é capturada por uma câmera CMOS. Esta câmera captura a luz emitida dos cristais que entram em contato com o sensor. Este feito de um polímero que com voltagem apropriada emite luz.

- Sensor de Imagem Mutiespectral: A captura é feita pelas variações de comprimentos de onda e pelas condições ópticas.

4.1.3 Aquisição da Impressão Digital

A qualidade de características biométricas de uma Impressão Digital pode ser dividida em três níveis (URL1):

- Global: Descreve a formação geral das Linhas. Normalmente se observam os deltas e o núcleo que digital possa ter. Essas formações são usadas como pontos de controle, em que as demais linhas são organizadas partir desses pontos. A orientação geral das linhas é importante para a classificação e indexação em grandes grupos.

- Local: Está relacionada com as minúcias. As formas mais utilizadas por sistemas automatizados são a ponta de linha e a bifurcação. A extração delas depende muito da qualidade da amostra capturada.

- Fina: Esta está baseada nos detalhes entre as linhas, isto é, a posição e formação geral dos poros de suor. Esse tipo de extração só é viável em imagens com alta resolução.

O processo de extração pode ser dividido em quatro etapas:

1) Recorte da Digital, em que a imagem é separada do seu fundo;

2) Levantamento de Direções, em que a imagem é analisada para a determinação da direção do fluxo dos cristais da digital;

3) Limiarização e afinamento, em que se segmenta a imagem e se efetua a análise por similaridade dos níveis de cinza, para se destacar as minúcias;

4) Extração das minúcias, em que a imagem afinada é varrida, para o levantamento das minúcias encontradas.

4.1.4 Comparação de Características

Não é possível obter amostras idênticas por diversas razões como a forma que o usuário interage com o dispositivo, cicatrizes ou transpiração. Tendo isso em mente, um sistema deve ser capaz de comparar impressões digitais e conseguir validar amostras extraídas de um mesmo indivíduo, mesmo que haja diferenças entre elas.

O campo de comparação de impressões digitais é vasto, mas todas as tecnologias podem ser agrupadas em três categorias:

- Comparação entre Minúcias: Consiste em usar as coordenadas em que as minúcias extraídas estavam localizadas, os ângulos e a forma das minúcias para efetuar a comparação. Essa é a forma mais popular de comparação no Mercado;

- Comparação pela Correlação: Os algoritmos de comparação usam a intensidade de cor dos pixels das digitais sobrepostas a fim de achar o grau de similaridades entre as características;

- Comparação por Cristas: É utilizada para fins de comparação informações como orientação, freqüência, e forma dos cristais papilares.

4.1.5 Vantagens e Desvantagens

Algumas vantagens que tem destaque das tecnologias de reconhecimento por impressão digital são:

- Nível de precisão alto, dependendo do dispositivo;
- Pela Impressão Digital ser o dado biométrico com mais tempo de estudo, já existe tradição quanto ao seu uso;
- Há grande base de dados de Digitais;
- A captura de uma Digital é fácil, de baixo custo e uma amostra ocupa pouco espaço no banco.

Já as Desvantagens de destaque são:

- Em Algumas Culturas, o uso da Digital não é aceito, por ser associado à identificação de criminosos, analfabetos ou por questões de higiene;
- A qualidade das Impressões digitais tem grande variação entro de uma população;
- Sensores mais baratos podem ser adulterados.

4.2 ÍRIS

O Reconhecimento pela Íris faz uso do padrão formado pelas fibras, rugas, estrias, sulcos, veias, fendas e coloração. Esse padrão é único para cada indivíduo.

Essa tecnologia de reconhecimento tem avançado nos últimos tempos e tem se mostrado boa para aplicações em larga escala.

Algumas aplicações [5]:

- *Privium System*: É o sistema mais antigo que faz a identificação para controle de fronteira de passageiros frequentes no aeroporto de Amsterdam;

- *Biometric Automated Tooset* (BAT): Reconhecimento pela íris feita pelo celular de indígenas, para identificar indivíduos foragidos.

4.2.1 Anatomia

A parte externa do olho, visível, é composta basicamente pela esclera, íris e pupila.

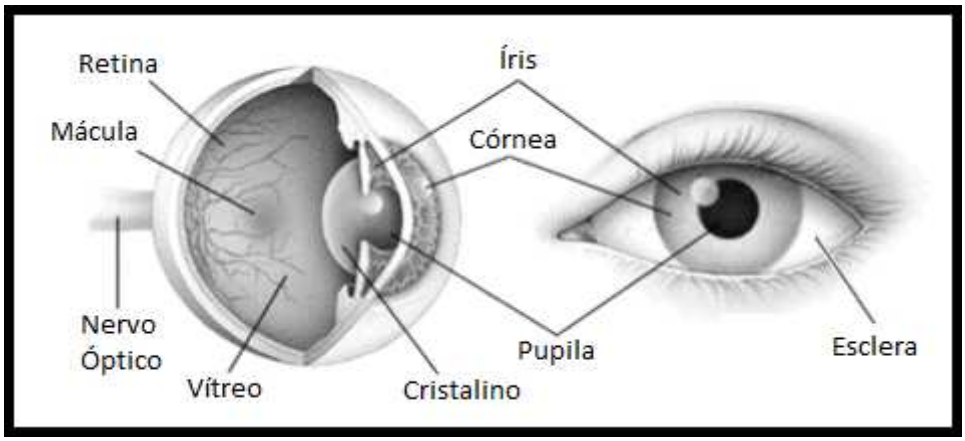


Figura 10. Anatomia do Olho. Modificada de (URL7).

Descrição da anatomia do olho:

- Esclera: parte branca do olho;
- Conjuntiva: fina membrana que reveste a esclera;
- Córnea: estrutura anesférica e transparente que, em conjunto com a esclera, forma a túnica fibrosa do olho;
- Pupila: abertura no centro da íris. Ela quem permite a passagem de luz para o interior dos olhos;
- Íris: estrutura que contém coloração que controla a abertura da pupila;
- Retina: camada de tecido nervoso que recobre internamente a parte posterior do olho. É ela quem capta a imagem e cria impulsos que são enviados ao cérebro pelo nervo óptico;

- Nervo óptico: Conecta o olho ao cérebro. É ele quem transmite os impulsos e também “decodifica” sob a forma de imagens;

- Cristalino: lente situada no interior do olho. Serve para focalizar os raios de luz sobre a retina;

- Mácula: uma pequena área sobre a retina que contém células hiper-sensíveis à luz;

- Vítreo: substância gelatinosa transparente que preenche todo o interior do olho.

Normalmente a íris não se altera, após o primeiro ano de vida. Alguns casos de alteração ocorrem devido à doença ou interferência externa. A íris é formada por várias estruturas randômicas, o que faz dela uma boa característica para reconhecimento.

4.2.2 Aquisição da Íris

A forma mais comercial de captura para os sistemas tem sido o uso de iluminação *Near Infrared* (NIR) porque:

1. A luz produzida não é perceptível ao olho humano, portanto não causa desconforto;

2. A reflexão da luz é melhor que a luz visível;

3. A melanina presente na íris absorve grande parte da luz visível, porém reflete muito da luz do NIR. A iluminação com a luz do NIR consegue isolar padrão presente na íris, mas não consegue capturar todas as particularidades da íris, pois na prática se captura os pontos mais escuros;

4. O controle de iluminação do ambiente é bem mais tranquilo quando se utiliza o NIR do que quando se utiliza a luz visível.

Os modelos comerciais tipicamente requisitam o posicionamento do usuário de 4 a 12 polegadas do sensor de captura, para assim capturar somente a íris.

A extração tem como sua primeira etapa a segmentação, para isolar a íris do restante da imagem. Para se extrair informações aplica-se a chamada demodulação. As coordenadas de cada área da íris são quantificadas com dois bits de precisão [6].

Após a segmentação, é necessária a normalização do *template*, pois o números de informações extraídas de cada íris pode variar, pois depende da qualidade da imagem.

No método proposto por Daugman, a imagem é convertida em coordenadas polares, para que cada minúcia identificada seja representada usando um parâmetro angular entre 0 e 360 e por um parâmetro radial. Assim a imagem da íris é representada em uma imagem retangular, em que o eixo horizontal tem o valor da fronteira radial e o eixo vertical tem o valor da fronteira angular, em que cada ponto é representado por coordenadas.

A imagem normalizada é dividida em uma malha 128 por 8. Cada bloco é passado por um filtro de Gabor 2D para se extrair as informações. A resposta de fase do filtro é medida. Essa medida é um número complexo e é quantizado em dois bits, que resulta num *template* consistente de 256 bytes (128 x 8 x 2 = 256). A máscara da malha correspondente também é computada para ser usada na avaliação da qualidade.

O *template* 256-byte é conhecido como *IrisCode* .

Outros métodos [6]:

- Proposta é feita por Wildes, em que a detecção da borda é baseada no gradiente de transformadas de Hough, para localizar a íris. As similaridades são comparadas segundo o método de correlação;

- O algoritmo proposto por Li Ma faz uso de um banco de filtros Gabor para capturar características locais e globais da íris, para formar um vetor de tamanho fixo. O reconhecimento é feito pela distância euclidiana entre dois vetores.

4.2.3 Comparação da Íris

Aplica-se o método proposto por Daugman para a comparação de códigos extraídos de duas íris (*IrisCodes*), chamado Distância de Hamming Normalizada (*Normalized Hamming Distance* - HD).

Para cada bit correspondente dos *IrisCodes*, suas máscaras correspondentes são comparadas. Se o resultado mostra que os bits dos *IrisCodes* têm a possibilidade ser terem sido fornecidos pelo mesmo usuário, então eles serão comparados.

O *score* é obtido depois de todas as comparações bit-a-bit, em que os bits comparados e considerados não compatíveis são contabilizados, depois do descarte dos bits que não foram considerados possíveis para se comparar.

O *score* é então comparado com o limiar estabelecido pelo sistema, para conseguir chegar a sua tomada de decisão.

4.2.4 Vantagens e Desvantagens

As principais vantagens desse sistema de reconhecimento são:

- A precisão deste tipo de tecnologia de reconhecimento é muito alta, com FAR e FRR muito baixas;
- A probabilidade de uma íris ser igual a outra é 1 em 1078, ou seja, nem mesmo gêmeos possuem o mesmo padrão em suas íris;
- A mutabilidade da íris é bem reduzida, por estar protegida pela pálpebra e não tende a variar com o envelhecimento do indivíduo;
- Permite captura sem o contato do sensor de captura com a íris diretamente, ou seja, forma não invasiva de captura de imagem;
- O tempo de análise e codificação de uma íris é relativamente curto;
- Espaço alocado para o armazenamento de informações, *IrisCodes* e suas máscaras, é relativamente pequeno.

As principais desvantagens são:

- A íris pode ser ocultada por diversos fatores, como pálpebras, cabelo e adereços;
- Dilatamento da pupila distorce a íris e se encontra atrás de uma superfície curva e refletora;
- Exige colaboração do usuário;
- Alvos em movimento tendem a tornar o processo de reconhecimento lento;
- Iluminação prejudica a captura de imagens, portanto o ambiente deve ser controlado para melhor eficácia;
- Doenças no olho prejudicam a identificação.

4.3 MÃO

A mão do ser humano possui informações suficientes em sua estrutura para ser caracterizada como um identificador para o reconhecimento de indivíduos. Muitas de suas aplicações estão voltadas para o controle de acesso a áreas restritas.

Por mais que o estudo quanto à geometria da mão ser usada como identificador, atualmente esse tipo de tecnologia é utilizado para verificação, ou seja, necessita-se de outro tipo de reconhecimento, como senhas ou chips, para adquirir o *template* de comparação.

Além do reconhecimento pela geometria, estudos têm se voltado a averiguar viabilidade quanto ao uso da impressão palmar como uma forma de reconhecimento, porém ainda são estudos bem recentes e ainda não se encontram no foco de interesse quanto à aplicabilidade no mercado.

4.3.1 Aquisição da Imagem

Existem características como o tamanho e largura dos dedos, grossura, localização de fendas, formas que fazem da mão um membro possuidor de características únicas e possíveis de distinguir os indivíduos.

A leitura dessas características em todos os sistemas usados atualmente se faz elo uso de câmera, mais comumente *scanners* compostos de câmera, leds infravermelhos e espelhos.

Os sensores usados possuem pinos, visto nas Figuras 11 e12, na superfície de uma plataforma especial que ampara a mão, eles servem para:

1. Posicionamento correto da mão do usuário;

2. Força o usuário a espalhar os dedos, o que faz a imagem da mão mais nítida para a extração das características;

3. Servem como pontos de referência na hora da extração, reduzindo a complexidade desta fase;

4. Faz com que o usuário tenha um nível de interação com o dispositivo, sendo que o usuário precisa fazer certa pressão nos pinos. Isso provê certa prevenção a *spoofing*.

Figura 11. Leitor de Geometria da Mão. Extraído de (URL8).

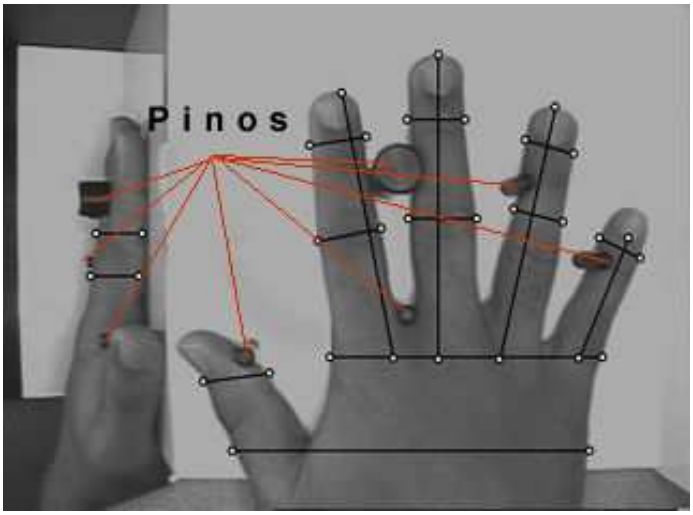


Figura 12. Imagens do perfil e parte de trás da mão. Extraído de (URL8).

A iluminação infravermelha do dispositivo de reconhecimento usa uma escala de cinca, simplificando o processo de extração das minúcias. As informações coletadas são a respeito da superfície, ignorando digitais, possíveis cicatrizes e pigmentação.

O sensor capta duas imagens da mão, uma de cima e a outra da lateral, esse método é conhecido como *scanning* ortográfico. É então capturada múltiplas perspectivas 2D da mão para inferir medidas em 3D da mão.

O scanner obtêm cerca de 96 medidas da mão, convertendo-as em um *template* de nove bytes que é então armazenado no banco de dados [6].

4.3.2 Comparação da Mão

A comparação é feita entre duas silhuetas, a da imagem fornecida, a da silhueta armazenada no banco de dados, esta selecionada por outro método de reconhecimento, e de seus respectivos *templates*. Como dito anteriormente, o reconhecimento por geometria da mão é um sistema de verificação.

Existem diferentes algoritmos de comparação, incluindo distâncias Euclidianas e Mahalanobis, distância de *Hamming,* Modelos d Mistura Gaussiana *(Gaussian Mixture Models* - GMM) e redes neurais [1]. Os melhores resultados são apresentados pelos algoritmos baseados em GMMs (URL1).

Para compressão de dados, se tem usado técnicas como *Principal Component Analysis* (PCA) e *Idependent Component Analysis* (ICA) nas características extraídas e nas silhuetas capturadas.

4.3.3 Vantagens e Desvantagens

Os pontos fortes em relação à autenticação por meio da geometria da mão são:

- A coleta é fácil e não invasiva;
- A extração de características é computacionalmente eficiente;

- Os perfis são pequenos, portanto é fácil a construção de sistemas de sistemas dedicados e isolados. Além de reduzir as necessidades de espaço no banco de dados;

- Há pouca relutância quanto ao uso da geometria da mão como identificador;

- É adequado ao uso da multibiometria, em especial em conjunto com a impressão digital e impressão palmar.

Quanto aos pontos fracos, podem-se destacar:

- Não é suficientemente distintiva para fins de identificação, sendo somente utilizada para verificação;

- Não é uma tecnologia para ser aplicada em larga escala;

- Como é necessário o contato do usuário com o dispositivo, existem preocupações quanto à higiene;

- Os equipamentos de aquisição têm um tamanho relativamente grande, pois a câmera de aquisição tem que ter certa distância para que se obtenha o efeito óptico desejado;

- Para uma aquisição eficiente, cabe ao usuário colaborar, com o correto posicionamento da mão na plataforma, orientada pelos pinos. Pode ser um pouco desconfortável.

