Capítulo 4

Autenticação usando Sinais Biométricos: Fundamentos, Aplicações e Desafios

Eduardo Cerqueira, Paulo Resque, Iago Medeiros, Lucas Bastos,
Alex Santos, Thais Tavares, Denis Rosário, Aldri Santos e Michele Nogueira

Abstract

Our systems and data (e.g., websites, smartphones, safes, cars, banks, airports) are protected by traditional authentication methods. However, the growing concern about information security and the deployment of smart cities are demanding efforts to find solutions that prevent theft, loss, unauthorized copy, or the forgery of keys, tokens, and passwords. The Internet of Things (IoT) enabled a large increase of personal data collected and published in the Internet. In this context, biometric authentication has earned more and more place as a security solution because they demand, in general, physical presence, vitality, and they are hard to falsify. Among the biometric signals used in academic or commercial products, we mention: iris, face, the palm of hand, fingerprints, walking, voice, electrocardiogram (ECG), electroencephalogram (EEG), and photoplethysmogram (PPG). This chapter brings the state-of-the-art about the use of several biometric signals in an authentication system, contextualizing the applications already developed and the challenges they faced when coexisting with Smart Cities and the Internet of Things. Each type of biometric signal has its own challenges for data acquisition, cost, feature selection, and method to implement the classification. In addition, this chapter presents a review of the machine learning techniques used in biometric systems. The proper choice of the identification technique and classification directly influences results, costs and also the required amount of input data, and the quality of the captured data.

Resumo

Nossos sistemas e dados (ex. websites, smartphones, cofres, carros, bancos, aeroportos) ainda são protegidos por métodos tradicionais de autenticação. Porém, a crescente preocupação com a segurança da informação e a implantação de cidades inteligentes vêm exigindo esforços para encontrar soluções que evitem o roubo, perda, cópia ou falsificação da chaves, tokens ou senhas. A IoT possibilitou um grande aumento na quantidade de dados pessoais coletados e publicáveis na Internet. Nesse contexto, os sistemas biométricos têm ganhado cada vez mais espaço como solução de segurança por exigir a presença física, vitalidade, ser de difícil falsificação. Dentre os sinais biométricos utilizados na academia ou em produtos comerciais citamos: a íris, a face, a palma da mão, as digitais, o padrão no modo de andar, a voz, ECG, EEG e PPG.

Este capítulo traz o estado da arte sobre a utilização de diversos sinais biométricos em sistemas de autenticação, contextualizando as aplicações já desenvolvidas e os desafios que enfrentaram ao coexistirem com Cidades Inteligentes e a Internet das Coisas (IoT). Cada tipo de sinal biométrico tem seus desafios quanto a aquisição de dados, o custo, a seleção de características e o método de implementar a classificação. Além disso, este capítulo também apresenta uma revisão das técnicas de aprendizado de máquina utilizadas em sistemas de biometria. A escolha adequada da técnica de identificação de padrões e classificação influencia diretamente os resultados obtidos, os custos e também os requisitos da quantidade de dados de entrada e qualidade dos dados capturados.

4.1. Introdução: a IoT e a expansão da biometria

Atualmente, a Internet das Coisas (IoT) está presente na vida cotidiana da maioria das pessoas nas grandes cidades. Quase todos os lugares já possuem dispositivos inteligentes. Por exemplo, sensores em edifícios e em veículos e alguns itens embarcados em sistemas eletrônicos com conexões entre si ou com a Internet, permitindo, assim, a coleta e o compartilhamento de dados [Dhanvijay and Patil 2019]. A IoT permite que mais objetos sejam controlados e os dados sejam sensoreados remotamente através de uma infraestrutura de rede preexistente. Isto permite que haja maior interação de sistemas computacionais com o mundo real, aumentando, assim, a eficiência em serviços nas cidades inteligentes. Hoje em dia esses serviços estão geralmente ligados ao transporte, à segurança e ao lazer da população, proporcionando o uso mais eficiente de recursos públicos e melhorando a qualidade de vida da população.

A globalização e a redução no custo de produção de dispositivos eletrônicos contribuíram para a expansão da IoT, a qual passou a oferecer tecnologia para países em desenvolvimento na Ásia e na África, e o acesso à rede mundial de computadores (Internet). Diferentes instituições têm feito previsões para o lançamento e a implantação de produtos e serviços de IoT [Columbus 2018]. Os gastos com estes produtos atingirão a marca de 1 trilhão de dólares em 2022 e está em forte expansão, principalmente em países em desenvolvimento e com grande população, como a China e a Índia. Para a [Ericsson 2018], a estimativa é de que haja 3,5 bilhões de dispositivos com rede celular em 2023, como observado na Figura 4.1. Ou seja, uma taxa de crescimento de 27% por ano. A *DBS Asian Insights* acredita que o setor atinja apenas 20% do seu potencial de aplicações em 2019, abrindo caminho para a Inteligência Artificial (IA) e para a Realidade Aumentada.

Contudo, as pesquisas mostram que existem barreiras para a implantação de serviços de IoT. [Bosche et al. 2018] realizaram um *survey* em 2016, e o refizeram em 2018, buscando avaliar a percepção de diversos *players* do mercado em relação às implantações em IoT. Através desses levantamentos, os pesquisadores constataram que as novas tecnologias de virtualização como *Microsoft Azure* e AWS têm possibilitado a expansão de serviços em IoT. Porém, as preocupações com os aspectos de segurança ainda estão entre as maiores barreiras para a adoção de soluções, como ilustra a Figura 4.2. Diferentes aplicações possuem requisitos específicos de segurança computacional. Os sistemas biométricos surgem como uma excelente solução para quando for necessário que haja acesso físico direto, podendo oferecer uma solução escalável com a IoT, protegendo-a de acesso sem autorização, de troca de identidades ou evitando a checagem manual de credenciais, por exemplo. Os sistemas biométricos podem reconhecer indivíduos com base

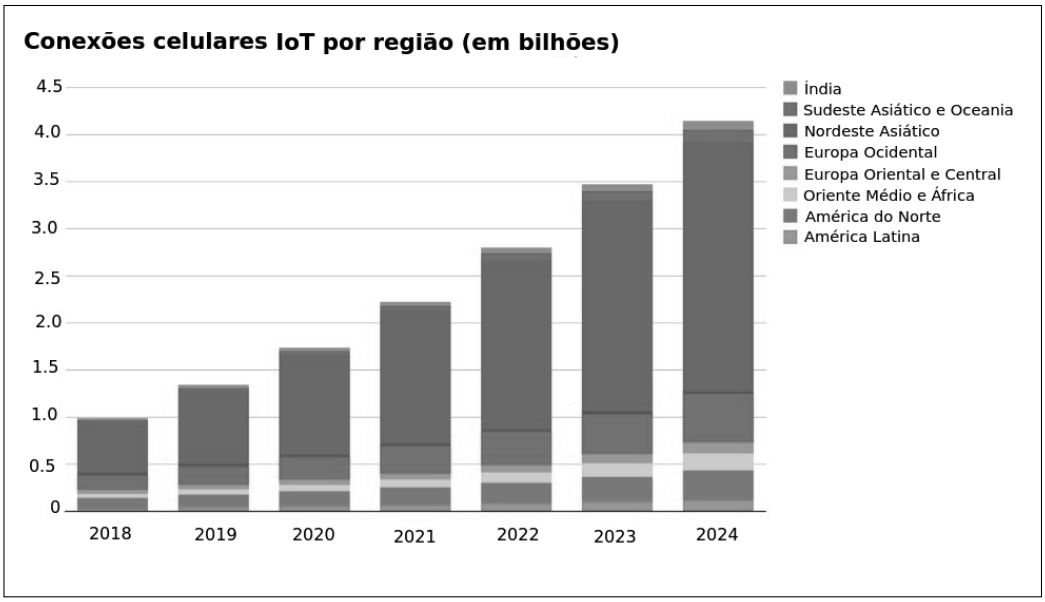

Figura 4.1: Projeção da quantidade de dispositivos IoT conectados (Adaptado de [Ericsson 2018])

em seu comportamento ou suas características biológicas. No *survey*, os consumidores afirmam que comprariam mais dispositivos de IoT e estariam dispostos a pagar um valor até 22% mais caro caso entendessem que as vulnerabilidades de segurança foram tratadas. O potencial para a IoT é imenso e está presente em diversos domínios como *healthcare*, sistemas de transporte, monitoramento ambiental, cidades inteligentes, controle industrial e outros, ainda mais quando a associamos com o aumento de vazão e redução de latência esperados com as tecnologias de 5G.