4.4 FACE

Os estudos em cima do reconhecimento do indivíduo pela face são relativamente recentes. A capacidade de se reconhecer uma pessoa é algo que o ser humano possui e aprimora ao longo de seu crescimento. Porém é complexo desenvolver esse tipo de capacidade em um sistema automatizado de reconhecimento, visto que a mutabilidade da aparência externa de uma pessoa é algo inevitável e que deve ser considerado quando se desenvolve um sistema. Uma

aplicação bastante conhecida é quanto à personalização feita pelo Facebook, em que a rede social se utiliza do reconhecimento facial para marcar pessoas em fotos.

Existem tecnologias que fazem uso de modelos 2D e, atualmente, os modelos 3D tem ganhado espaço. A captura pode ser feita por vídeo ou câmera.

Para um desempenho satisfatório dos sistemas de reconhecimento por face, devem ser levados em consideração alguns fatores que interferem na nos resultados obtidos pelo sistema:

- Pose e Expressão: Causam muito impacto em sistemas que usam modelos 2D. Sistemas aplicados no mercado são capazes de lidar com movimentos leves, porém o desempenho decai em um cenário não controlado;

- Fatores Comportamentais: Estilo, cicatrizes, tatuagens e outras aquisições feitas pelo indivíduo que o modificam;

- Fatores Físicos: Adereços, penteados e barbas interferem na captura da face e identificação de minúcias.

- Compressão de Imagem e Interoperabilidade: A compressão é muito importante para a transmissão e armazenamento, porém o problema é determinar o quando de qualidade e desempenho podem ser cedidos para o nível de compressão utilizado pelo sistema. Outra preocupação é o uso de diferentes algoritmos de compressão, comparação e normas adotadas. Estes têm impacto na interoperabilidade, por mais que já existam formatos padronizados de *templates*;

- Fatores do Ambiente: Iluminação e local onde ocorre a captura da imagem podem prejudicar no desempenho do sistema;

- Distância: A distância entre o dispositivo de captura e o indivíduo traz impacto na resolução da imagem e no desempenho do sistema.

- Ataques *Spoofing*: O uso de fotografia no processo de aquisição.

4.4.1 Reconhecimento da Face por Modelos 2D

Os dispositivos de aquisição de imagem podem ser passivos, em que a captura decorre da luz refletida do objeto; ou ativos, em que a captura decorre da luz refletida da luz emitida pelo dispositivo.

Dispositivos passivos normalmente são mais utilizados comercialmente, podendo ser câmeras fotográficas, filmadoras entre outros. Já os dispositivos ativos tipicamente usam o espectro infravermelho.

O processo de Captura pode ser dividido em 3 partes:

1) Aquisição: Decisão binária se a imagem obtida se pode ou não detectar com sucesso a face do usuário;

2) Normalização: Processo que assegura que os pixels entre os olhos estão corretamente alinhados ao longo dos eixos x e y, em uma medida previamente determinada pelo sistema;

3) Segmentação: Separa a face do fundo da imagem, para que sejam feitas as extrações das minúcias.

A Extração e Comparação dependem da correta detecção das características e da repetição da detecção dessas mesmas características anteriormente extraídas e armazenadas em *templates*.

O Processo de Extração tem duas abordagens:

- Sistema de Características de Eigen: Baseado em características Específicas do Rosto, como nariz, olhos, boca, sobrancelhas. O sistema calcula a distância relativa entre as características detectadas. O maior problema reside no tempo, pois as pessoas estão em contínua mudança. Assim, o *template* precisa possuir prazo de validade;

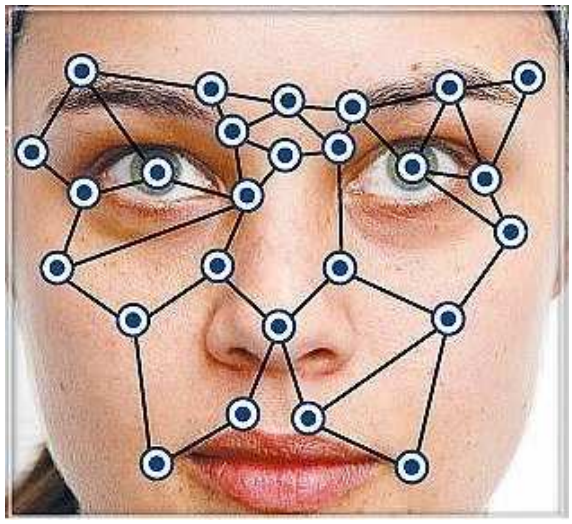


Figura 13. Medição de pontos por meio do destaque de características da Face Extraído de (URL4).

- Sistema de Faces de Eigen [6]: Cada imagem é mapeada em um sistema bidimensional. Estas imagens são convertidas em um conjunto de áreas claras e escuras. O algoritmo reconhece estes padrões e armazena em *templates*.

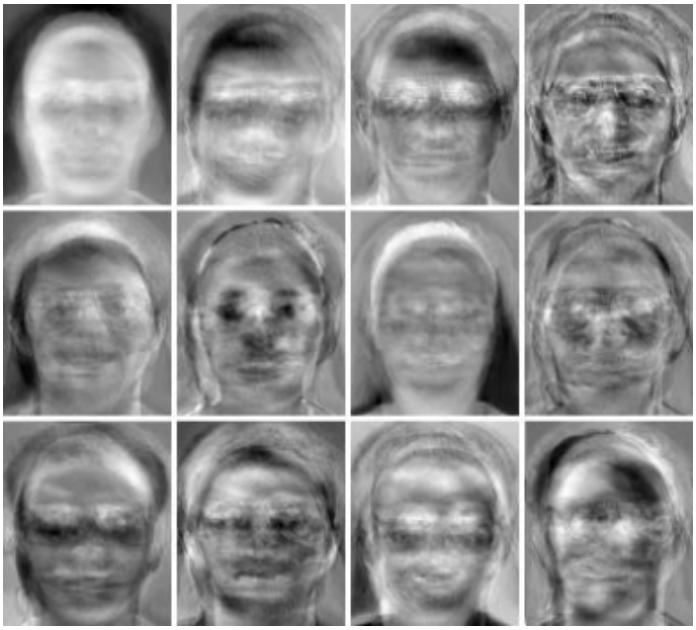


Figura 14. Imagens cridas pelo Sistema de Faces de Eigen. Extraído de [9].

4.4.2 Reconhecimento da Face por Modelos 3D

Sistemas que utilizam a representação 3D capturam toda a geometria da face, conseguindo reduzir o impacto das influências externas e expressão de caráter comportamental.

Do mesmo jeito que o modelo 2D, o modelo 3D também faz uso dos métodos passivos e ativos para a captura de imagem. A imagem construída pode ser representada por polígonos ou por um método intermediário, entre 2D e 3D, representada na Figura 16.

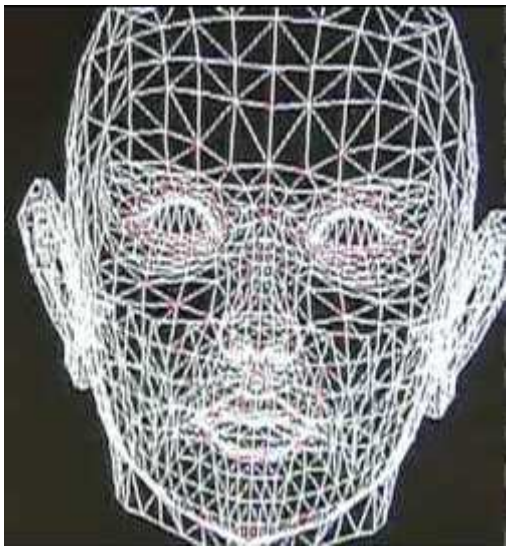


Figura 15. Reconstrução Facial 3D por meio de polígonos. Extraído de (URL5).

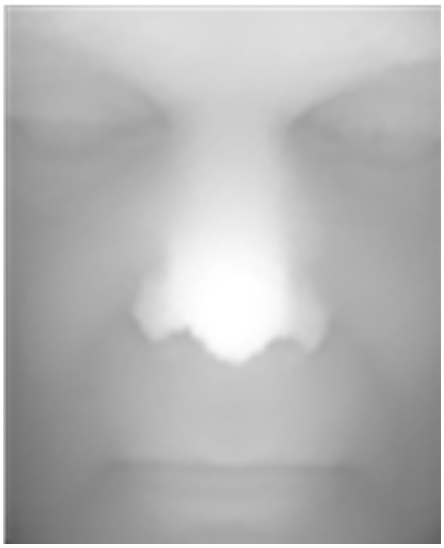


Figura 16. Reconstrução Facial Intermediária. Extraído de (URL6).

Outra forma de Reconhecimento por Faces que tem ganhado espaço é o uso de câmeras térmicas de infravermelho que capturam os vasos sanguíneos sobre a face. Isso faz com que as mudanças na aparência causem menos impacto.

4.4.3 Vantagens e Desvantagens

As principais vantagens da autenticação do usuário por meio desse tipo de reconhecimento são:

- Bastante aceitação quanto ao uso desse tipo de sistema de reconhecimento, já que as documentações também portam fotografia;

- Menor intrusividade, pois não exige contato direto e, às vezes, nem colaboração do usuário;
- Baixo custo dos equipamentos de aquisição de imagens;

Já as desvantagens desse tipo de sistema são:

- Necessidade de iluminação controlada;
- Fácil fraude, com o uso de fotografia na fase de aquisição de amostra;
- Boa para aplicações de verificação em pequena escala, todavia o uso em aplicações de identificação em larga escala se mostram ainda deficientes;
- Posicionamento do usuário pode prejudicar a captura e, consequentemente, validação do usuário;
- Alterações faciais prejudicam a validação;
- O uso de adereços prejudica o reconhecimento da face.

4.5 VOZ

O reconhecimento de um indivíduo pela sua voz se utiliza de características como tonalidade e inflexão moldadas tanto pela parte comportamental do usuário quanto pela parte biológica. Uma das mais antigas aplicações de sistema de verificação de voz é o *Home Shopping Network* (HSN), usado para redução de fraude e reconhecimento de clientes.

O interesse inicial deste sistema foi para se obter conexões telefônicas seguras [6].

4.5.1 Geração da Voz

A voz é produzida na laringe, estrutura alongada de forma irregular que conecta a traquéia a faringe. É nela onde se encontram as cordas vocais, duas pregas musculares localizadas horizontalmente que vibram ao passar do ar, emitindo assim o som.

A dimensão das cordas varia de acordo com o sexo, idade e categoria da voz (de 14 a 21 mm das mulheres e de 18 a 25 mm dos homens (URL10)). Elas nas cartilagens ligadas entre si por uma musculatura e são cobertas de uma mucosa que é estimulada por movimentos ondulatórios de baixo para cima e de frente para trás.

As cordas fazem movimentos de aproximação e afastamento, o que correspondem a altura tonal. Quanto mais alta a freqüência, mais agudo é o som.

A voz é o resultado do equilíbrio entre duas formas> a força do ar que sai dos pulmões com a forma muscular da laringe. Qualquer problema que afete esse equilíbrio tem como consequência a alteração da voz (URL11).

O som emitido pelas pregas para por um “auto-falante” natural que consiste no conjunto da faringe, boca e nariz, conhecidos como cavidades de ressonância.

O estado de humor do indivíduo influencia diretamente a voz, assim como a região onde a pessoa nasceu e sua cultura. Por isso que a voz é considerada um dado biométrico de caráter comportamental e biológico.

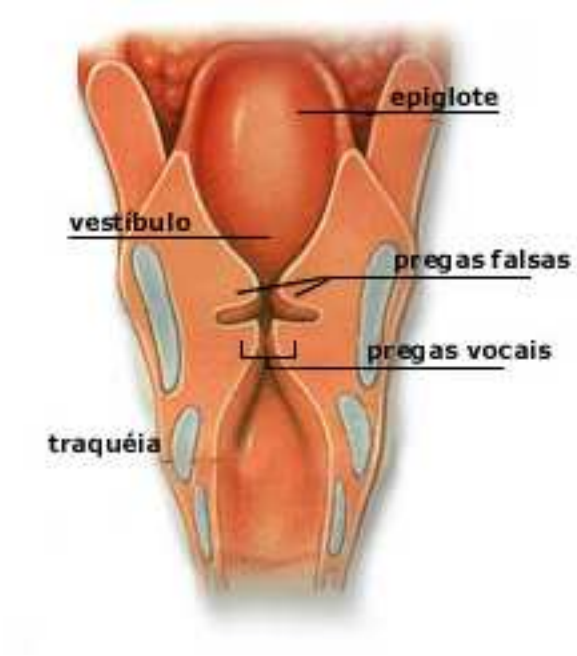


Figura 17. Localização das Cordas Vocais. Extraído de (URL12).

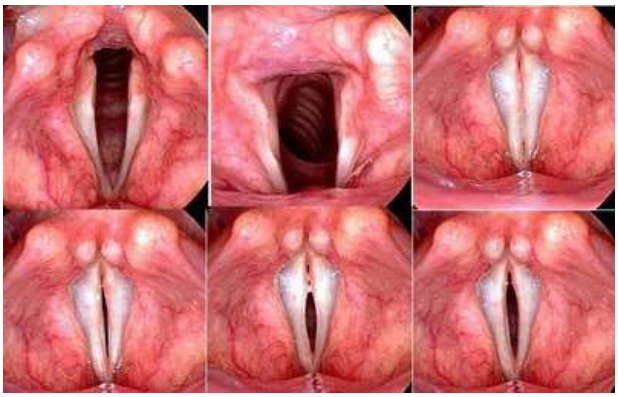


Figura 18. Cordas Vocais. Extraído de (URL 13).

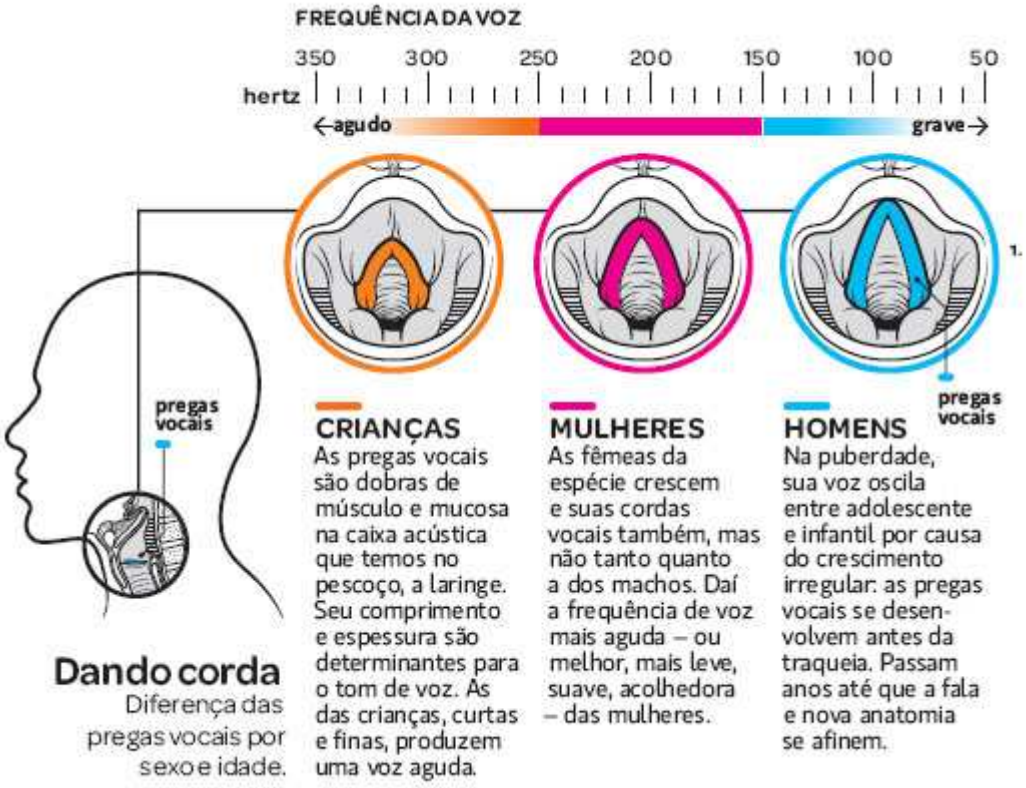


Figura 19. Diferenças das pregas vocais por sexo e idade. Extraído de (URL14).

4.5.2 Sistemas de Reconhecimento por Voz

O reconhecimento por voz pode ser aplicado tanto para a identificação quanto para a verificação de um indivíduo. Os sistemas que utilizam esse tipo de reconhecimento são categorizados pelo tipo de amostra que requisitam de seus usuários:

- Texto fixo: O usuário pronuncia palavra ou frase pré-determinada, secreta e gravada na fase de cadastro. Seria uma extensão do texto dependente;

- Dependente do texto: O usuário pronuncia palavra ou frase pré-determinada fornecida pelo sistema. O sistema deve ter consciência das amostras que devem ser obtidas então isso faz com que o sistema forneça uma proteção a ataques de repetição, por meio de gravações reproduzidas. Do mesmo jeito que o texto fixo, a fase de cadastro do usuário tende a demorar;

- Independente do texto: O usuário fala frases ou palavras que ele próprio seleciona. O sistema não tem consciência das amostras a serem obtidas. O que foi obtido usado no cadastro é diferente quando ocorre o processo de autenticação. Esse tio de sistema traz maior complexidade à comparação de duas amostras, tendo uma taxa de erro mais elevada;

- Conversacional: O usuário é questionado pelo sistema, cujas respostas são secretas, tornando esse tipo de sistema um misto de reconhecimento por algo que se sabe com a biometria da voz.

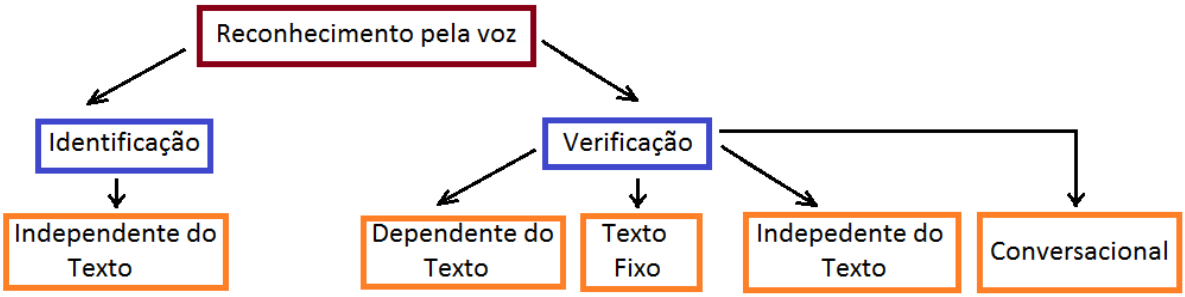


Figura 20. Tipos de sistema de Reconhecimento por Voz.

4.5.3 Extração e Comparação

Os sinais de áudio são compactados e transformados em vetores com as características extraídas do discurso.

A maioria dos sistemas que trabalha com o reconhecimento por voz faz uso da análise cepstral.

O processo de reconhecimento é feito com base na comparação de duas formas de onda. A análise cepstral permite representar as similaridades entre as duas ondas em um *matching score* por meio da distância euclidiana.

O *matching score* é calculado pela probabilidade de uma onda ter sido gerada pela mesma pessoa quem cadastrou a forma de onda armazenada no *template*.

4.5.4 Vantagens e Desvantagens

Os pontos fortes desse tipo de tecnologia de reconhecimento são:

- A voz, assim como a face, é uma biometria utilizada instintivamente como uma forma de autenticação;
- Sistemas com infraestrutura telefônica são o principal alvo desse tipo de reconhecimento, pois o protocolo de autenticação se torna amigável, passiva e não invasiva;
- O custo dos equipamentos é baixo, além de poder ser facilmente desenvolvida sobre os sistemas telefônicos;
- Permite protocolos de autenticação de segurança incremental, ou seja, o sistema pode requisitar a voz do usuário para melhor tomada de decisão;
- Em aplicações conversacionais e de Independente do texto, o processo de autenticação não precisa ser separado. Tornando o processo totalmente integrado.

Já os pontos fracos, podem ser destacados:

- Esse tipo de sistema pode ser enganado por imitação de pessoas habilidosas ou por gravações da voz do usuário genuíno. Também existem sintetizadores que podem imitar a voz;
- A tecnologia de texto fixo possibilita a criação de usuários inexistentes em sistemas de registro e autenticação remotos;
- A qualidade do áudio é suscetível ao ruído do ambiente. Também podem ser inseridas distorções na captação pelo dispositivo e pelo canal de transmissão do sinal;
- O padrão de voz é vulnerável ao estado do usuário (saúde, emoção, pressa, sono, preguiça, entre outros).

4.6 ASSINATURA

Uma assinatura manuscrita representa o método mais antigo e usado de autenticação de um indivíduo. Ela é usada com o significado de aprovação, aceitação, validação de documentos e contratos, entre outros.

Há duas formas de se analisar a assinatura como um dado biométrico: por meio de sua dinâmica de assinatura e por meio de pontos específicos da assinatura.

Analisando somente o contexto da tradicional assinatura no papel, a fraude se torna muito mais possível, pois imitar uma caligrafia é relativamente fácil. Todavia, estender o dado à sua dinâmica dificulta esse tipo de ataque, além de trazer uma prevenção a *spoofing*, porque necessita que o indivíduo seja ativo no processo de captura.

O Reconhecimento por meio da Dinâmica de Assinatura faz uso da captura de comportamentos específicos executados por um indivíduo quando ela efetua sua assinatura.

Esse tipo de reconhecimento faz uso de: pressão, aceleração, ritmo, inclinação da caneta, espaçamento entre as letras, sequência feita para a formação de letras e como são inseridos pontos e traços no ato da escrita ou se eles são postos depois do término de cada palavra.

4.6.1 Extração e Comparação da Assinatura

Os sistemas de Verificação por Assinatura podem ter seu processo de captura dividido em:

- *Off-line* ou estática: A assinatura é executada de modo convencional, por caneta ou lápis, em documentos de papel e depois a assinatura é digitalizada por meio de uma câmera ou scanner;

- *Online* ou dinâmica: A assinatura é feita em um dispositivo eletrônico. Esses equipamentos são capazes de capturar as características dinâmicas temporais da assinatura. Esse tipo de captura usa conjuntamente o reconhecimento pela dinâmica.

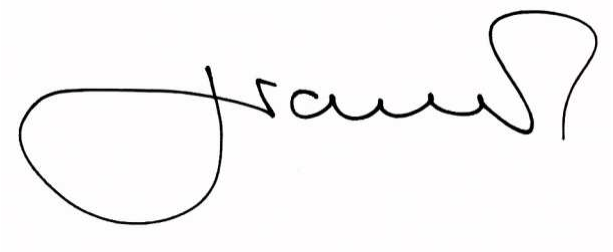


Figura 21. Assinatura adquirida por forma estática. Extraído de (URL16).

Figura 22. Assinatura adquira por forma dinâmica. Adaptado de (URL17).

Os dispositivos de captura são baseados no contato da caneta com a superfície sensível à interação. Estes podem ser divididos em três tipos: aquisição por meio da caneta, por meio da superfície e por meio de ambas.

O processo de extração, a área da dinâmica, envolve em registrar um fluxo de vetores característicos colhidos em pontos temporais equidistantes, traduzidos em variáveis. Por exemplo, A= (x,y,p,Θx,Θy) em que A é vetor penta-dimensional composto seguintes vetores:x e y correspondem a posição da caneta, p é força axial exercida na caneta, Θx e Θy registram os ângulos da caneta no plano xy [6].

Alguns produtos comerciais também incorporam à como padrão de reconhecimento os formatos geométricos da letra.

A comparação entre as assinaturas incluem medida de distâncias euclidianas entre as trajetórias das canetas, medidas de correlação regional e reconhecimento temporal-probabilístico como cadeias de Makov ocultas.

A tomada de decisão deve ser baseada em quatro possibilidades (URL1):

1. Classificadores Probabilísticos: Envolve a comparação entre as distribuições de densidade de probabilidade entre as características de um usuário e o conjunto de características gerais. A distância entre essas distribuições é feita para fixar o grau de importância das minúcias

captadas do usuário. A decisão é baseada na distância Euclidiana, determinada sobre um conjunto de características;

2. Classificadores Elásticos: Baseada no DTW (*Dynamic Time Warping*), técnica mais antiga. Ela computa as distâncias de tempo mínimais entre o vetor capturado e o vetor-modelo que está armazenado no banco de dados. O objetivo é encontrar um alinhamento temporal entre a assinatura e o modelo por meio da verificação;

3. Redes Neurais: Faz a verificação, por meio do treinamento, da dinâmica entre duas assinaturas, mas tem um desempenho fraco em relação aos demais métodos;

4. Cadeias de Markov Ocultas: Mais popular forma de classificação temporal, com aplicações nas áreas de voz, escrita e gesticulação. A vantagem vem da possibilidade de aceitar a variabilidade ao mesmo tempo em que se capturam características específicas da assinatura.

4.6.2 Vantagens e Desvantagens

Entre as vantagens quanto ao uso da tecnologia de reconhecimento por assinatura, pode-se destacar:

- A assinatura dinâmica é um conjunto de duas informações, assinatura e o ato de escrever, que podem ser colhidos por equipamentos apropriados;

- É um método bem aceito pelas pessoas;

- A dinâmica de assinatura é muito mais complicada para se falsificar, sendo que existe uma classificação quanto ao nível de sofisticação do fraudador: fraude sem nenhum esforço (*zero-effort*), aperfeiçoamento caseiro (*home-improved*), aperfeiçoamento aprimorado (*over-the-shouder*), fraude profissional (*professional*).

Quanto às desvantagens, podem-se destacar:

- A característica biométrica é bastante variável, pois há pessoas que assinam não obedecendo ao padrão cadastrado (oferecendo inconsistência). O sistema teria que permitir limiares personalizados quanto à tomada de decisão, o que colocaria em risco a segurança.

4.7 DNA

O Reconhecimento por meio do Ácido Desoxirribonucleico (ADN) é extensivamente utilizado em aplicações forenses. Esse tipo de reconhecimento já demonstrou ter alta acurácia, porém é um sistema lento, caro e invasivo, ou seja, seu uso em aplicações de rotina diária é bem complicado. Além disso, a acurácia tende a cair quanto mais os indivíduos possuem parentesco próximo.

Toda a base de dados de DNAs é utilizada para aplicação da lei como:

- CODIS – *Combined DNA Index System*;
- Base de dados da Interpol;
- ABIS – *Automated Biometric Identification System*.

O DNA ou ADN é um aglomerado de moléculas que contém o material genético do ser vivo. É esse material que determina as características físicas e é determinante para o bom funcionamento do organismo. Sua constituição é composta por quatro bases fundamentais: adenina, timina, citosina e guanina. Estas bases podem se organizar em pares em até três bilhões de combinações, sendo assim a tecnologia que faz uso do DNA para a identificação é extremamente segura.

Gêmeos Monozigóticos têm o mesmo perfil de DNA. O principal uso do DNA é quanto à verificação de paternidade.

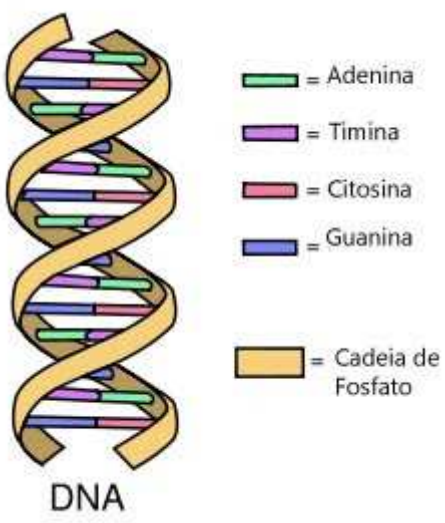


Figura 23. Estrutura do DNA. Extraído de (URL18).

O processo de aquisição e identificação é dividido em três fases:

1. Preparação: Amostras retiradas do indivíduo (sangue, saliva, dentes, ossos, cabelos) e assim segue a separação das amostras genéticas, que devem ser purificadas;

2. Sequenciação: As amostras genéticas tratadas são colocadas em um equipamento que efetuará o seqüenciamento do DNA;

3. Análise: A sequência obtida é analisada e comparada com a sequência-modelo armazenada no banco de dados, para efetuar a autenticação do individuo.

4.7.1 Vantagens e Desvantagens

A principal vantagem quanto ao uso do DNA quanto a autenticação de indivíduos é pela precisão que este dado oferece, pois a probabilidade de duas pessoas com o mesmo perfil de DNA é menor que um para cem bilhões.

Quanto às desvantagens, podem-se destacar:

- O processo de identificação ou verificação não pode ser feito em tempo real;

- Tecnologia altamente intrusiva, pois é necessário fornecer amostras físicas do usuário para se analisar o dado biométrico. Para as outras tecnologias se necessita somente de uma representação.

4.8 RETINA

A retina, como vista anteriormente, é uma camada interna no fundo do olho composta de vasos sanguineos que capta imagens e produz impulsos nervosos que são direcionados ao cérebro. É um dos sistemas biométricos mais seguros, porém a captura da imagem da retina é complicada.

O processo de captura deve manter o indivíduo parado, mantendo o olho em um ponto focal até que a câmera consiga extrair uma imagem aceitável.

Como o padrão dos vasos é único, portanto o uso desse dado biométrico se mostra bastante preciso. Sua captura é realizada por uma luz de baixa intensidade enviada por um acoplador óptico.

Esta é uma técnica praticamente inviolável, pois a interação do usuário com o dispositivo faz com que o sistema tenha detecção a ataques *spoofing*, isto é, só é possível a autenticação de um indivíduo se ele estiver vivo.

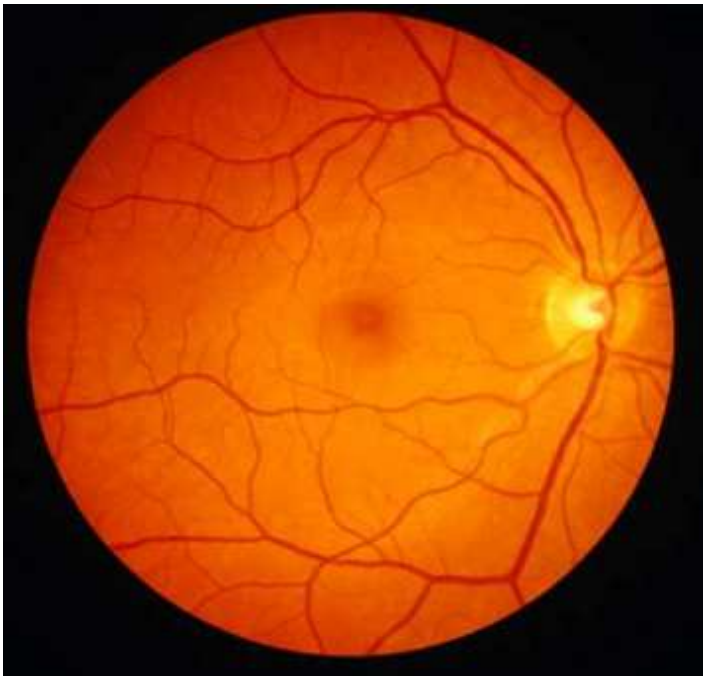


Figura 24. Retina. Extraído de (URL9).

4.8.1 Vantagens e Desvantagens

As principais vantagens que se pode destacar quanto a esse tipo de reconhecimento são:

- Unicidade extremamente alta da retina;
- Imune a ataques *spoofing*;
- Tecnologia extremamente segura no quesito de se obter cópia da retina de alguém, pois o padrão só pode ser adquirido com o consentimento do mesmo;
- Não é possível remover os olhos de uma pessoa sem que a retina seja danificada;
- O padrão da retina é estável ao longo da vida;
- Possui *template* reduzido;
- Não existem relatos de fraudes ou rejeições incorretas.