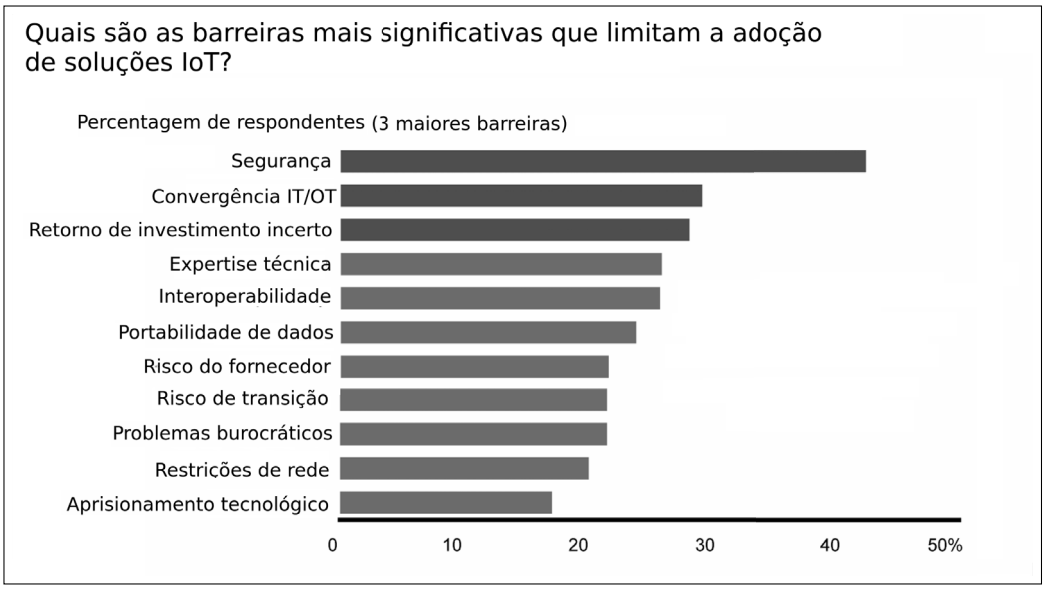

Figura 4.2: Barreiras para a adoção de IoT (Adaptado de [Bosche et al. 2018])

Esses fatores têm motivado pesquisadores a buscar por soluções para fornecer

segurança dos dados ao transmitir informações de saúde através de múltiplos sensores. Um dos desafios consiste em como restringir o acesso aos dados e serviços apenas a usuários autorizados, visto que este controle passa pela autenticação da identidade do usuário. Na sociedade moderna, garantir a correta identificação de um indivíduo tornou-se um requisito essencial para aplicações de tempo real. As aplicações vão desde investigação forense, controle de imigração, transações financeiras e segurança computacional. Nesse contexto, os dispositivos móveis possuem um papel importante na vida cotidiana, não somente pela comunicação mas também pelo entretenimento e pelas relações sociais. É preciso proteger dados bancários, *emails*, fotografias, vídeos e diversos outros dados confidenciais.

Com o aumento de dispositivos conectados à rede, o escopo por potenciais ataques *hackers* ou outros crimes cibernéticos também aumentou. Há o risco de utilização de dispositivos controlados remotamente para ataques de *botnet*, onde milhares de dispositivos podem ser utilizados em conjunto para um ataque em rede. Os ataques clássicos de *Man-in-the-middle*, no qual o invasor faz de forma transparente o intermédio na comunicação entre dois dispositivos, podem enviar informações falsas ou coletar informações sensíveis. Houve um aumento de ocorrência no roubo de dados e de identidades, quando o usuário utiliza de modo descuidado os dispositivos, como telefones celulares, *smartwatches* e outros. O acúmulo de muitas informações em dispositivos pessoais deixa as pessoas vulneráveis a grandes impactos caso esses dados sejam violados. Assim, garantir a segurança desses dados somente com o uso de senhas não tem sido mais suficiente frente aos ataques possíveis. Essa necessidade crescente por proteção dos dados sensíveis fez com que a busca por soluções mais seguras aumentasse, com destaque maior para a biometria. Os sistemas de segurança biométrica podem substituir métodos tradicionais que utilizam senhas ou PINs gestuais na tela do dispositivo. Os métodos embarcados em *smartphones* são reconhecimento por digitais, por face, assinatura, de voz e por íris.

O escaneamento de digitais começou a se popularizar em 2013 com a chegada do *iPhone 5S*. Inicialmente, os usuários podiam registrar suas digitais para desbloquear o *iPhone*, depois passaram a utilizar a digital para autenticar o processamento de compras através do sistema de pagamento *Apple Pay*. Três anos depois, grande parte dos *smartphones* modernos já possuíam sensores de digitais como o *iPhone* 8 e 8 *Plus*, *Samsung Galaxy* S8 e *Galaxy Note* 8, LG G6 e V30, *Huawei Mate* 10, *Google Pixel* 2 e *Pixel* 2 XL, *OnePlus* 5 e 5T, além de muitos outros. Em poucos anos os aparelhos celulares incorporaram a biometria, o que até então parecia um recurso de filmes de ficção científica.

Atualmente, os dispositivos vestíveis podem medir sinais biométricos vitais e não vitais, tais como temperatura corporal, frequência cardíaca, pressão arterial, eletromiograma (EMG), eletrocardiograma (ECG), fotopletismograma (PPG), frequência respiratória, dentre outros sinais. Nesse contexto, a biometria refere-se a tecnologias usadas para medir características físicas ou comportamentais humanas, tais como as fornecidas pela íris, face, impressões digitais, retina, geometria da mão, voz ou assinaturas para detectar e reconhecer indivíduos. Por exemplo, os dispositivos vestíveis no antebraço podem obter sinais de ECG/PPG, processá-lo para extrair as características que identifiquem o usuário e utilizar tal informação tanto para identificação quanto para autenticação.

De um modo geral, estes diferentes sinais vitais ou não vitais são processados em um sistema biométrico em duas etapas: a primeira ligada a captura dos dados e outra ligada

ao reconhecimento. Na etapa de captura, o sistema biométrico coleta o traço biométrico e extrai um conjunto de *features* (características) relevantes e armazena o modelo desses dados extraídos em um *database* (banco de dados). Na etapa de reconhecimento, o sistema captura novamente o traço biométrico de um indivíduo, extrai as características desse sinal e compara esse conjunto de características com os padrões armazenados no banco de dados de modo que possa afirmar de quem é a identidade.

O objetivo deste capítulo que documenta o conteúdo dessa Jornada de Atualização em Informática (JAI) é possibilitar uma revisão do estado arte da utilização de diversos sinais biométricos em sistema de autenticação e suas aplicações. São enfatizadas as particularidades de cada sinal biométrico em termos de acurácia e características utilizadas para identificação de indivíduos. Além do mais, será apresentado ao leitor o conhecimento das diversas técnicas de aprendizado de máquina que usualmente são usadas em sistemas biométricos. Com o conhecimento das características de cada sinal e das técnicas de inteligência computacional existente, o leitor pode aplicar esse conhecimento em base de dados de repositórios públicos disponíveis para estudo.

O restante deste capítulo do JAI está organizado da seguinte forma. A Seção 4.2 apresenta a evolução histórica do uso de biometria e as aplicações de segurança já utilizadas. A Seção 4.3 trata dos aspectos técnicos para a coleta das características únicas de um sinal biométrico. Essa extração de características é essencial para um sistema eficiente de biometria. A Seção 4.4 apresenta as tecnologias de aprendizado de máquina utilizadas comumente em sistemas biométricos. Na Seção 4.5, apresentamos uma breve parte prática com a indicação de bases de dados públicas e avaliações de técnicas de aprendizado de máquina para sistemas biométricos. Na Seção 4.6, são apresentadas as conclusões e oportunidades de pesquisa para o tema.

4.2. Sinais Vitais e Segurança: Evolução Histórica

Diversas evidências mostram que a biometria já vem sendo utilizada desde o mundo antigo por diversas sociedades. Na Babilônia em 1900 A.C. [Daluz 2014], as digitais eram utilizadas em contratos para dar validade aos mesmos. Porém, foram os chineses que aproveitaram melhor o potencial da biometria, utilizando as digitais dos dedos para uma variedade de funcionalidades, incluindo desde registro da população e em cenas de crimes até para validar documentos importantes utilizando as digitais de um lado e um selo oficial do outro lado em documentos para casamento, divórcio, registros do exército e outros. Isso ocorria pois o domínio da escrita era restrita a uma parcela bem pequena da população. Até hoje, a digital é utilizada em documentos em casos que a pessoa não sabe ou não pode assinar. Apesar de ter surgido há tanto tempo, somente em 1901, foi fundado o primeiro escritório de investigação de digitais, a polícia da Inglaterra, conhecida como *Scotland Yard* que foi o primeiro órgão de investigação oficial a ter um departamento dedicado para digitais. Depois disso, a utilização de digitais começou a se espalhar pelas polícias do mundo todo. Nessa época, o reconhecimento através de digitais não era automático, pois era um trabalho complicado, manual e demorado. Além dessas dificuldades, a quantidade de registros ainda era pequena.

A primeira publicação científica sobre o reconhecimento automático biométrico foi realizada por Mitchell Trauring na revista científica *Nature* em 1963 sobre a corres-

pondência entre digitais do dedo [Trauring 1963]. O desenvolvimento de sistemas automatizados baseados em outros traços como voz [Pruzansky 1963], rosto [Bledsoe 1966] e assinatura [Mauceri 1965] também começaram por volta dos anos 60. Somente depois surgiram os sistemas baseados em geometria da mão e íris, assim, a biometria vem evoluindo nos últimos 50 anos. Há uma citação interessante publicada em [Wayman 2007], onde foi feita uma análise dos avanços da biometria entre 1960 e os anos 1990: *"A quick overview of biometric history shows that much of what we consider to be "new" in biometrics was really considered decades ago."* Novas soluções biométricas, que chegaram recentemente a produtos cotidianos, já vinham sendo estudados há muitos anos.

Saindo no mundo forense e judicial, o uso de biometria de digitais chegou ao dia a dia da população através dos celulares e se expandiu por outros setores como segurança predial e serviços médicos, de modo a prover maior segurança e praticidade na identificação dos usuários. Outros tipos, como o reconhecimento facial, só começaram a se popularizar recentemente. O primeiro dispositivo foi lançado em 2011 pela empresa *Google*, o *Galaxy Nexus*, porém naquela época o sistema não se mostrou muito eficaz, ainda necessitando de melhorias. O sistema melhorou a partir do *Galaxy* S8 e teve novo salto com o lançamento do *Iphone* X, no qual o usuário precisava apenas registrar o rosto no celular e depois conseguia acesso instantâneo à tela inicial ou outros serviços que antes eram realizados através de senhas. Ainda hoje, há a necessidade de evolução dos sistemas baseados na face utilizados por muitos celulares devido à qualidade dos sensores ou ao processamento utilizado. Ou seja, ainda é um campo aberto para pesquisa assim como toda a biometria.

Devido a diferentes níveis de segurança ao usar senhas, digitais e o rosto, vários aparelhos celulares utilizam mais de uma opção de biometria. Vinculando o reconhecimento facial para desbloquear o dispositivo e a digital para autorizar uma compra de algum produto/serviço. Além do *Iphone* X, outros dispositivos já utilizam o reconhecimento facial, *Galaxy* S8, *Galaxy Note* 8, LG V30, *OnePlus* 5T, HTC U11, *Huawei* P10, *Moto* G5, *Xiaomi Mi* 6 e *Xiaomi Mi* MIX 2 [Insider 2019]. O escaneamento de íris está mais presente em dispositivos lançados na Ásia, como o *Fujitsu* NX F-04G e *Microsoft Lumia* 950, ambos lançados em 2015. A *Samsung* inclui a funcionalidade no *Galaxy* S8 e *Galaxy Note* 8 lançado em 2017. Assim como o reconhecimento facial, o reconhecimento de íris não atingiu ainda um grau de confiabilidade alto suficiente para ser utilizado em meios de pagamento, por exemplo, sendo utilizada geralmente como um recurso para desbloqueio de tela e diversificação para o usuário. Nesses cenários, o usuário sempre precisa manter uma senha ou desenho padrão como medida de segurança de *backup* em caso de falha de uma das opções biométricas. O reconhecimento de voz ainda não apareceu como uma opção disponível em *smartphones*, apesar das grande marcas como *Apple*, *Google*, *Amazon* e *Microsoft* estarem investindo bastante em soluções com assistentes inteligentes de processamento de voz. Por outro lado, a biometria entrou no imaginário da população através dos filmes de ficção científica, apesar de alguns exageros e previsões que não se concretizaram, grande parte das projeções cinematográficas foram criadas baseadas de trabalhos em andamento pela comunidade científica da época. A Figura 4.3 traz uma linha do tempo do desenvolvimento da biometria até 2014.

Atualmente, os dispositivos vestíveis podem medir sinais biométricos vitais e não vitais, tais como temperatura corporal, frequência cardíaca, pressão arterial, ECG, EMG, frequência respiratória, dentre outras informações. Nesse contexto, a biometria refere-se