Em relação às desvantagens, podem-se destacar:

- Um número significativo de pessoas encontra dificuldades de terem sua retina capturada, por não saberem lidar com o equipamento de captura ou por possuírem problemas mais graves de saúde no olho;
- O equipamento é caro;
- Fraco desempenho em ambiente outdoor, pois a pupila se contrai, reduzindo a entrada de a luz do sensor de captura;
- Sistema intrusivo, que pode trazer desconforto do usuário uma vez que ele precisa olhar fixamente para um ponto infravermelho sem piscar por cerca de 5 segundos e se posicionar de 2 a3 centímetros do leitor.

4.9 PADRÃO VASCULAR

O padrão dos vasos sanguineos é baseado por uma estrutura de organização em rede única. Essa estrutura é formada no período embrionário e permanece relativamente constante ao longo do tempo.

Os sistemas que estão no mercado capturam o padrão formado pelas veias, pois esse tipo de tecnologia utiliza infravermelho para identificar as veias por meio da absorção de oxigênio e gás carbônico pelo sangue. Como a hemoglobina absorve melhor o gás carbônico, então ela fica mais evidente do que as artérias.

Do mesmo jeito que a retina, Iris e impressão digital, nem s gêmeos monozigóticos têm padrões iguais, nem o lado esquerdo e direito da mesma pessoa consegue uma mesma formação estrutural.

Algumas aplicações recentes têm usado o padrão vascular para permissão de acesso lógico ou físico. Esse tipo de tecnologia pode ser vista em Auto Atendimentos (ATMs no Japão) e na identificação de pacientes em hospitais (*Carolinas Healthcare System* – CHS).

Normalmente há três partes da mão utilizada para o reconhecimento: dedos, palma da mão e parte de trás da mão.

Figura 25. Reconhecimento por Padrão Vascular. Adaptado de (URL15).

4.9.1 Aquisição do Padrão

A aquisição do padrão formato das veias se faz pelo uso de iluminação por infravermelho que podem penetrar na pele humana em até três milímetros.

Há dois tipos de imagem:

- Reflexivo: a fonte de iluminação vem por baixo da superfície a ser capturada e o sensor captura a imagem refletida pela região subcutânea;

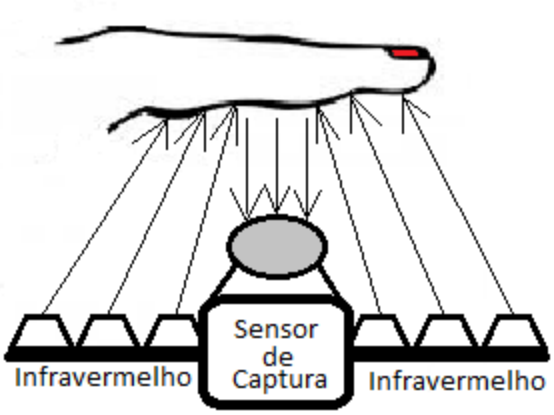


Figura 26. Captura por tipo reflexivo.

- Transmissivo: a fonte de iluminação projeta sua luz por cima do objeto a ser capturado e o sensor, do lado oposto, captura a luz que passa pelo tecido. Esse método usa partes menores e com o tecido mais fino, como os dedos.

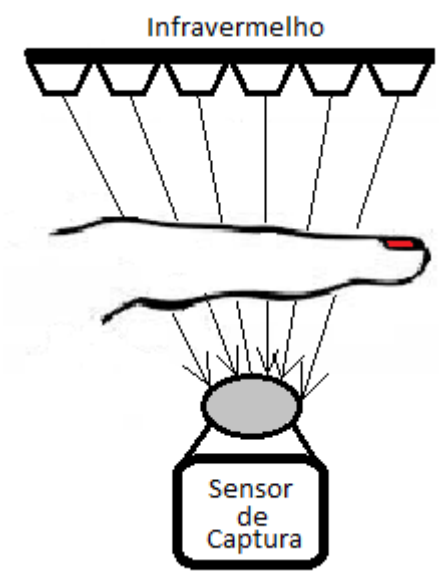


Figura 27. Captura por tipo transmissivo.

4.9.2 Extração e Comparação do Padrão

A imagem capturada, com as veias já mais escuras que o restante, deve passar por um processo para a extração do padrão. Esse processo segue as seguintes etapas:

- Extração da Região de Interesse: Esta etapa separa a região de interesse do restante;
- Redução de ruído: O tipo reflexivo de captura da imagem introduz certo ruído. Este deve ser removido para melhor qualidade da imagem;
- Segmentação: extração das bordas das veias. O modo como de extração é dependente da metodologia de comparação.

A forma como se faz a comparação de dois padrões pode ser dividido em dois grupos:

- Comparação de bordas: O nível de similaridade é calculado baseado na correlação entre o padrão das bordas de duas imagens. Os padrões são sobrepostos e assim se determina o nível de similaridade. O

padrão de veias também pode ser visto como um gráfico 2D e a partir daí se utilizam técnicas de comparação dos dois gráficos;

- Comparação de pontos: Similar ao processo de comparação da digital. Um padrão de veias é formado por fim de linha e bifurcações abruptas. Estas descontinuidades podem ser traduzidas em coordenadas no espaço 2D juntamente com o tipo de descontinuidade. A comparação é feita na comparação espacial desses pontos, com outros atributos, para gerar um *score* de similaridades (*matching score*).

4.9.3 Vantagens e Desvantagens

As principais vantagens desse tipo de tecnologia de autenticação biométrica são:

- Veias estão presentes por todo o corpo, assim a captura pode ser feita em várias áreas do corpo;
- As veias estão localizadas por baixo da pele e não podem ser afetadas por escoriações ou sujeiras na camada exterior da pele, o que também dificulta a falsificação;
- O uso desses sistemas é bastante prático, simples e a análise é rápida;
- A técnica de captura de imagem não requer interação física da parte do corpo com o dispositivo, o que preserva a higiene no processo;
- É muito pequena a probabilidade de haver dois indivíduos com o mesmo padrão vascular, nem mesmo gêmeos têm o mesmo padrão;
- O fluxo de sangue pode ser usado como uma prevenção a ataques por meio de dados biométricos falsos, pois certifica que a pessoa está viva.

Em relação às desvantagens, podem- se destacar:

- Há vários fatores que podem prejudicar a qualidade da imagem como: temperatura corporal, temperatura do ambiente, umidade, distribuição desigual de calor, entre outros;

- Custo é razoável para se comprar os equipamentos e suas dimensões são consideráveis;

- Há pessoas que têm receios infundados quando a captura de imagem, imaginando que pode ser uma experiência dolorosa.

4.10 MODO DE ANDAR

A estrutura do esqueleto, o peso e a coordenação motora de uma pessoa fornecem características únicas a forma de andar que a pessoa adquire. O reconhecimento por meio do modo de andar pode ser feito com uma relativa distância e têm ganhado interesse quanto a aplicações na área de vigilância.

Figura 28. Modos de se caminhar. Extraído de (URL19).

Todavia mesmo que esse tipo de reconhecimento de tenha ganhando força, o ritmo do momento pode ser influenciado pela dinâmica fornecida pelo indivíduo. Além da possibilidade de ser alterada por fatores externos.

4.10.1 Vantagens e Desvantagens

A principal vantagem do reconhecimento por melo modo de andar é que ele pode ser feito considerando uma distância razoável entre o dispositivo e o indivíduo.

Quanto às desvantagens, podem-se destacar:

- A forma de caminhar pode ser influenciada por fatores externos, saúde e humor do indivíduo a ser identificado;
- Acontecem mudanças no modo de andar durante as fases de visa do ser humano.

4.11 DINÂMICA DE DIGITAÇÃO

O Reconhecimento por meio da Dinâmica de Digitação usa do ritmo de toques no teclado como forma de autenticação de um indivíduo. Normalmente é uma tecnologia complementar, em que acontece a verificação do indivíduo em conjunto com o fornecimento de uma senha secreta.

O objetivo dessa tecnologia é medir a velocidade, pressão, tempo do duplo clique sobre a mesma tecla.

Os sistemas são classificados quanto à entrada recebida, que podem ser:

- Estática: Em que o usuário escreve um texto específico e por um tempo limitado;
- Contínua: A análise é feita sobre o que se escreve por um prazo de tempo indeterminado;
- Aplicação Específica: Esse tipo de entrada está preocupado com a parte comportamental. Por exemplo, o padrão de digitação de uma

pessoa para um e-mail corporativo é diferente do padrão da mesma pessoa quanto a digitação de um e-mail informal [5].

A mecânica de digitação pode ser separada em dois tipos:

- Tempo de pressão de uma mesma tecla: Medida de tempo ente a pressão e a soltura de uma dada tecla;
- Tempo entre teclas: Tempo entre de pressão e soltura de teclas sucessivas.

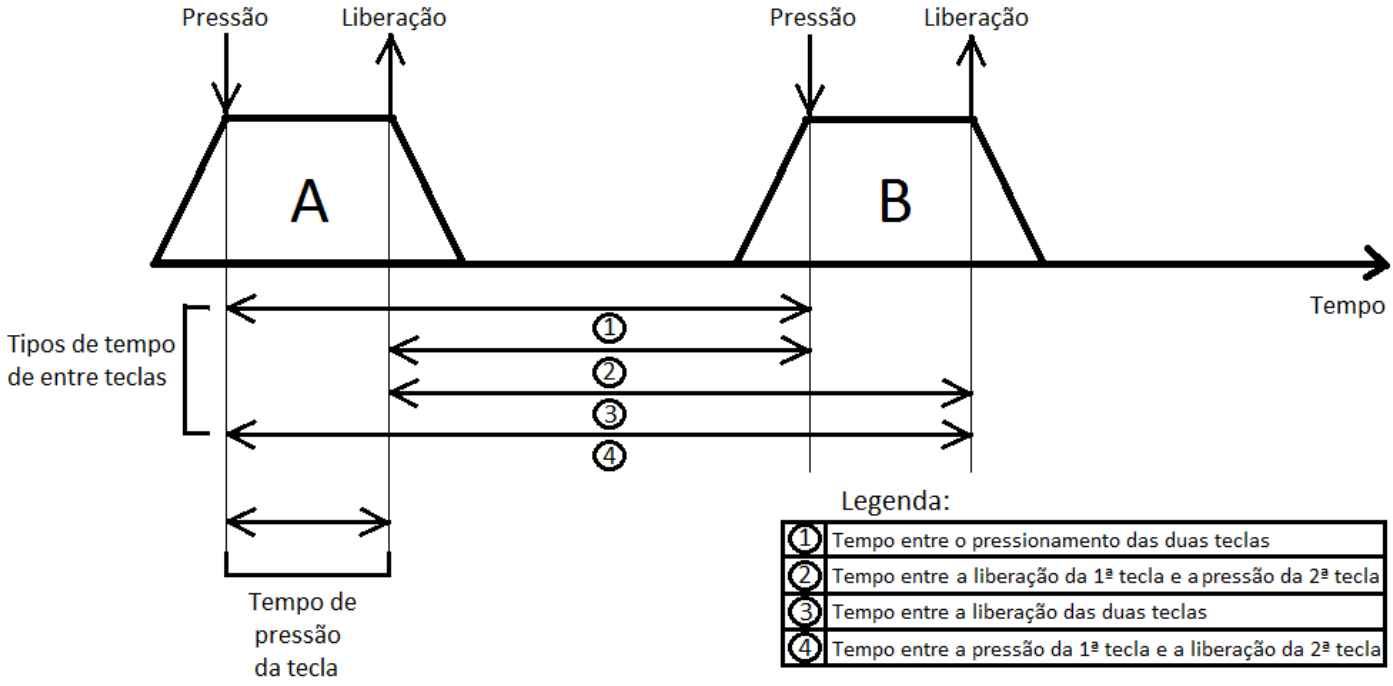


Figura 29. Demonstrações dos tipos de mensuração de tempo de digitação.

4.11.1 Vantagens e Desvantagens

Os pontos fortes da autenticação por meio da dinâmica de digitação são:

- Baixo custo de equipamento, uma vez que um teclado é relativamente barato;
- Facilidade quanto à utilização;

- Em todos os ambientes corporativos há a existência de computadores. Portanto a adição desse tipo de reconhecimento não implica na aquisição de mais equipamento;

- Método não invasivo.

Quanto aos pontos fracos, podem-se destacar:

- Como esse tipo de sistema mede padrões de comportamento por parte do usuário, então esse padrão pode ser alterado pelo estado físico ou te humor do mesmo;

- Tecnologia mais voltada para o modo de verificação, ou seja, é uma forma de reconhecimento complementar.

5. MULTIBIOMETRIA

A maioria das aplicações relacionadas ao Reconhecimento por meio da biometria faz uso somente de um dado biométrico para seus processos. Sendo estes cada vez mais requisitados a aplicações em larga escala e rotineiras.

Porém esse modelo de identificação necessita considerar uma densidade demográfica variada de usuários, ambientes diferentes para instalação da tecnologia, maior demanda quanto ao desempenho e processamento.

Há uma dificuldade de um sistema unimodal isto é, que trate apenas um aspecto biométrico, suprir o requisito de identificar unicamente um indivíduo. Portanto uma solução usual está na combinação de duas ou mais biometrias a fim de proporcionar maior confiabilidade, precisão na identificação de um indivíduo e uma maior abrangência para a população, permitindo assim a diminuição das vulnerabilidades tais como as fraudes, e diminuir as taxas de erro, dando reforço nos princípios de autenticidade quanto à tomada de decisão sistêmica. Sistemas baseados nesse princípio, de uso em conjunto de diversas técnicas biométricas, são denominados sistemas multibiométricos.

Para se projetar um sistema multibiométrico, devem-se considerar alguns fatores como:

- Quais biometrias serão utilizadas e a quantidades de minúcias a serem extraídas;
- Qual será o nível de integração e como se dá a combinação das informações;
- Qual a metodologia a ser aplicada;
- A natureza da aplicação;
- Processo de aquisição de amostras sequencial ou paralelo;
- O custo-benefício do projeto.

Devido à incipiência da área, a maior parte dos estudos em multibiometria tem feito combinações de somente duas ou três biometrias [10].

5.1 TIPOS DE SISTEMAS

Existem algumas categorias para os sistemas multibiométricos baseados no tipo de entrada recebida pelo sistema ou o número de componentes a serem usados no processo de cadastro e verificação ou identificação. A Figura 30 mostra os diferentes tipos de sistemas biométricos.

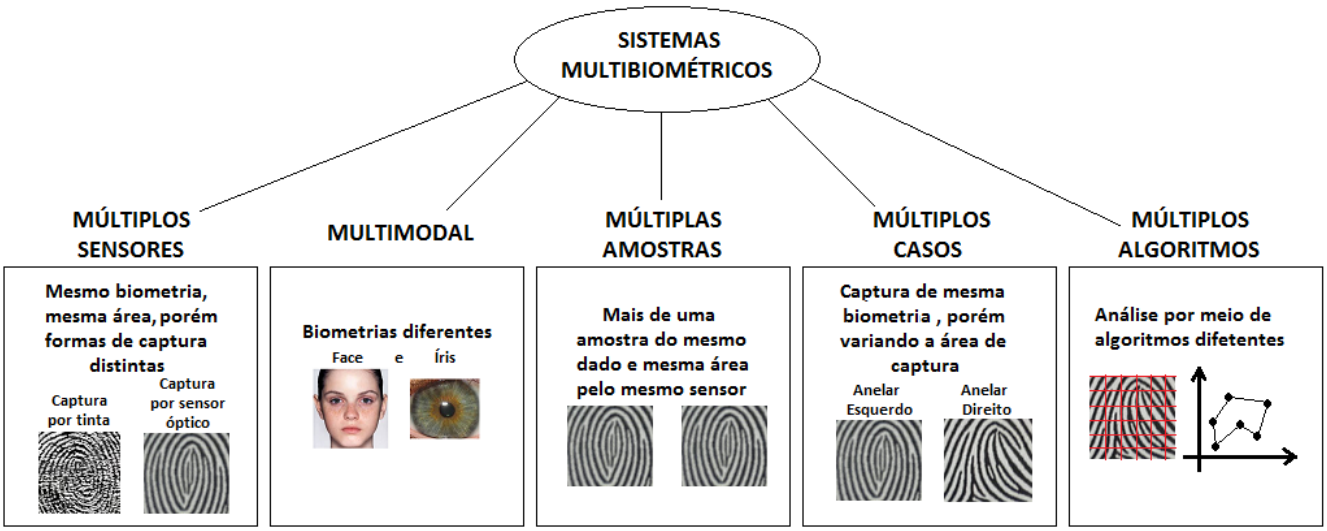


Figura 30. Tipos de Sistemas Multibiométricos.

5.1.1 Múltiplos Sensores

Nesses sistemas se utilizam vários tipos de dispositivos envolvidos na captura de uma mesma biometria, na mesma região. Esses sistemas são capazes de capturar diferentes níveis de informação, uma vez que a resolução da a amostra varia. Dependendo do projeto do sistema, não é necessário que o usuário necessite interagir mais de uma vez, todas as amostras são adquiridas em paralelo.

5.1.2 Multimodal

Esses sistemas usam duas biometrias diferentes. Os processos de adquirir, extrair características e comparar vêm de tecnologias distintas e a fusão pode acontecer em qualquer uma dessas etapas, para que a tomada de decisão seja feita de forma mais precisa. Esses sistemas tendem a ser mais caros, mas são os tipos mais comuns vistos em aplicações.

5.1.3 Múltiplas Amostras

Esses sistemas adquirem mais de uma amostra da mesma biometria, pelo mesmo equipamento e na mesma região. A combinação dessas múltiplas amostras tende a reduzir a variação do vetor de características.

5.1.4 Múltiplos Casos

O tipo do dado biométrico é o mesmo, mas as capturas das amostras acontecem em áreas distintas.

5.1.5 Múltiplos Algoritmos

A amostra a ser processada é a mesma, contudo a forma que será extraída as características, criação de *template* e comparação serão distintos devido ao uso de mais de um algoritmo no sistema.

5.2 NÍVEL DE FUSÃO

A fusão das informações obtidas das biometrias em um sistema multibiométrico pode acontecer em três situações:

- Na fase de extração de minúcias;
- Na fase de se comparar, para formar uma avaliação quanto às similaridades (match score);
- Na etapa da tomada de decisão.

Vale lembrar que essas três fases são baseadas nos cinco subsistemas que compõem um sistema biométrico: Aquisição, Processamento de Sinal, Armazenamento de Dados, Comparação e Tomada de Decisão.

Há outras possíveis formas de fusão, mas elas devem ser baseadas nos cinco subsistemas citados acima. A intenção de abordar essas três situações é para passar a ideia de como pode ser feita uma fusão no sistema multibiométrico e como ela contribui para o aperfeiçoamento do reconhecimento por biometria.

5.2.1 Fusão na Extração

A fusão na fase de extração de minúcias consiste em reunir em um modelo, para armazenamento ou comparação, padrões extraídos separadamente das biometrias, cada qual com o seu sensor adequado para captura.

Após a etapa da fusão, o processo do sistema segue como qualquer outro sistema biométrico, conforme são vistos nas Figuras 31 e 32.

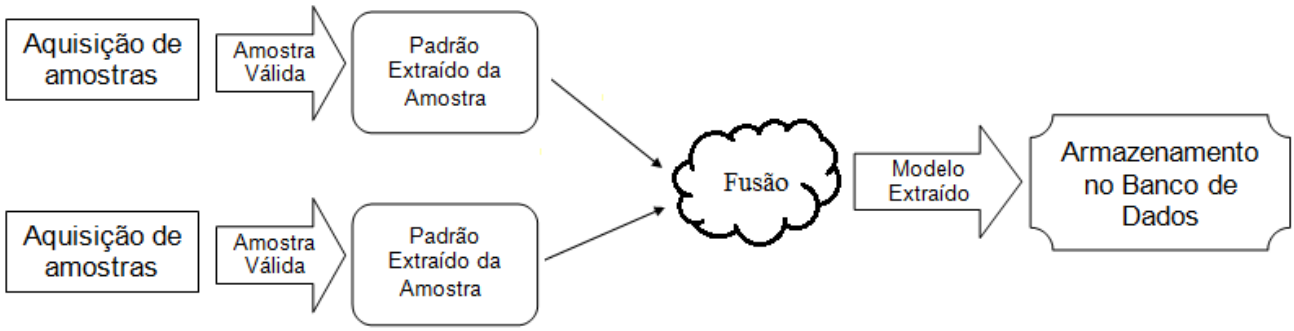


Figura 31. Cadastro de um Sistema Multibiométrico com Fusão na fase de Extração.

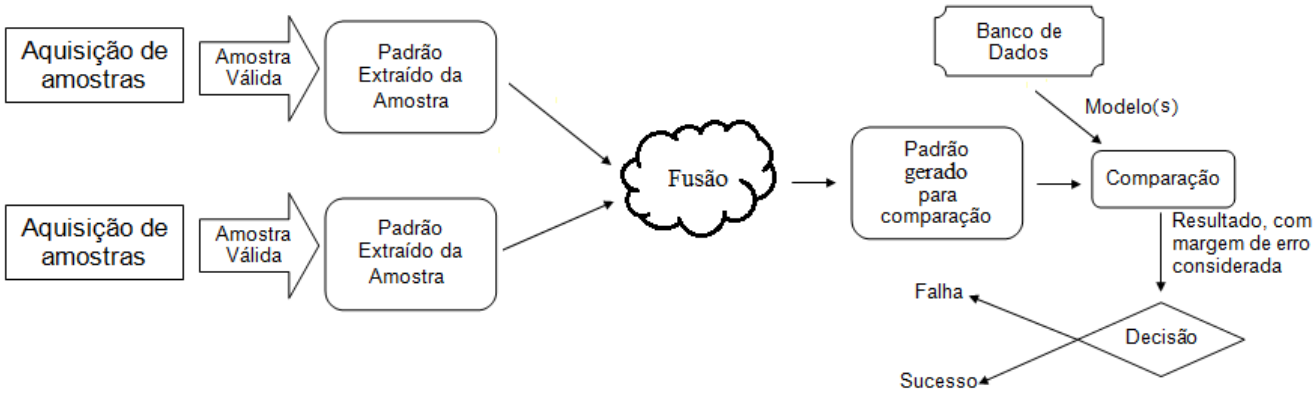


Figura 32. Verificação/Identificação de um Sistema Multibiométrico com Fusão na fase de Extração.

Não há muito interesse neste método porque:

- As minúcias ao passarem pelo processo de fusão podem se tornar incompatíveis numericamente ou também o usuário pode não possuir alguma das características solicitadas;

- O desenvolvimento do *score* de similaridades (*match score*), feito na fazer de comparação para a tomada de decisão, pode ser prejudicado.

Mesmo para um sistema unimodal, já é difícil encontrar um bom gerador de modelos (*templates*).

5.2.2 Fusão na Comparação

A fusão na fase de comparação consiste em realizar os subsistemas de aquisição, extração de minúcias, criação do *template* e armazenamento de forma separada. Os *matching scores* gerados separadamente são fundidos para se criar um *score* total, para assim ser feita a tomada de decisão. Os processos desse tipo de sistema podem ser vistos nas Figuras 33 e 34.

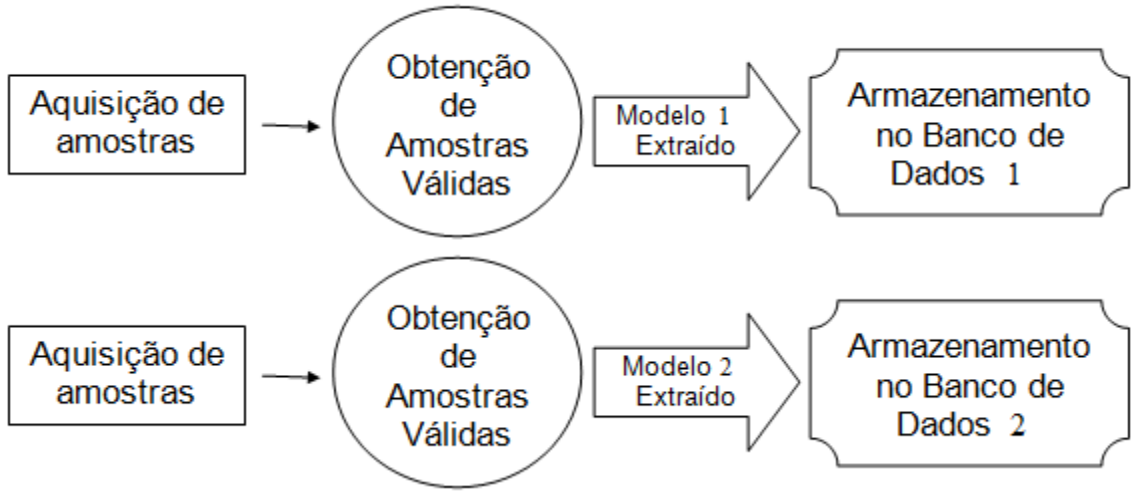


Figura 33. Cadastro de um Sistema Multibiométrico com Fusão na fase de Comparação e Decisão.

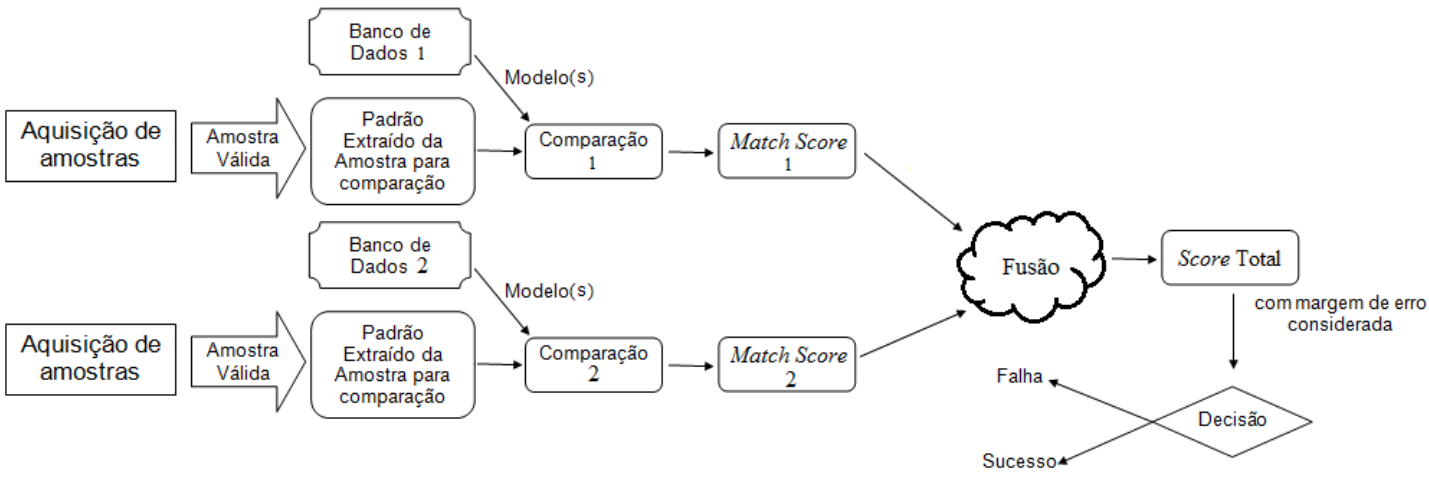


Figura 34. Verificação/Identificação de um Sistema Multibiométrico com Fusão na fase de Comparação.

O *Score* Total pode ser formado pelas seguintes formas [6]:

- Soma dos *matching scores*, colocando um peso em cada característica;
- Árvore de decisão, usando a comparação de diferentes *scores* para a tomada de decisão;
- Análise Linear Discriminante: transforma vetores tridimensionais de match *score* em um novo subespaço, em que a separação entre classes do *score* do usuário genuíno e o do impostor é maximizada. Os parâmetros ótimos são previamente obtidos empiricamente. O *score* resultante é definido por meio da distancia entre o centro das duas classes.

Esse tipo de sistema é o mais pesquisado na área de multibiometria, pois é a forma mais viável para o desenvolvimento de sistemas multibiométricos e o completo entendimento a respeito de como se comporta a etapa de fusão em testes em larga escala.

5.2.3 Fusão na Decisão

A fusão na fase de decisão é baseada na integração das decisões obtidas separadamente para se obter uma decisão final. Esta é a forma ais simples de se desenvolver um sistema multibiométrico, pois todos os subsistemas funcionam separadamente, como sistemas de uma biometria atuando de forma paralela. Ao final, depois da conclusão das etapas de decisão, é que a fusão ocorre e é por meio de uma votação, métodos baseados na estatística bayesiana[1], ou pelo uso das regras lógicas “e” e “ou” para que assim ocorra a autenticação do indivíduo.

O processo de Cadastro é igual ao da fusão na fase de comparação, Figura 33. O processo de autenticação (por meio da verificação ou identificação) pode ser visualizado na Figura 35.

[1] Métodos baseados em estatísticas bayesianas consistem obter densidades de probabilidades das tomadas de decisões de cada biometria paralela para depois fazer a combinação dessas densidades, por meio da regra do produto, para ser gerada a decisão final.

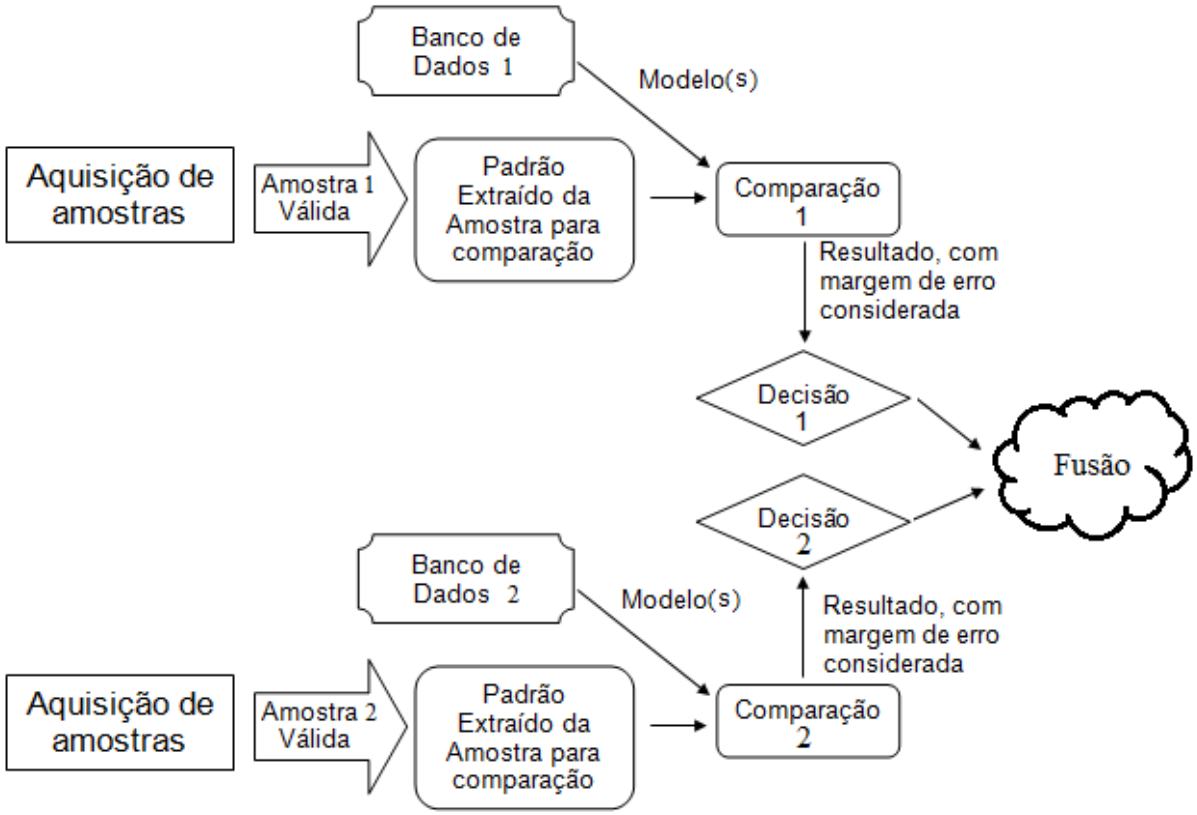


Figura 35. Verificação/Identificação de um Sistema Multibiométrico com Fusão na fase de Decisão.