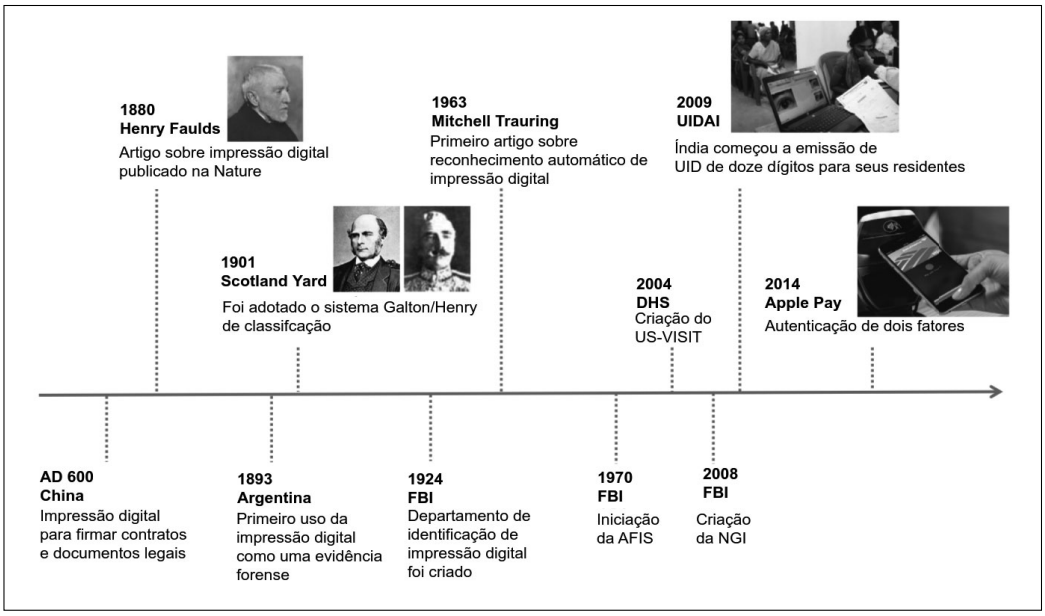

Figura 4.3: Linha do tempo das aplicações com biometria

às tecnologias usadas para medir características físicas ou comportamentais humanas, tais como as fornecidas pela íris, face, impressões digitais, retina, geometria da mão, voz ou assinaturas para detectar e reconhecer indivíduos. A biometria fornece não apenas uma alternativa para IDs ou números PIN (esquemas baseados em conhecimento) para autenticar alguém em um sistema, mas também um método de autenticação contínua. Além disso, ela possui vantagens relacionadas à clonagem, perda de dispositivos e adivinhação de senhas. Embora a biometria possa reduzir limitações de segurança associadas a senhas, os sistemas biométricos também são vulneráveis a ataques de falsificação, ataques de vinculação equivocada de usuários (ou seja, quando um impostor tenta se passar por outro usuário), além de possivelmente aumentar os custos com *hardware* e *software* comparado com o uso de senha ou *token* [Jain et al. 2016]. Mesmo a identificação facial, a qual passou a ser utilizada recentemente em dispositivos móveis, possui riscos associados a falta de confidencialidade, com o uso de imagens publicadas na Internet em sistemas que usam as imagens da face, além das limitações na distinção de gêmeos legítimos. Por esses motivos, julga-se importante a avaliação dos diversos tipos de biometrias existentes, onde a combinação entre elas e o uso adicional de senhas tradicionais seja a solução adotada pela maioria dos sistemas no futuro.

Para entender o papel da biometria e do uso de sinais vitais para aplicações de segurança, é necessário visualizar como a estrutura típica de um sistema de segurança e/ou autenticação baseado em biometria. A Figura 4.4 apresenta aspectos interessantes de um sistema típico de autenticação. Um sistema típico de biometria possui dois estágios de operação, um estágio ligado a captura dos dados e outro ligado ao reconhecimento. Na etapa de captura, o sistema biométrico coleta o traço biométrico e extrai um conjunto de *features* (características) relevantes, armazena um modelo desses dados extraídos em um banco de dados (normalmente é referido como *template*/padrões), e assim consegue associar esses dados coletados a um indivíduo. Na etapa de reconhecimento, o sistema

captura novamente o traço biométrico de um indivíduo, extrai as características desse sinal e compara esse conjunto de características com os padrões armazenados no *database* (banco de dados) de modo que possa afirmar se a identidade é aquela reivindicada ou não.

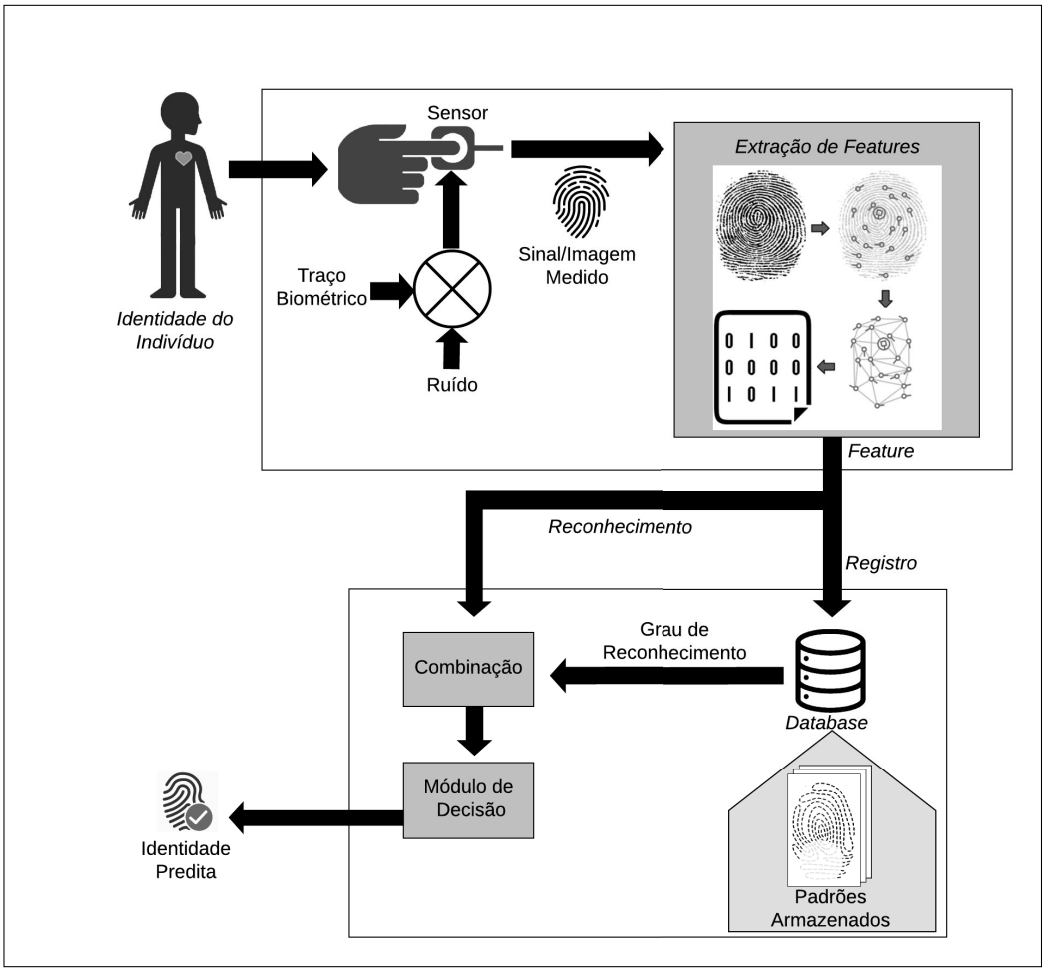

Figura 4.4: Um típico sistema de biometria

4.3. Extração de *features* dos sinais biométricos

Os sinais biométricos, tais como EMG, ECG, PPG e outros, desempenham um papel crucial na autenticação, fornecendo características individuais como uma forma de controle de acesso e identificação de seres humanos por suas características, tais como sinais vitais. Portanto, é necessário considerar técnicas exclusivas de extração de características para sinais biométricos adquiridos de dispositivos vestíveis. Por exemplo, os dispositivos vestíveis obtêm sinais de ECG/PPG, processam os para extrair as características que identifiquem o usuário e utilizam tal informação para identificação e autenticação.

Um sistema típico de biometria possui duas fases de operação: (i) a inscrição ou registro do indivíduo e (ii) o reconhecimento. A primeira fase coleta os sinais biométricos dos indivíduos. Assim, nessa fase, é extraído um conjunto de características relevantes e armazenadas em um banco de dados como um *template*, de modo a associar àquelas características a um usuário ou indivíduo. Na segunda fase, o sistema captura a carac-

terística novamente do indivíduo e a compara aos dados armazenados; através do uso de diversas técnicas de aprendizado de máquina o sistema responde se os dados coletados são do indivíduo alvo ou não.

Teoricamente, qualquer sinal anatômico, comportamental ou fisiológico de um indivíduo pode ser usado como um marcador biométrico. Contudo, a escolha de qual marcador utilizar depende dos requisitos da aplicação e do grau de algumas propriedades a serem satisfeitas: (i) exclusividade ou distinção, (ii) durabilidade, (iii) universalidade, (iv) coleta, (v) desempenho, (vi) aceitação do usuário, (vii) invulnerabilidade e $(viii)$ integração. A Figura 4.5 apresenta as principais características humanas usadas em identificação biométrica. Nas próximas subseções, serão descritos os aspectos técnicos da extração de *features* de sinais biométricos.

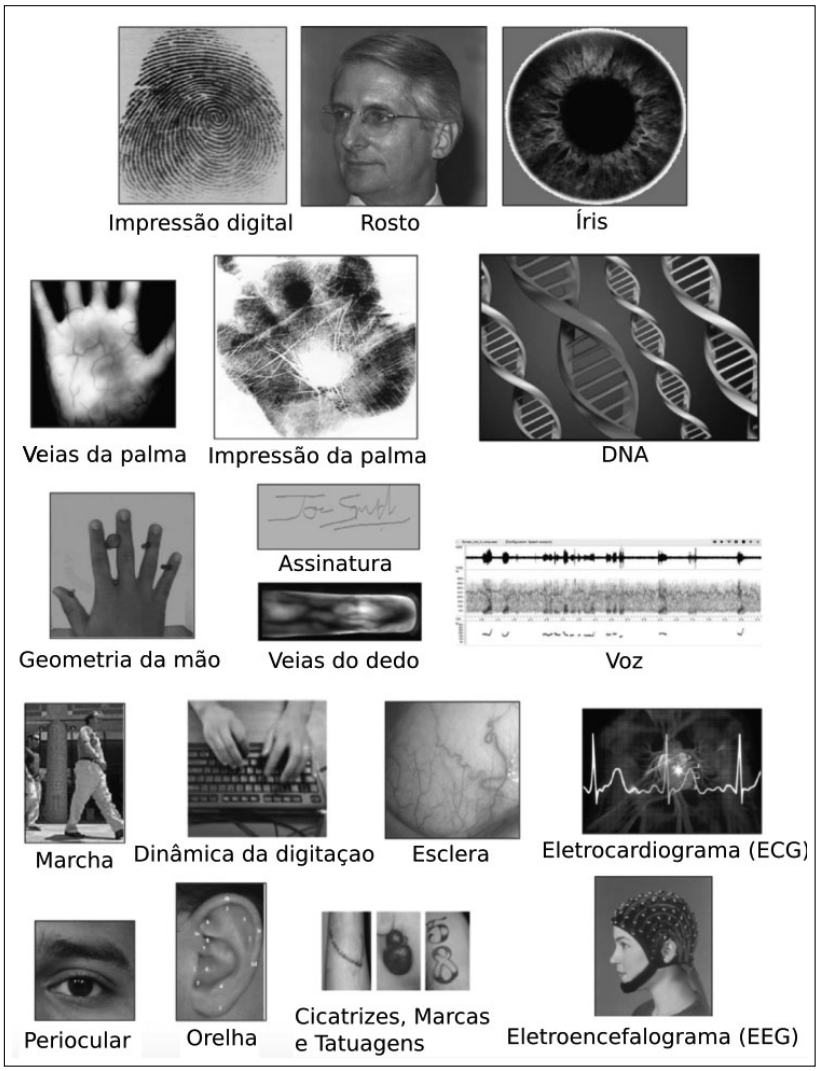

Figura 4.5: Características mais utilizadas em sistemas de identificação biométrica

4.3.1. *Features* consideradas no reconhecimento de mãos

A impressão digital é uma informação humana usada como biometria. Porém, há vários atributos, além das impressões digitais, que foram identificados e testados, tais como

palmprint (impressão da palma), geometria da mão, impressão das juntas dos dedos, região abaixo das unhas e o padrão das veias da mão (Figura 4.6). No entanto, os atributos baseados em mão são uma extensão da tecnologia de impressão digital [Unar et al. 2014].

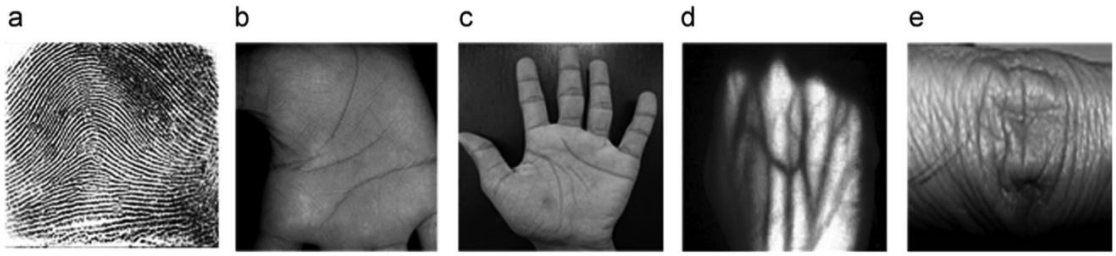

Figura 4.6: Modalidades das regiões da mão: (a) impressão digital (b) impressão da palma, (c) geometria da mão, (d) padrão das veias da mão, (e) articulação dos dedos (Adaptado de [Unar et al. 2014])

O sistema de reconhecimento de impressão digital caracteriza as texturas de cumes e sulcos (linhas) presentes nas pontas dos dedos. As linhas são quase paralelas, com exceção de alterações do padrão, chamadas de minúcias. Existem categorias para estes pontos característicos (minúcias), como arco, presilha interna, presilha externa e verticilo [Liu 2010]. Individualmente, os pontos de minúcia executam a tarefa de reconhecimento. Como todos os outros sistemas biométricos, um módulo de aquisição captura as pontas dos dedos, de preferência, a partir de imagens de alta resolução e o sistema extrai os sulcos, alguns pontos singulares e pontos de minúcia. A Figura 4.7 mostra o processo de extração de *features* para a impressão digital, onde são detalhados a coleta, o mapeamento e o registro das informações, como dados a serem inseridos no *database* para reconhecimento. Outros sistemas, como os baseados na geometria da mão, conseguem trabalhar com imagens de baixa qualidade, capturando as linhas principais, rugas e textura.

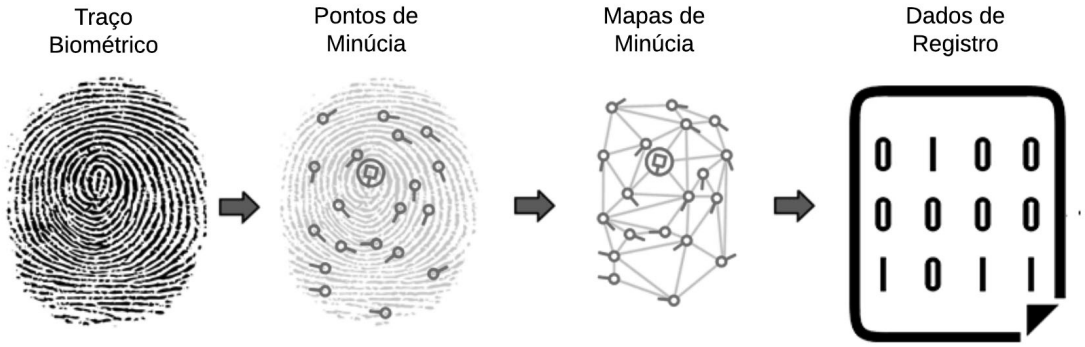

Figura 4.7: Identificando pontos de minúcia

Estes métodos de aquisição de imagens utilizados nas modalidades baseadas das mãos usam dados de sensores ópticos, térmicos, de silício ou imagens de ultrassom.