5.3 CONSIDERAÇÕES QUANTO AO USO DE SISTEMAS MULTIBIOMÉTRICOS

O desenvolvimento dos sistemas multibiométricos visa solucionar problemas presentes em tecnologias que envolvem somente uma biometria, portanto esse tipo de tecnologia tem uma aplicabilidade em larga escala, como programas de identificação de âmbito nacional ou controle de fronteiras. Um exemplo é o projeto *Unique Identification Authority of India* (UIDAI) que começou em 2009, ele pretende atender 1,2 bilhões de residentes com um Número Único de Identificação (UID). Ele efetua a captura das digitais (10 dedos pousados/batidos), íris (ambos os olhos) e face [10].

Há vários desafios a serem vencidos na multibiometria, sendo que o tipo de sistema deve essencialmente depender do nível de precisão e do nível de abrangência, fatores que se comportam de maneira inversa. Outros fatores que também influenciam são:

1. Custo: A escolha da quantidade de biometrias a serem usadas no sistema e a quantidade de minúcias a serem extraídas é normalmente ditada pelo nível de segurança que se quer obter, o tipo de aplicação e pela capacidade de arcar com as despesas. O custo é diretamente proporcional à quantidade de biometrias selecionadas;

2. Correlação: O desempenho de um sistema depende da independência dos paramentos a serem usados nas técnicas de fusão. Por exemplo: um sistema com múltiplos algoritmos que usam a mesma amostra estão altamente correlacionadas, pois se utilizam das mesmas informações [5];

3. Fatores Humanos: A interação humana tende a ser mais complicada do que em um sistema que usa somente uma biometria, pois a aquisição de amostras pode ser seqüencial ou paralela, pode exigir maior tempo de interação e ocasionar desconforto. Um sistema paralelo tende a ser mais agradável para o usuário, mas encarece o sistema;

4. Arquitetura de Fusão: Qual é o tipo mais adequado de fusão? Isso depende de uma série de fatores práticos como o ambiente de operação, viabilidade financeira e das informações a serem obtidas, a densidade da população a ser usuária do sistema, entre outros;

5. Qualidade das Amostras: Há certos tipos de fusões que exigem uma reformulação quanto à medida de qualidade da amostra. Sendo um ramo de pesquisa recente, ainda há vários obstáculos quanto à melhor forma de ser organizar os equipamentos de captura, como as informações obtidas serão combinadas na etapa de fusão e como se devem interpretar os resultados obtidos;

6. Privacidade: A privacidade do usuário é o fator não técnico que mais gera desafio nesta área de pesquisa. Os sistemas multibiométricos obtêm mais informações e, na maioria dos casos, capturam minúcias de diferentes áreas. Medidas apropriadas de segurança e políticas de privacidade devem ser adotadas para todos os sistemas biométricos, e

devem ser especialmente levados em conta no desenvolvimento de sistemas multibiométricos.

6. PROPOSTA DE AVALIAÇÃO DE TÉCNICAS BIOMÉTRICAS

Após um extenso estudo teórico a respeito dos assuntos vigentes da área do reconhecimento do indivíduo por meio da biometria, este capítulo vem para desenvolver um método de análise, com a formação de um *Ranking* base, para avaliar tecnologias biométricas de forma genérica.

Este *ranking* serve como uma base para a avaliação das aplicabilidades, sendo atribuído peso às características de avaliação de maior relevância. Isso serve para do ranking original se derivar outros rankings de avaliação, com a finalidade de se selecionar a melhor tecnologia a ser empregada em determinado cenário prático.

O objetivo é apresentar uma visão global dos pontos essenciais das tecnologias, sem, contudo, detalhar cada um desses pontos destacados. Para isso, foi feito um estudo teórico prévio.

O *ranking* é baseado em características e funcionalidades empregadas como soluções fornecidas pelos sistemas de reconhecimento, pois o interesse é buscar um *checklist* das funcionalidades, ferramenta prática com que se faz a pontuação. Posteriormente um novo *checklist* é criado, esta é a ferramenta que é usada na adaptação dos diversos cenários, pois sua construção acentua as prioridades de cada aplicação e com ele se atribui os pesos.

Durante a pesquisa bibliográfica, se tornou claro que a avaliação de tecnologias biométricas não pode ser obtida de uma fórmula matemática. Existem modelos matemáticos para uma biometria específica baseados em estimativas estatísticas obtidas com testes. Além de não haver uma avaliação formal de sistemas multibiométricos.

Assim, as pontuações serão feitas conforme os resultados achados em pesquisas recentes, pois este trabalho não conta com equipamentos nem com *templates* suficientes para de obter resultados próprios. Além disso, segundo o *Nacional Institute of Standards and Technology* (NIST) é preciso, para obter resultados precisos, ter uma população entre 10.000 a 30.000 usuários pelo menos [6].

A contribuição desta proposta será desenvolvida em algumas etapas:

1. Apresentação de Características Globais;
2. Seleção de Tecnologias Biométricas a serem avaliadas;
3. Atribuição de pontuação conforme o nível fornecido por cada tecnologia, conforme as características apresentadas;
4. Disposição em um *Ranking* Base;
5. Avaliação de alguns cenários, para mostrar como se adapta o *ranking* base para as aplicações práticas.

6.1 CARACTERÍSTICAS GLOBAIS

As características globais estão relacionadas ao que se deve obter das tecnologias em questões como viabilidade, abrangência e desempenho. Demais características que têm certo nível de influência foram incluídas nas características citadas a seguir, pelo critério de afinidade.

6.1.1 Características Biométricas

As características biométricas estão relacionadas aos pontos fundamentais tratados na motivação do trabalho (item 1.2): universalidade, singularidade, coletável, permanente e desempenho. Vale levar em conta também alguns fatores complementares como a aceitação e a evasão do sistema.

6.1.2 Custo

O investimento a ser feito no sistema é fundamental para viabilizar o projeto. Portanto o custo consiste nos preços de softwares de controle e equipamentos de captura. A infra-estrutura é padrão então não interfere na diferenciação de uma biometria para outra, portanto não é contabilizada [6].

6.1.3 Intrusividade

A intrusividade é o nível de aceitação natural por parte do usuário quanto à tecnologia. Nela, além da parte física, entram aspectos como cultura e nível de colaboração por parte do usuário.

6.1.3.1 Cooperação do Usuário

As tecnologias que conseguem efetuar a autenticação do usuário sem que ele note que está sendo monitorado são consideradas tecnologias de baixo nível de intrusão. Isso também vale quanto ao cadastro e comparação, quando a aquisição de amostras também é feita de forma que o usuário nem perceba a captura faz com que a tecnologia tenha baixo nível de intrusividade.

Outro fator a ser considerado é se, na necessidade de uma interação física, a parte a ser exposta pelo sensor de captura é uma área sensível, como a íris ou retina, ou não sensível, como as mãos ou a face. Interação com áreas sensíveis tem o nível de intrusividade alto e interação com áreas não sensíveis do corpo tem nível de intrusividade baixo.

Uma intrusividade considerada média é obtida por parte das tecnologias que se utilizam de biometrias de caráter comportamental, como a assinatura e a voz [6].

6.1.4 Precisão

A precisão se remete à confirmação ou rejeição corretamente aplicada pelo sistema de autenticação a um usuário. Para isso, avaliam-se as taxas de erros obtidas dos resultados avaliados: FAR, FRR e ERR. Maiores detalhes sobre essas taxas, vide capítulo 3.

É por meio dessas taxas que se avalia a precisão, pois [10]:

- Menor o valor da FAR, melhor é a eficácia do sistema;
- Menor o valor da FRR, mais fácil é a identificação do usuário;
- Menor for a EER, maior é a precisão do sistema biométrico.

Além disso, se considera que um sistema possui baixo nível de precisão quanto este trabalha com biometrias comportamentais. Já os sistemas que utilizam biometrias fisiológicas possuem alto nível de precisão.

6.1.4.1 Múltiplas Amostras

A precisão pode ter influência na qualidade da aquisição de amostras, para fins de comparação e cadastramento. Inclusive, a coleta de várias amostras pode ser caracterizada como um sistema multibiométrico. Sua finalidade consiste em obter medidas com melhor qualidade.

De acordo com as pesquisas feitas por Alexandre F. de Moraes [6], um sistema biométrico apresenta um resultado satisfatório se possuir ao menos cinco imagens dos usuários cadastrados no *template* criado para os sistemas de reconhecimento que têm características que podem sofrer muita variabilidade em suas minúcias. Isso ocorre, por exemplo, em sistemas que usam a face e impressão digital como forma de reconhecimento.

Múltiplas amostras mostram que a tecnologia que trabalha com biometria que está predisposta a mudar, seja por fatores biológicos, comportamentais ou externos,oferece risco quanto ao nível de precisão. Sendo assim, quanto menos amostras forem necessárias, menor é a variação sofrida pela biometria e melhor é para a precisão do sistema.

6.1.5 Privacidade

A privacidade se refere a manter sigilosas as informações dos usuários que têm acesso ao sistema de reconhecimento. Para isso, é necessário oferecer proteção contra invasores ao banco de dados, que armazena essas informações. Também se deve garantir que terceiros não consigam acesso ao canal por onde essas informações trafegam.

6.1.5.1 Base de Dados

A Base de Dados é uma estrutura lógica que tem como finalidade o armazenamento de informações dos usuários cadastrados. Sua estrutura é essencialmente centralizada, com *backup* opcional para dar maior segurança às

informações contidas nele. Todavia, há tecnologias que somente armazenam o *template* em um identificador (objeto) e efetuam a comparação para a validação, aumentando o risco de fraude ou acesso não autorizado aos dados.

Essa base deve permitir o trafico de informações a toda a infra-estrutura que o sistema biométrico comporta, podendo ter vários terminais localizados em inúmeros países.

Além disso, para uma maior segurança, alguns sistemas efetuam o recadastramento automático, atualizando os *templates* quando o sistema verifica pequenas variações ao longo do uso do usuário.

6.1.5.2 Confidencialidade

Garantia de segurança das informações capturadas e armazenadas pelos sistemas de reconhecimento. Com isso se usa a criptografia desses dados, mais especificamente a criptografia simétrica [6], para satisfazer as necessidades impostas pelas aplicações.

Existe criptografia de chave forte e chave fraca. A chave forte demanda muito tempo e recurso computacional por ser uma chave com muitos bits a serem decifrados, assim provê maior segurança ao sistema.

6.1.5.3 Segurança Lógica

A proteção das informações que são armazenas e trafegam entre o banco de dados centralizados e os terminais de uso é essencial para qualquer sistema digital. Ainda mais se sua abrangência é grande no ponto de vista geográfico, com vários terminais interconectados.

Para a proteção e prevenção de intrusão a infra-estrutura e servidores, alguns fatores devem ser considerados [6]:

- Instalação de sistemas de prevenção à ataques tanto na rede quanto nos servidores, que identificam o padrão de ataque e conseguem bloquear;

- Firewall da rede, controle dos acessos externos à rede onde se encontram os servidores.

6.1.5.4 Tipo de Reconhecimento

As tecnologias que têm como autenticação por meio da identificação do usuário contém uma maior privacidade, devido à sua robustez e nem a necessidade de tecnologia complementar. Assim, as tecnologias que efetuam a verificação possuem menor nível de privacidade.

6.1.6 Segurança

A segurança das informações obtidas e armazenas depende de uma série de fatores que fazem com que essas informações devidamente protegidas. Alguns dos principais pontos são desenvolvidos a seguir.

6.1.6.1 Controle de Tentativas

A quantidade de tentativas feitas pelo usuário é verificada por meio dos registros de autenticação e pelos *logs* do sistema. Isso faz com que se tenha acesso às tentativas de fraudes no sistema.

Os registros de auditoria também estão presentes nas tentativas de recadastramento e falhas de autenticação [6].

6.1.6.2 Infra-estrutura de Segurança na Comunicação de Dados

Para se obter uma infra-estrutura segura, é preciso atender a alguns requisitos [6]:

- Confidencialidade: Proteção das informações contra acesso e cópia de agentes externos e internos não autorizados;

- Integridade: Proteção da informação quanto a possíveis modificações, tanto informações do usuário quanto programas que atuam no funcionamento do sistema, por pessoas não autorizadas;

- Autenticidade: Identificação do usuário ou da origem de uma mensagem;

- Disponibilidade: Proteção de serviços prestados pelo sistema, para que eles não sejam danificados ou disponíveis a quem não seja autorizado;

- Controle de Acesso: Efetuar a validação ou rejeição de prestação de serviços e recursos fornecidos pelo sistema;

- Não Repúdio: O remetente de uma mensagem ou ação não se negue ao futuro envio de mensagem ou realização da ação, isto é, repetição da interação entre o usuário e o sistema. Do mesmo jeito que o destinatário não se negue a receber essa mensagem ou ação.

Para que esses requisitos sejam satisfatoriamente supridos, o uso de algumas tecnologias complementares pode ajudar: emprego de certificação digital, criptografia, autenticação por meio de senhas, entre outros.

6.1.6.3 Maturidade da Solução

Este item faz alusão ao tempo, experiência de uso e ao nível de robustez da tecnologia a ser avaliada.

A Impressão Digital, por exemplo, têm sistemas implementados em larga escala, os chamados *Automated Fingerprint Identification System* (AFIS):

- São capazes de processar amostras obtidas de várias formas de captura, tais como amostras adquiridas por pintura, sensor óptico, entre outros;

- Tem um banco de dados de 10 milhões de digitais;

- As comparações são extremamente rápidas, com o uso de um sofisticado hardware e técnicas de classificação de ponta;

- O *template* extraído pode ser manualmente analisado ou organizado por peritos na área.

O AFIS hoje pode ser encontrado em aplicações movidas pela aplicação da lei, como identificação de criminosos, como também em sistemas de controle de fronteira e identificação de cidadãos. O reconhecimento pela impressão digital feito pelo FBI e o *Unique Identity Number* (UID) realizado pelo governo da Índia são exemplos práticos desse tipo de tecnologia [6].

6.1.6.4 Reconhecimento Adicional para Identificação

Se o sistema opera como verificador de usuário, então este necessita de uma forma complementar de identificação, a fim de efetuar a fase de comparação. Para isso, se podem usar objetos físicos (cartões síncronos, *smartcard*), palavra, sequência de números ou frase sigilosas que forneçam a identificação do usuário.

Nos meios físicos, é possível armazenar o *template* modelo. Isso faz com que o sistema possua um *backup* caso haja problemas no acesso ao banco de dados. O sistema pode somente fazer a conferência entre a amostra fornecida em tempo real e o *template* modelo do identificador.

6.1.6.5 Tipo de Reconhecimento

A forma de operação consiste e realizar a autenticação por meio da identificação ou da verificação. No item de privacidade, foi visto que tecnologias de identificação se sobressaem às tecnologias de verificação. Contudo, no quesito de segurança, o sistema se torna mais seguro quando este precisa de uma forma de reconhecimento adicional, um artifício que comprove a identidade do usuário e otimize a busca do *template* modelo para comparação. O objeto identificador também pode já fornecer o *template* modelo para o sistema.

Sistemas em larga escala têm preferência pela verificação, uma fez que a identificação provoca maior tempo de processamento, complexidade e aumento nas taxas de erros. Isso causa lentidão e baixa confiabilidade para o sistema. Inclusive o NIST realizou vários testes quanto à forma de operação e foi constatado que as aplicações usando a identificação não são satisfatórias para o uso em larga escala [6].

6.1.6.6 Verificação prévia da Identidade do Usuário

Seria uma verificação anterior ao cadastro do usuário. Nele pode envolver:

- Exigência de documentos físicos, compostos de foto e assinatura, que comprovem a sua identidade. Assim se pode verificar algumas informações do usuário, como antecedentes criminais e perfil de crédito de compras;

- Acesso a bancos de dados de criminosos internacionais, como o *Terrorist on Watch List* (TOWL).

6.1.7 Tempo

O tempo é um item essencial, pois fator de operação em tempo real nos processos de cadastramento, autenticação e autoria é de interesse para as tecnologias biométricas, principalmente para aplicações em larga escala. O objetivo é que o sistema forneça resultados logo após o momento da interação, para que facilite o uso do usuário e forneça maior eficiência para a empresa que utiliza a tecnologia biométrica.

6.1.7.1 *Template*

Dependendo do seu tamanho, influencia no tempo de trafego, alocação de espaço no banco e no tempo operacional do sistema.

6.1.7.2 Tempo de Autenticação

A velocidade, principalmente para aplicações em larga escala, é fundamental para efetuar o reconhecimento de um indivíduo. Portanto a tecnologia que requer menor tempo para a realização de seus processos tem maior interesse no mercado, sendo assim obtém maior pontuação.