Devido à redução do custo dos sensores de imagem, assim como o pequeno tamanho para guardar o *template*, torna os atributos da região da mão como uma boa opção para muitos tipos de aplicações, em comparação com assinaturas biométricas mais complexas. No entanto, a biometria manual tem desafios. As imagens distorcidas, o contato físico com o dispositivo de imagem, a necessidade de cooperação do usuário, doenças da mão (artrite), contaminantes naturais para a imagem (como células mortas, cicatrizes, cortes, pele úmida e/ou seca), e sensores de imagens com superfícies sujas ou oleosas que comprometem a eficácia do sistema. Outros fatores também influenciam a precisão da mão.

A presença de usuários não treinados e não cooperativos colocando de forma imprópria o polegar no sensor, como apontado por [Jain and Duta 1999], [Ross et al. 1999], pode prejudicar o reconhecimento [Kukula and Elliott 2006]. Dedos pequenos também são mais complicados para reconhecimento. É importante notar que a mão humana é um objeto flexível e sua silhueta pode sofrer deformações não lineares que dificultam o processo de captura e reconhecimento de mão. Como exemplo, temos o dedo do polegar que se deforma mais do que outros quatro dedos. Assim, excluir o dedo polegar do cálculo do vetor de recursos resolve esse problema [Duta 2009]. Mesmo assim, [Chen et al. 2005] mostrou que os sistemas de formas manuais são vulneráveis a ataques de falsificação.

Alguns trabalhos encontrados na literatura abordam técnicas de *Deep Learning* para realizar o reconhecimento de mãos, principalmente envolvendo impressões digitais e impressão de veias da palma. [Sajjad et al. 2018] propuseram uma nova técnica híbrida, composta por reconhecimento das mãos e o reconhecimento facial, que garante a autenticidade do usuário ao sistema. Uma das duas etapas do esquema proposto testa os dados biométricos coletados em modelos baseados em Redes Neurais Convolucionais (*Convolutional Neural Networks* - CNN) para detectar um possível *spoofing* (falsificação) desses dados. Caso não seja atestado fraude, o sistema realiza a autenticação do usuário. Para impressões digitais coletadas com baixa qualidade, [Wang et al. 2016] propuseram um algoritmo de reconhecimento dessas impressões, melhorando sua qualidade a partir de pontos de *features*. Este algoritmo também é baseado em CNN e sua taxa de reconhecimento é comparada com a taxa de reconhecimento baseada na Análise de Componentes Principais e *k-Nearest Neighbor* (k-NN). Outra abordagem de *Deep Learning* para melhorar o desempenho de sistemas de identificação por impressão digital foi proposta por [Su et al. 2017]. Essa abordagem consiste na detecção de poros na pele através da capacidade de classificação e aprendizado de *features* das CNNs. A fim de aumentar a robustez contra os materiais falsificados, [Zhang et al. 2016] propuseram um novo método de detecção de impressão digital 2D, principalmente para *smartphones*, combinando CNNs com dois descritores locais (Padrão Binário Local e Quantização de Fase Local). Por fim, [Jung and Heo 2018] introduziram uma nova arquitetura de CNNs para o problema de detecção de vivacidade das impressões digitais, a qual pode fornecer uma estrutura mais robusta para treinamento e detecção de redes do que os métodos anteriores. A proposta permite controlar o nível aceitável de falsos positivos ou falsos negativos das impressões digitais coletadas.

4.3.2. *Features* consideradas no reconhecimento ocular

Para o reconhecimento ocular, três modalidades foram as mais utilizadas ao longo da história e estão ilustradas na Figura 4.8. Modalidades de região ocular como retina, íris

e padrão das veia da esclera, ganharam considerável atenção de pesquisadores devido a região ocular possuir sinais mais precisos, altamente confiáveis, bem protegidos, estável e quase impossíveis de forjar assinaturas biométricas [Oinonen et al. 2010]. Um sistema de identificação da retina leva conta a estrutura única e invariante de veias sanguíneas presentes na retina humana para estabelecer a identidade. O processo de escaneamento captura algumas *features* relacionadas às marcas (como posição e bifurcações dos vasos sanguíneos) ou medidas da área de referência (fóvea ou o disco ótico).

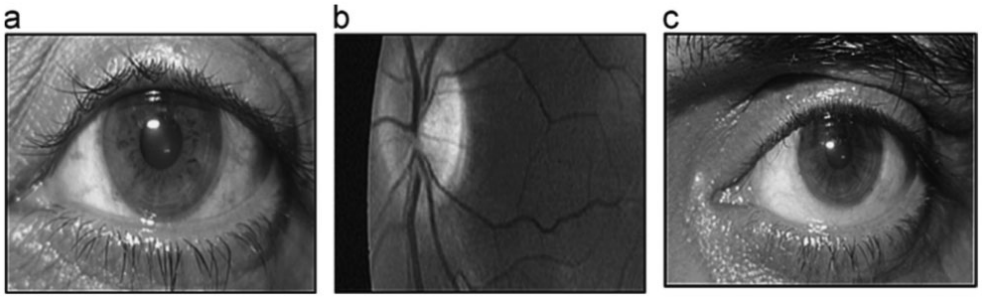

Figura 4.8: Modalidades da região ocular: (a) íris, (b) retina, (c) esclera (Adaptado de [Unar et al. 2014])

Já um sistema de identificação baseado em escleras considera o padrão vascular dos vasos sanguíneos presentes na região da esclera do olho humano [Lumini and Nanni 2017]. O sistema baseado em íris cria um modelo usando os padrões únicos presentes na íris como as criptas, linhas radiais, área da pupila, área ciliar e anel limite [Daugman 2010]. Foram propostos modelos onde tanto as cores quanto as formas eram utilizadas para distinguir as pessoas. Apesar das primeiras propostas de utilização da íris terem iniciado em 1936 com Frank Burch, o primeiro sistema completo foi implementado somente no início dos anos 1990 com uma câmera para capturar a imagem da íris, algoritmos para processar as imagens e retirar a região da íris e código de representação da íris capaz de convertê-la em um código binário compacto. Ou seja, cada íris de um indivíduo era convertido para uma espécie de *hash* e utilizado a distribuição de distâncias *hamming* para classificá-las.

Recentemente, as técnicas de *Deep Learning*, especialmente utilizando CNNs, têm mostrado grande potencial para a classificação de imagens. O primeiro trabalho aplicando *Deep Learning* ao reconhecimento de íris foi o *framework* DeepIris, proposto por [Liu et al. 2016], o qual reconhece íris heterogêneas, das quais as imagens foram obtidas com diferentes tipos de sensores, e estabelece a similaridade entre um par de imagens de íris usando CNNs. [Gangwar and Joshi 2016] também desenvolveram um aplicativo para o reconhecimento da íris em imagens obtidas de diferentes sensores, chamado DeepIrisNet, através de CNN. Além disso, duas arquiteturas da CNN foram apresentadas, a saber, DeepIrisNet-A e DeepIrisNet- B, sendo a primeira baseada em camadas convolucionais padrão, e a segunda baseada em camadas de iniciação [Szegedy et al. 2015].

Outras abordagens propostas como [Al-Waisy et al. 2018] utilizaram um sistema multi-biométrico, usando as íris esquerda e direita de uma pessoa. Experimentos foram realizados em bancos de dados de imagens NIR (próximo ao infravermelho) obtidos em ambientes controlados. O processo tem cinco etapas: detecção de íris, normalização de íris, extração de *features*, correspondência com *Deep Learning* e, finalmente, a fusão de escores

correspondentes de cada íris. Durante a fase de treinamento, os autores aplicaram diferentes configurações e arquiteturas da CNN e escolheram a melhor com base nos resultados do conjunto de validação. [Nguyen et al. 2017] demonstraram que os descritores genéricos usando *Deep Learning* são capazes de representar as características da íris. Uma descrição desse sistema pode ser visualizada na Figura 4.9.

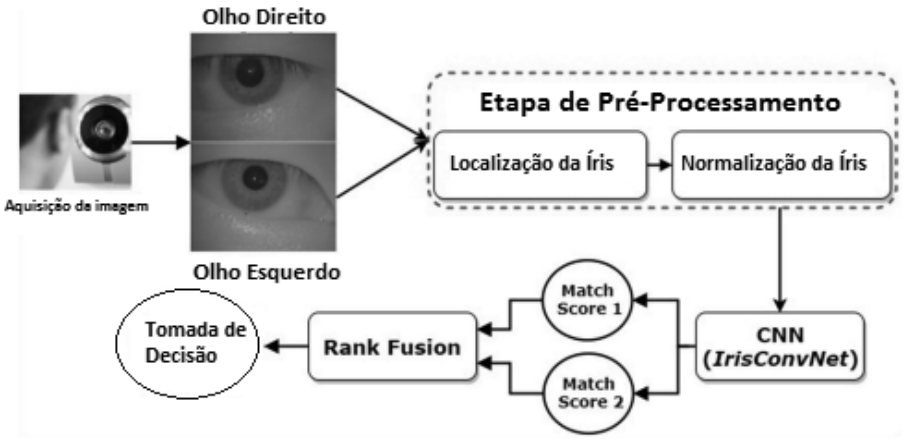

Figura 4.9: Esquema de Identificação utilizando CNN e Íris dos olhos Direito e Esquerdo (Adaptado de [Al-Waisy et al. 2018])

De um modo geral, os trabalhos de reconhecimento de íris utilizam uma imagem de entrada que passa por um processo de normalização, localização da íris e segmentação antes de ser utilizada em uma técnica de inteligência computacional. Todas essas abordagens têm limitações práticas. Por exemplo, o padrão vascular da retina só pode ser visto expondo o olho humano a uma luz infravermelha, enquanto a textura da íris pode ser adquirida através da iluminação do olho humano com uma luz perto da infravermelha ou luz de comprimento de onda invisível [Daugman 2010]. A íris se torna uma abordagem promissora em assinaturas biométricas oculares devido a sua aquisição de imagens menos invasiva. As modalidades da região ocular exigem um alto grau de cooperação por parte dos sensores médicos/químicos, o alto custo de sensores de imagem, e reflexões de fontes de luz ambiente. Esses requisitos eventualmente limitam a sua utilização em ambientes industriais ou a sua utilização em dispositivos com limitações de recursos.

4.3.3. *Features* consideradas no reconhecimento facial

O reconhecimento facial humano é uma técnica bem conhecida, já que o rosto humano é o mais natural traço biométrico usado para reconhecer indivíduos por séculos. Um sistema de reconhecimento facial leva em conta algumas características/*features*, como distância entre os olhos, boca, lado do nariz, imagem da face inteira, pontos de canto, contornos, pelos faciais, redondeza de face, etc [Unar et al. 2014]. Mesmo com muitos recursos disponíveis, esses sistemas não garantem uma identificação confiável na presença de alguns artefatos, como o uso de cirurgias plásticas, sendo necessários alguns novos algoritmos para mapear essas possíveis alterações. Por exemplo, o sistema deve estar preparado para reduzir o impacto das mudanças pessoais ao longo do tempo sobre a

precisão de tais sistemas. A comunidade de pesquisa propôs a ideia de reconhecimento humano baseado em termografia facial com objetivo de fornecer um sistema robusto de reconhecimento de face. A Figura 4.10 mostra as modalidades faciais e de termografia facial usadas para identificar os indivíduos.

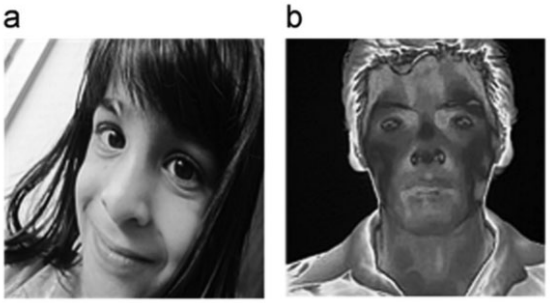

Figura 4.10: Modalidades na região facial: (a) face, (b) termografia facial (Adaptado de [Unar et al. 2014])

A estrutura não linear da face humana faz dela um sofisticado problema de reconhecimento de padrões, bem como uma área ativa de pesquisa em aplicações de visão computacional [Abate et al. 2007]. Em relação às medidas de segurança, é necessária a utilização de *features* 3D ao invés de *features* 2D não apenas para melhorar a acurácia e reduzir erros de reconhecimento, mas também para reduzir a possibilidade de falsificação, quando um invasor tenta ser outra pessoa.

Nos últimos anos, as técnicas de rede neural, como *Deep Learning* e CNN, alcançaram bom desempenho em várias tarefas de visão computacional, desde classificação de imagem até a detecção de objetos e segmentação semântica. Ao contrário das abordagens de visão computacional tradicionais, os métodos de *Deep Learning* demonstraram resultados satisfatórios no desafio visual do reconhecimento da grande escala de imagens (ILSVRC) [Krizhevsky et al. 2012]. Juntamente com a popularidade de *Deep Learning* em visão computacional, mais pesquisas estão surgindo para explorar esta técnica na resolução de tarefas de detecção de rostos. Em geral, o reconhecimento facial pode ser considerado como uma tarefa de detecção de objeto de especialidade em visão computacional. [Sun et al. 2018] explora tais técnicas para a detecção facial.

Tendo em vista o crescimento no uso de técnicas de inteligência artificial em reconhecimento facial, várias empresas estão lançando serviços que se beneficiam dessa tecnologia. A China é um país líder nesse setor em várias frentes: seja permitir sacar dinheiro em caixas eletrônicos de bancos sem uso de cartão, fazer compras em lojas de conveniência [Zuo 2019], viajar sem passagem ou identidade em um aeroporto [Kinetz 2019] e outros. Entretanto, alguns atos podem ser considerados duvidosos por partes das autoridades, como cobrar multas para as pessoas que não atravessam na faixa de pedestre e exibir tais pessoas em um mural da vergonha [Baynes 2019], ou guardas usarem *smart glasses* para avaliar quem o sistema considera como infrator [Russel 2019], podendo ser pessoas que realmente cometeram crimes graves como assassinato ou roubo, pessoas que simplesmente atravessaram a rua fora da faixa, ou até mesmo pessoas que foram identificadas erroneamente [Dodds 2019]. Em outros locais, como em Nova Déli, as autoridades conseguiram encontrar crianças desaparecidas ao usar esta tecnologia [Times 2019].

Ainda haverá muitos debates sobre o tema e aplicação consciente do uso de reconhecimento facial, sendo que alguns lugares são mais favoráveis (como em Londres [Wright 2019]) e outros já entraram em processo de banimento (como em San Francisco [Kate Conger 2019]). O uso de reconhecimento facial é uma das técnicas biométricas mais famosas atualmente por estas aplicações. Apesar de polêmico, cabe ao governo, empresas legais e sociedade verem formas de aplicar seu uso de forma benéfica para a população, sem tentar infringir questões de privacidade.