6.1.7.3 Tempo de Cadastramento

Importante para se analisar a eficiência do sistema [6]. No caso da multibiometria, se deve considerar se a forma de captura ocorre em paralelo (todas as biometrias utilizadas são capturadas ao mesmo tempo) ou em sequência (uma

biometria só é capturada se não houver nenhuma outra sendo capturada ou a biometria anterior já terminou sua fase de aquisição). No caso, a segunda é a forma atualmente adotada devido aos recursos computacionais e tempo de processamento somam-se os tempos de captura.

6.1.8 Volume

A população de usuários é um grande fator de relevância, pois nele é que se verifica quantidade de espaço alocada para armazenamento de dados, quanto tempo pode ser gasto com os processos de cadastro e autenticação e as distorções que se pode ter nos resultados. Afinal quanto maior a população, menor deve ser o limiar da proporção de erros para se aumentar a conveniência, porém menor será a segurança do sistema.

6.1.8.1 Interoperabilidade

A padronização da forma de se criar *templates* proporciona a interoperabilidade, pois não importará qual sistema fez a captura. Além da padronização de *templates*, também se tem esforços quanto ao uso de sensores, chaves de indexação, padrão da base de dados e protocolos de comunicação [6]. Esses padrões têm o objetivo de se estender a todos os fabricantes de tecnologias biométricas, viabilizando a comunicação entre os sistemas, independente do país que adota esse tipo de sistema.

6.2 SELEÇÃO DE TECNOLOGIAS BIOMÉTRICAS

Nessa etapa, são selecionadas as tecnologias que melhor se aplicam aos possíveis cenários do mercado. Nesse sentido, são escolhidas as seguintes tecnologias mais usuais: Digital, Face, Geometria da Mão e Íris.

Essas biometrias citadas acima possuem equipamentos robustos, com maior maturidade, além de estarem na maioria dos estudos feitos em aplicações práticas.

Quanto à multibiometria, será desenvolvido um *ranking* à parte, com a combinação de 2 a 3 das biometrias selecionadas. Seu método será pela soma das pontuações das biometrias avaliadas individualmente e com a atribuição de peso nas características. Para isso, está sendo considerado que acontece a fusão na fase

de decisão (seção 5.2.3) e o tempo de aquisição sequencial. Essas decisões foram tomadas tendo em vista a complexidade da fusão em etapas anteriores à tomada de decisão e os recursos necessários para a aquisição em paralelo. A aplicação de pesos será basicamente referente às exigências nos cenários que serão apresentados na etapa final.

6.3 ATRIBUIÇÃO DE PONTOS

Devido à diversidade de formas de se avaliar o desempenho das tecnologias biometrias, se faz necessário adquirir um jeito de alinhar as pesquisas bases utilizadas neste critério de pontuação, com finalidade de se obter um padrão que seja derivado de uma adaptação satisfatória.

No primeiro momento serão colocadas as tabelas de avaliação dos dados biométricos, extraídos de suas respectivas fontes. Após a ciência das formas de avaliação, será selecionado um melhor critério de pontuação, que consiga abarcar todas as informações com o mínimo de distorção.

Como foram relacionadas anteriormente, as características globais a serem usadas no Ranking Base são: Características Biométricas, Custo, Intrusividade, Precisão, Privacidade, Segurança, Tempo e Volume. Todas receberão peso 1, pois não será gerado o ranking a partir de uma aplicação específica.

6.3.1 Características Biométricas

Tabela 6. Comparação entre as Tecnologias Biométricas. Adaptado de [10].

Biometrias	Universalidade	Singularidade	Permanência	Coletabilidade	Desempenho	Aceitabilidade	Evasão
Assinatura	BAIXA	BAIXA	BAIXA	ALTA	BAIXA	ALTA	ALTA
Digital	MÉDIA	ALTA	ALTA	MÉDIA	ALTA	MÉDIA	MÉDIA
Face	ALTA	BAIXA	MÉDIA	ALTA	BAIXA	ALTA	ALTA
Geometria da Mão	MÉDIA	MÉDIA	MÉDIA	ALTA	MÉDIA	MÉDIA	MÉDIA
Íris	ALTA	ALTA	ALTA	MÉDIA	ALTA	BAIXA	BAIXA

Para a finalidade desse trabalho, é realizada uma média aritmética das características.

6.3.2 Custo

De acordo com o relatório do Panorama Geral sobre Biometrias [10], se tem:

- Tecnologias com baixo custo: Assinatura, Digital e Geometria da Mão;
- Tecnologias de médio custo: Face (2D);
- Tecnologias de alto custo: Face (3D) e Íris.

6.3.3 Intrusividade

De acordo com o relatório do Panorama Geral sobre Biometrias [10] e demais fontes se têm:

- Alta Intrusividade: Íris;
- Média Intrusividade: Digital e Geometria da mão;
- Baixa Intrusividade: Assinatura e Face.

Seguem como principais formas de avaliação: se é invasiva a tecnologia (precisa de interação física), se a área do corpo é sensível ou não, aceitação por questões culturais, entre outras.

6.3.4 Precisão

A seguir seguem 2 tabelas diferentes, este trabalho analisou as duas para montar sua própria tabela de precisão.

Tabela 7. Taxas de FAR. Adaptado de [6].

Biometrias	FAR
Digital	10^{-8}
Face	10^{-2}
Geometria da Mão	10^{-4}
Íris	10^{-10}

Tabela 8. Taxas de FAR. Adaptado de [3].

Biometrias	FRR	FAR	Fonte
Assinatura	$\frac{3\ a\ 10}{100}$	$\frac{1}{100}$	V. Nalwa, *In Biometrics: Personal ID in Networked Society*
Digital	$\frac{3\ a\ 7}{100}$	$\frac{1\ a\ 100}{100.000}$	FVC 2000, U. Bologna, n=100, db3, Melhores resultados de fornecedores
Face	$\frac{10\ a\ 20}{100.000}$	$\frac{100\ a\ 10.000}{100.000}$	FRVT 2000, NIST, n=227, temporal (T3), Melhores resultados de fornecedores
Geometria da Mão	$\frac{1\ a\ 10}{100}$	$\frac{1}{100}$	*National Physics Laboratory*, UK, *Recognition Systems* Inc.
Íris	$\frac{1\ a\ 10}{100}$	0	*National Physics Laboratory*, UK, Sandia Labs

Para achar a taxa de aceitação, utilizaremos a seguinte fórmula: 1- FAR. Foram usados os valores que mais favorecem as tecnologias, ou seja, as menores taxas de falsa aceitação.

Tabela 9. Tabela de Precisão.

Biometrias	FAR	1 - FAR	Precisão
Assinatura	10^{-2}	0,9	BAIXA
Digital	10^{-8}	0,9999999	ALTA
Face	10^{-3}	0,99	MÉDIA
Geometria da Mão	10^{-4}	0,999	MÉDIA
Íris	0	1	ALTA

6.3.5 Privacidade

Como este critério não tem tabelas específicas, avaliando as tecnologias biometrias, então a avaliação deste trabalho será baseada em descrições obtidas nas diversas fontes em que esse trabalho se baseou.

- Assinatura (Dinâmica):

Aspectos Positivos

- Informação capturada sem meio físico intermediário (papel);
- Assimilação de vários aspectos além da caligrafia em si, como velocidade, pressão e pausas;
- Suscetível a mudanças, tanto comportamentais quanto de maturidade do autor.

Aspectos Negativos

- Baixo desempenho na comparação automatizada;
- Inúmeros documentos como passaporte e RG, se utilizam da assinatura como identificador.

O uso da assinatura é a forma de autenticação mais antiga composta de vários bancos de dados físicos, como cartórios, e alguns bancos de dados digitais, como assinatura digital impressa no passaporte. Essa forma de reconhecimento é extremamente vulnerável a fraudes e mudanças do próprio usuário. Portanto é mais

adequada como uma tecnologia complementar de reconhecimento. Sendo assim recebe baixo grau de privacidade.

- Digital:

Aspectos Positivos	Aspectos Negativos
➢ Variedade de fornecedores com diversos tipos de *templates* e algoritmos;	➢ Suscetível a ataques *Spoofing*;
➢ Alto grau de complexidade;	➢ Baixa qualidade de amostras pela falta de habilidade do usuário;
➢ Adequado tanto para o modo de identificação quanto verificação.	➢ Possibilidade de uso como prova forense.

A impressão digital, na área da biometria, é o dado mais consolidado e antigo. Possui vários bancos de dados com inúmeros *templates* armazenados, sendo viável o trabalho desse tipo de tecnologia em larga escala. O grande desafio é a prevenção de fraudes por conta de dados reproduzidos por meio de objetos inanimados, algo possível de ser tratado com um reconhecimento complementar quanto à vivacidade do usuário. Assim o nível de privacidade é baixo, pela grande viabilidade de se conseguir informações confidenciais do usuário por meio de sua digital.

- Face:

Aspectos Positivos	Aspectos Negativos
➢ Tecnologia recente;	➢ Possibilidade de captura sem autorização;
➢ Mudança na aparência e o uso de adereços ajudam na proteção da identidade.	➢ Diversos documentos têm fotografia;
	➢ Acesso a informações por meio

de identificação feita pela foto em redes sociais.

A face é uma biometria cujo interesse no seu uso como dado biométrico vem crescendo, principalmente na área de vigilância. Todavia, como a face é uma biometria altamente exposta, bastante utilizada em redes sociais, isso faz com que ela forneça um baixo nível de privacidade.

- Geometria da Mão

Aspectos Positivos	**Aspectos Negativos**
➢ Usada somente na verificação; ➢ Precisa de um dispositivo, que haja contato entre o usuário, para a aquisição de dados; ➢ Característica visível, porém pouco visada.	➢ Não há.

O nível de privacidade é alto fornecido pela tecnologia que se usa da geometria das mãos como meio de reconhecimento, isso é demonstrado pelas listagens acima.

- Íris

Aspectos Positivos	**Aspectos Negativos**
➢ Necessita de muita cooperação por parte do usuário, portanto é quase impossível ser capturada sem o consentimento; ➢ Não é utilizada para aplicação da lei, portanto não é prova contra	➢ Uso na identificação de um indivíduo; ➢ Os *templates* não têm muita variação de um fabricante para

crimes;
- Parte sensível, protegida por adereços, como óculos;
- Alto grau de complexidade.

outro, o *IrisCode* é patenteado.

Por mais que a íris seja uma biometria difícil de capturar, quando se tem acesso a ela, facilmente pode se identificar o indivíduo, pois as tecnologias adotam quase um padrão quando a configuração de *templates*. Sendo assim, o nível de privacidade é considerado médio.

6.3.6 Segurança

No ponto de vista intra-estrutura, maturidade da solução, tipo de reconhecimento e outros critérios, a segurança proporcionada pelas biometrias selecionadas é avaliada como:

Tabela 10. Segurança das Biometrias.

Biometrias	Segurança
Assinatura	BAIXA
Digital	ALTA
Face	BAIXA
Geometria da Mão	MÉDIA
Íris	ALTA

6.3.7 Tempo

O tempo está relacionado com a captura e os processos feitos até a tomada de decisão, com a validação ou rejeição do usuário.

Nessa característica global se seguirão os critérios de cadastro e tempo para se autenticar um usuário, ambos retirados da dissertação de mestrado de Alexandre F. de Moraes [6] e no livro *Guide of Biometrics* [8].

Tabela 11. Tempo de Cadastro e Autenticação.

Biometrias	Tempo de Cadastramento	Tempo de autenticação
Assinatura	MÉDIO	BAIXO
Digital	MÉDIO (94 seg)	BAIXO (19 seg)
Face	ALTO (180 seg)	BAIXO (10 seg)
Geometria da Mão	BAIXO (57 seg)	BAIXO (10 seg)
Íris	ALTO (136 seg)	BAIXO (12 seg)

6.3.8 Volume

O volume está relacionado à aplicação em pequena, média e alta escala. Aquelas tecnologias biometrias que podem ser aplicadas a larga escala recebem uma alta avaliação e aquelas que são viáveis somente a pequena escala recebem baixa avaliação.

Tecnologias que podem ser aplicadas em:

- Larga Escala: Assinatura, Digital e Íris;
- Média Escala: Assinatura, Digital, Geometria da Mão e Íris;
- Pequena Escala: Assinatura, Digital, Face, Geometria da Mão e Íris.

6.4 *RANKING* BASE

Após a análise das avaliações dos 8 critérios globais propostos para a avaliação das 5 tecnologias biométricas também selecionadas anteriormente, pode-se inferir que a melhor forma de se alinhar todas as informações é pela utilização da seguinte métrica:

Tabela 12. Definição e descrição das pontuações.

Pontuação	Descrição
1	Pontuação mínima, atribuída aos baixos níveis obtidos pelas tecnologias nos critérios globais
2	Pontuação mediana, atribuída aos níveis aceitáveis, porém com necessidade de aperfeiçoamento das tecnologias
3	Pontuação máxima, atribuída às tecnologias que atingiram níveis satisfatórios nos critérios

Tabela 13. Comparação entre as Tecnologias Biométricas com Pontuação.

Biometrias	Universalidade	Singularidade	Permanência	Coletabilidade	Desempenho	Aceitabilidade	Evasão
Assinatura	1	1	1	3	1	3	3
Digital	2	3	3	2	3	2	2
Face	3	1	2	3	1	3	3
Geometria da Mão	2	2	2	3	2	2	2
Íris	3	3	3	2	3	1	1

Tabela 14. Características Biométricas com Pontuação.

Biometrias	Média Aritmética
Assinatura	1,9
Digital	2,4
Face	2,3
Geometria da Mão	2,1
Íris	2,3

Tabela 15. Custo com Pontuação.

Biometrias	Custo
Assinatura	3
Digital	3
Face	(2+1)/2 = 1,5
Geometria da Mão	3
Íris	1

Tabela 16. Intrusividade com Pontuação.

Biometrias	Intrusividade
Assinatura	3
Digital	2
Face	3
Geometria da Mão	2
Íris	1

Tabela 17. Precisão com Pontuação.

Biometrias	Precisão
Assinatura	1
Digital	3
Face	2
Geometria da Mão	2
Íris	3

Tabela 18. Privacidade com Pontuação.

Biometrias	Privacidade
Assinatura	1
Digital	1
Face	1
Geometria da Mão	3
Íris	2

Tabela 19. Segurança com Pontuação.

Biometrias	Segurança
Assinatura	1
Digital	3
Face	1
Geometria da Mão	2
Íris	3

Tabela 20. Tempo com Pontuação.

Biometrias	Tempo de Cadastramento	Tempo de autenticação	Tempo (média aritmética)
Assinatura	2	3	2,5
Digital	2	3	2,5
Face	1	3	2
Geometria da Mão	3	3	3
Íris	1	3	2

Tabela 21. Volume com Pontuação.

Biometrias	Volume
Assinatura	3
Digital	3
Face	1
Geometria da Mão	2
Íris	3

Tabela 22. *Ranking* Base.

Características Globais	Assinatura	Digital	Face	Geometria da Mão	Íris
Características Biométricas	1,9	2,4	2,3	2,1	2,3
Custo	3	3	1,5	3	1
Intrusividade	3	2	3	2	1
Precisão	1	3	2	2	3
Privacidade	1	1	1	3	2
Segurança	1	3	1	2	3
Tempo	2,5	2,5	2	3	2
Volume	3	3	1	2	3
TOTAL	16,4	19,9	13,8	19,1	17,3

Para as combinações do *ranking* da multibiometria, são utilizadas observações feitas não só neste trabalho como nas referências em que o mesmo se baseou. Assinatura, Face e Geometria da Mão serão utilizadas como tecnologias complementares, pois são tecnologias que essencialmente trabalham no modo de verificação. Digital e Íris oferecem a robustez e o requisitos necessários para atuarem como tecnologias que trabalham no modo de identificação.

Podem ser feitas outras combinações, isso vai depender de qual o propósito da aplicação e o orçamento para sua viabilização.

Tabela 23. *Ranking* Multibiometria.

Características Globais	Assinatura + Digital	Geometria da Mão + Digital	Assinatura + Digital + Geometria da Mão	Face + Íris	Digital + Íris	Digital + Face
Características Biométricas	4,3	4,5	6,4	4,6	4,7	4,7
Custo	6	6	9	2,5	4	4,5
Intrusividade	5	4	7	4	3	5
Precisão	4	5	6	5	6	5
Privacidade	2	4	5	3	3	2
Segurança	4	5	6	4	6	4
Tempo	5	5,5	8	4	4,5	4,5
Volume	6	5	8	4	6	4
TOTAL	36,3	39	55,4	31,1	37,2	33,7
Normalizado	18,2	19,5	18,5	15,6	18,6	16,9

6.5 AVALIAÇÃO DE ALGUNS CENÁRIOS

Para a constituição dos rankings personalizados, adaptados aos cenários propostos a seguir, foram criados três grupos quanto ao nível de importância das tecnologias:

- Alta: Aspectos críticos da tecnologia biométrica, nos pontos de vista de projeto, implementação e aplicação;
- Média: Aspectos que tem relevância, ma não são cruciais paras finalidades práticas;
- Baixas: Consideradas características opcionais. Acrescentam qualidades ao desempenho do sistema, mas não tem prioridade.

Com isso se constrói outro *checklist*, que servirá dizer quais são as prioridades requeridas pelo projeto e quais critérios têm média e mínima relevância.

Tabela 24. Definição e descrição de Pesagem.

Peso	Descrição
1	Peso mínimo, atribuído aos critérios de menor relevância para o projeto
2	Peso médio, atribuído aos critérios de relevância, mas que não tem prioridade
3	Peso máximo, atribuído ao checklist de prioridades do projeto

6.5.1 Sistema Eleitoral

No Brasil, por exemplo, é pelo Sistema Eleitoral que traça regras e diretrizes a serem seguidas com a finalidade de se eleger, dentre os candidatos, políticos que ocupem os cargos públicos do Poder Executivo (Presidente, Governadores e Prefeitos) ou do Poder Legislativo (Senadores, Deputados Federais, Deputados Estaduais e Vereadores). Nesse sentido, segue na Tabela 25 o *checklist* personalizado para o Sistema Eleitoral.

Tabela 25. *Checklist* de Prioridades do Sistema Eleitoral.

Características Globais	Peso a ser multiplicado
Características Biométricas	3
Custo	2
Intrusividade	2
Precisão	3
Privacidade	3
Segurança	3
Tempo	2
Volume	3

Tabela 26. *Ranking* do Sistema Eleitoral.

Características Globais	Assinatura	Digital	Face	Geometria da Mão	Íris
Características Biométricas	5,7	7,2	6,9	6,3	6,9
Custo	6	6	4,5	6	3
Intrusividade	6	4	6	4	2
Precisão	3	9	6	6	9
Privacidade	3	3	3	9	6
Segurança	3	9	3	6	9
Tempo	5	5	4	6	4
Volume	9	9	3	6	9
TOTAL	40,7	52,2	36,4	49,3	48,9

O resultado condiz com a realidade vivida no Brasil, que para as eleições de 2014 se realizou o recadastramento biométrico utilizando a digital como sua forma de reconhecimento. A digital é a biometria mais apropriada, afinal um dos fatores cruciais desse sistema é a identificação. Como a geometria da mão atualmente trabalha no modo de verificação, a tecnologia só é efetiva se houver outro reconhecimento auxiliando na busca do *template* para a comparação 1:1, além de sua aplicação não ser adequada para larga escala.

Outro ponto de destaque na Tabela 26 é que a Íris é a terceira melhor biometria para o sistema eleitoral, o que é uma opção interessante por ser uma biometria que oferece uma boa prevenção contra possíveis fraudes.

6.5.2 Identificação Civil

Um sistema de identificação de abrangência nacional, tal como proposto para o Sistema Nacional de Identificação Civil consiste em um único registro que, para cada cidadão, nato ou naturalizado, seja identificado em suas relações com a sociedade e com os organismos governamentais e privados.

Tabela 27. *Checklist* de Prioridades da proposta de Identificação Civil.

Características Globais	Peso a ser multiplicado
Características Biométricas	3
Custo	2
Intrusividade	2
Precisão	3
Privacidade	1
Segurança	3
Tempo	2
Volume	3

Tabela 28. *Ranking* da proposta de Identificação Civil.

Características Globais	Assinatura	Digital	Face	Geometria da Mão	Íris
Características Biométricas	5,7	7,2	6,9	6,3	6,9
Custo	6	6	5	6	2
Intrusividade	6	4	6	4	2
Precisão	3	9	6	6	9
Privacidade	1	1	1	3	2
Segurança	3	9	3	6	9
Tempo	5	5	4	6	4
Volume	9	9	3	6	9
TOTAL	38,7	50,2	34,9	43,3	43,9

A digital é uma biometria consolidada, robusta, capaz de identificar indivíduos. Já possui vários equipamentos no mercado e inúmeros *templates* capturados. Portanto era ter tido a maior nota dentre as 5 biometrias já era previsto.

6.5.3 Identificação da Retaguarda em Aeroportos

Um sistema de identificação que autentique somente indivíduos autorizados a trafegarem em ambientes restritos ao público. No caso, a proposta serve para os funcionários de companhias aéreas, como os pilotos, aeromoças, atendentes e os terceirizados que fazem parte do corpo funcional da empresa.

Tabela 29. *Checklist* de Prioridades da proposta de Identificação de Retaguarda em Aeroportos.

Características Globais	Peso a ser multiplicado
Características Biométricas	2
Custo	2
Intrusividade	2
Precisão	3
Privacidade	3
Segurança	3
Tempo	2
Volume	1

Tabela 30. *Ranking* da proposta de Identificação de Retaguarda em Aeroportos.

Características Globais	Assinatura	Digital	Face	Geometria da Mão	Íris
Características Biométricas	3,8	4,8	4,6	4,2	4,6
Custo	6	6	3	6	2
Intrusividade	6	4	6	4	2
Precisão	3	9	6	6	9
Privacidade	3	3	3	9	6
Segurança	3	9	3	6	9
Tempo	5	5	4	6	4
Volume	3	3	1	2	3
TOTAL	32,8	43,8	30,6	43,2	39,6

Pela digital ser a biometria que mais se tem aplicações, estudos e banco de dados, acaba que sua tecnologia se adapta bem nos mais diversos ambientes. Observamos 3 casos e nos 3 a digital prevalece.

Mas também se pode observar que a geometria da mão e a íris se aproximam. As diferenças em décimos significam o quão aptas essas tecnologias estão mesmo sendo de interesse recente seus estudos.

Neste cenário caberia o uso da geometria da mão com a complementação de um reconhecimento adicional como identificador, por meio de senha ou cartão, que atenderia satisfatoriamente as necessidades das empresas.

Já a íris pode ser aplicada a questões que exigem um nível maior de segurança, como na identificação de pilotos no painel de controle do avião, prevenindo assim a possibilidade de se a tomar do comando do avião por ataques terroristas.

7. CONCLUSÃO

A Biometria é uma vasta área, cheia de possibilidades e desafios. Ela é uma etapa fundamental para a progressão tecnológica, pois o indivíduo pode encontrar em si mesmo o seu identificador no mundo virtual.

Vivemos a era da Informação, que viabiliza um universo de informações, há uma integração econômica, social, política, cultural e comunicacional. Todavia, quanto mais as informações se entrelaçam, mais complexo fica realizar a proteção e preservação dessas informações e dos inúmeros usuários que fazem uso delas.

Há obstáculos a serem superados pelos sistemas biométricos, como [11]:

- Excesso de Informação: Traços únicos se apresentam desde áreas macroscópicas que compõem o indivíduo até fragmentos do DNA. Quanto mais se investiga, mais se acham novos traços que podem ser considerados traços com potencial biométrico. É desafiador conseguir, dentre tantas possibilidades, projetar um sistema biométrico eficiente e que satisfaça as necessidades que o mercado impõe;

- Paradoxo da População: Quanto mais variada e de grandes proporções é uma população, maior é a confiabilidade estatística dos testes. Contudo, ainda é necessário lidar com a influência genética, pois quanto maior o parentesco maior é o comprometimento do nível de precisão. Isso pode ser visto com o DNA, quanto maior o grau de parentesco, mais similaridades se encontra no material, chegando a ficarem idênticos quando analisamos materiais de dois irmãos monozigóticos;

- Privacidade: A aceitabilidade do uso dos sistemas biométricos é diretamente afetada pelo nível de privacidade e intrusividade. Assim a sociedade deve determinar qual é o nível de tolerância da perca da privacidade para elevar a segurança, justiça e eficiência;

- Intrusividade: É perfeitamente normal a rejeição da interação física necessária para a autenticação de um sistema biométrico. Entram

questões de higiene, posicionamento e políticas de uso dos dispositivos. Os sensores também podem desencadear constrangimento, pois usuários genuínos podem ser erroneamente rejeitados por não se comportarem de maneira natural ou não colaborarem;

- Ruídos: Na captura de amostras, a presença de ruídos é inevitável. Isso compromete o desempenho no reconhecimento. Os projetos dos sistemas devem identificar e ponderar as interferências, obstruções, condições ambientais, entre outros;

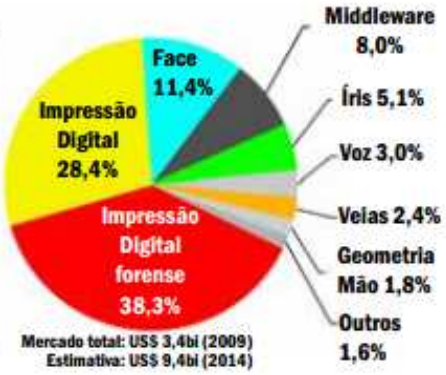
- Vulnerabilidade: Impostores e *Hackers* têm como objetivo burlar os sistemas. Fazem uso de objetos que imitam os traços genuínos a serem requisitados, inserem ou modificam informações. Quanto maior os acessos as informações sigilosas mais prejudiciais se tornam os ataques.

O interesse na multibiometria cresce, com a perspectiva de: aumentar a precisão dos sistemas de reconhecimento biométrico, prover mais segurança com o aumento das biometrias a serem fraudadas e tornar o sistema mais abrangente por oferecer mais de uma opção de biometria a ser cadastrada. Todavia é uma área nova, que tem muitas perguntas que ainda não tem respostas, como a melhor forma de criar *templates*, onde se deve inserir a etapa de fusão, quanto tempo leva para se obter resultados, entre outros.

As possibilidades quanto à utilização das tecnologias biométricas são enormes, promissoras e podem atingir vários ramos que necessitam de sistemas de reconhecimento com melhor desempenho. A Tabela 29 mostra a abrangência da biometria em 2009, com uma estimativa para o ano de 2014.

Tabela 31. Aplicações Biométricas no Faturamento Mundial do ano de 2009. Extraído de [11].

Forense	Governamental	Comercial
Identificação de corpos	Prevenção de crimes	Auxílio à medicina
Investigação criminal	Unicidade: RG, CNH	Controle de acesso
Parentesco	e-previdência, e-voto	Câmeras inteligentes
Crianças desaparecidas	Fronteiras	Comércio eletrônico



Mesmo com a análise de cenários mais definidos, como foi feito no capítulo anterior (6.5), existem critérios de relevância que não foram retratados, como quais são as biometrias que o público alvo pode fornecer. Entra questões com o fluxo de portadores de necessidades especiais ou o tipo de trabalho que a pessoa exerce (manual ou não).

Esse trabalho veio com o objetivo de apresentar esse novo universo que a biometria pode propiciar, pois mostra como podemos avaliar biometrias mesmo não havendo uma fórmula matemática geral para isso. O *Ranking* procura elucidar algumas das questões globais essenciais, proporcionando um direcionamento quanto à seleção da tecnologia biométrica que melhor atende as exigências impostas pelo consumidor.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Anil K., Jain, Arun,Ross and Salil, Prabhakar, 2004,"*An Introduction to Biometric Recognition*".

[2] Fumy,Walter, Paeschke, Manfred, 2011," *Handbook of eID Security: Concepts, Pratical Experiences, Tecnologies*",Publicis,1ª Edição.

[3] Koerich, Alessandro L., 2004, "Sistemas Biométricos", Apresentação XII Escola Regional de Informática, Sociedade Brasileira de Computação, Programa de Pós-graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná.

[4] Magalhães, P.S, 2005, "Estudo dos padrões de Digitação e sua aplicação na autenticação biométrica", Dissertação de Mestrado, Universidade do Minho, Departamento de Sistemas de Informação.

[5] Modi, Shimon K., 2011, " *Biometrics in Identity Management: Concepts to Applications*", Artech House.

[6] Morais, Alexandre F. de, 2006, "Método para Avaliação da Tecnologia Biométrica na Segurança de Aeroportos", Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo, S.Paulo, Brasil, 230 p.

[7] Pereira, Cipriano Luís Arede, 2012, "Dispositivos de Identificação", Tese de Mestrado, Escola Superior de Tecnologia e Gestão de Viseu, Instituto Politécnico de Viseu.

[8] Senior, Andrew W., Ratha, Nalini K.,Pankanti, Sharath, Connell, Jonathan H., Bolle, Ruud M., 2004, "*Guide to Biometrics*".

[9] Silva, Abel Bruno Nascimento, 2013, "Reconhecimento Facial Usando Eigefaces", Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil.

[10] Universidade de Brasília, Centro de Apoio ao Desenvolvimento Tecnológico, Laboratório de Tecnologias de Tomada de Decisão, 2014, "Panorama Geral sobre Biometrias", Brasília, Brasil.

[11] Vertamatti, Rodolfo, 2011, “Assimetria Humana no Reconhecimento Multibiométrico”, Tese de Doutorado, Escola Politécnica da Universidade de São Paulo, São Paulo, Brasil.

REFERÊNCIAS URL’S

(URL1)http://www.das.ufsc.br/~rro/pubs/sbseg06-biometria.pdf Acessado em 06 de junho de 2014.

(URL2)http://www.ibiometrica.com.br/biometria_sistemas.asp Acessado em 06 de junho de 2014.

(URL3)http://araquemce.blogspot.com.br/2010/12/materia-da-semana-impressao-digital.html Acessado em 09/06/2014.

(URL4)http://www.trunews.com/3d-biometric-identification-system-law-enforcement-gets-pilot-test/ Acessado em 15/06/2014.

(URL5)http://article.wn.com/view/2014/04/30/Next_Generation_Biometric_Fingerprint_Palm_Face_Iris_Vein_Vo/ Acessado em 15/06/2014.

(URL6)http://www.intechopen.com/books/new-trends-and-developments-in-biometrics/3d-and-thermo-face-fusion Acessado em 15/06/2014.

(URL7)http://www.compuland.com.br/anatomia/olho.htm Acessado em 17/06/2014.

(URL8)http://www.gta.ufrj.br/grad/07_2/carlos_eduardo/Produtos.html Acessado em 19/06/2014.

(URL9)http://www.case.edu/think/breakingnews/retinalgrant.html Acessado em 20/06/2014.

(URL10)http://www.studiomel.com/20.html Acessado em 20/06/2014.

(URL11)http://www.profala.com/arttf57.htm Acessado em 20/06/2014.

(URL12)http://www.virtual.epm.br/pacientes/fono/producao.htm Acessado em 20/06/2014.

(URL13)http://imagensdafisica.blogspot.com.br/ Acessado em 20/06/2014.

(URL14)http://blog.paramedico.com.br/saude/dia-mundial-da-voz-como-cuidar Acessado em 20/06/2014.

(URL15)http://pzycoderz.wordpress.com/2012/07/27/palm-vein-technology-3/ Acessado em 21/06/2014.

(URL16)http://www.online24.pt/como-criar-uma-assinatura-digital/ Acessado em 23/06/2014.

(URL17)http://www.olivetti.com/BR/Page/t01/view_html?idp=941 Acessado em 23/06/2014.

(URL18)http://aprendendo-quimica.blogspot.com.br/2011/12/extracao-caseira-do-dna-do-morango.html Acessado em 26/06/2014.

(URL19)http://www.bigstock.com.br/image-45020416/stock-photo-volta-da-cole%C3%A7%C3%A3o-ver-os-pessoas-andando-indo-pessoas-no-conjunto-do-movimento-pessoa-de-vista-traseira-peo-de-vista-traseira Acessado em 26/06/2014.

(URL 20)http://www.jusbrasil.com.br/topicos/293110/sistema-eleitoral Acessado em 05/07/2014.

(URL 21)http://www.planalto.gov.br/ccivil_03/leis/l9454.htm Acessado em 05/07/2014.