4.3.4. *Features* consideradas em sinais vitais

A Figura 4.11 ilustra os passos para a extração de *features* de sinais vitais encontrados na literatura. A maioria dos sistemas pode ser dividida em cinco etapas principais [Bonissi et al. 2013]: aquisição, pré-processamento do sinal, extração de *features*, correspondência e classificação. Geralmente, os sinais vitais são capturados por um sensor e pré-processados para remoção de ruídos. Em seguida, a detecção de picos do sinal vital é realizada para dividir o sinal em diferentes segmentos (batidas). Depois da segmentação e normalização, aplica-se a extração de *features*. As *features* resultantes são processadas para formar um *template*, o qual é comparado com o *template* de usuários autorizados. Finalmente, a classificação é aplicada para distinguir os dados de sinais vitais genuínos dos dados de sinais vitais impostores [Karimian et al. 2017, Sancho et al. 2018]. Por conta disso, a extração das *features* é a etapa mais importante, pois é quando as características do usuário são extraídas do sinal vital para que o processo de autenticação seja realizado. Na sequência, a extração das *features* de sinais ECG e PPG é descrita em detalhes.

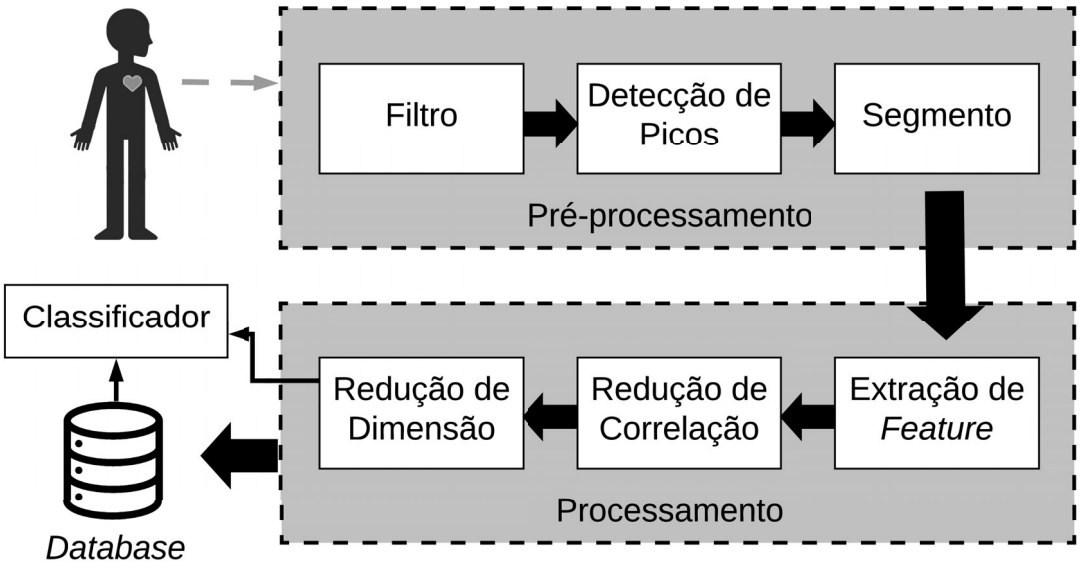

Figura 4.11: Esquema para extração de *features* de sinais vitais (Adaptado de [Karimian et al. 2017])

4.3.4.1. *Features* consideradas para sinais PPG

A fotopletismografia (PPG) é um método eletro-óptico, não invasivo, que mede o volume sanguíneo que flui através da parte do corpo humano em análise (exemplo: pulso, dedo, lóbulos auriculares, etc). Os sinais PPG refletem as ações pulsativas das artérias através da interação entre a hemoglobina oxigenada e os fótons. Acredita-se que cada pessoa tenha uma hemodinâmica e um sistema cardiovascular únicos [Yadav et al. 2018]. Por conta disso, os sinais PPG podem ser utilizados para autenticação biométrica.

Os sinais PPG são registrados através de uma combinação de LED, que emite luminosidade em uma parte do corpo, e Foto-Diodo (PD), que mede a luz absorvida pelos tecidos epiteliais. Esta combinação proporciona maior flexibilidade para o projeto de sistemas de autenticação. As medições indicam as mudanças no volume sanguíneo. Como o registro do PPG requer apenas LED e PD, ele é muito econômico, comparado aos outros traços biométricos. No contexto da biometria médica, o registro do PPG não requer nenhum tipo de gel, estímulo externo ou vários eletrodos e pode ser convenientemente registrado de praticamente qualquer parte do corpo [Yadav et al. 2018, Nakayama et al. 2019].

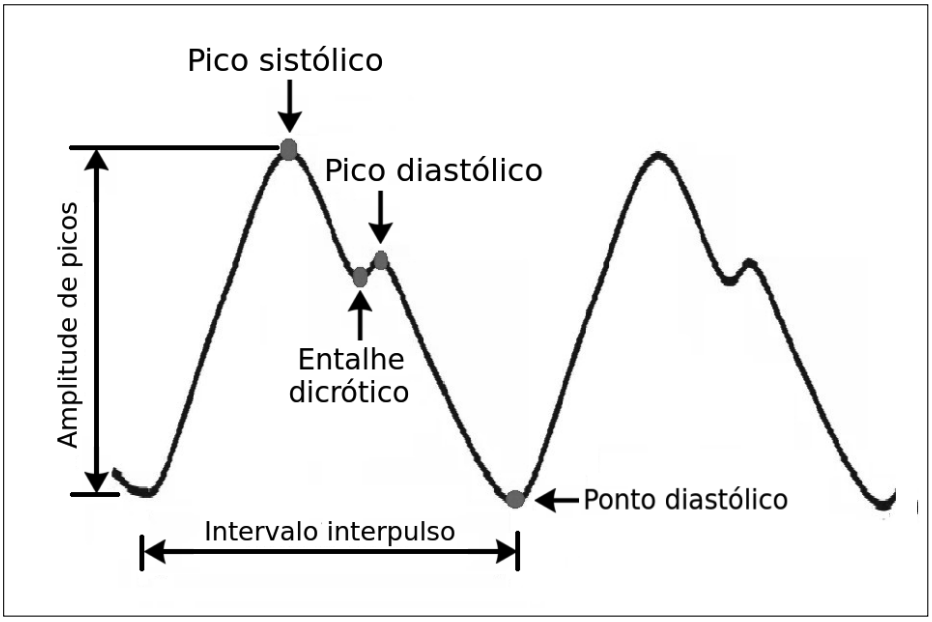

Figura 4.12: Pontos fiduciais de uma amostra de sinal PPG

Muitos trabalhos têm sido desenvolvidos para investigar a viabilidade de se aplicar sinais PPG como identificadores biológicos. Os sinais PPG apresentam pontos fiduciais como características de suas formas de onda. Esses pontos são pico sistólico, pico diastólico, entalhe dicrótico, intervalo interpulso, amplitude de picos, entre outras, como ilustrado na Figura 4.12. Os picos sistólicos representam a pressão sistólica, que é a pressão sanguínea mais alta durante a contração dos ventrículos, quando o coração está bombeando o sangue [Allen 2007]. A pressão sistólica aumenta durante a fase anacrótica do batimento cardíaco[Sarkar et al. 2016]. Os picos diastólicos representam a pressão diastólica, que é a menor pressão registrada pouco antes da próxima contração do coração, quando este está relaxado [Clark and Kruse 1990, Allen 2007]. A pressão diastólica é registrada durante a

fase catacrótica do batimento cardíaco [Sarkar et al. 2016]. Existe mais um ponto fiducial na forma de onda do sinal PPG que é o entalhe dicrótico. Ele consiste em uma ascendência secundária correspondente ao aumento transiente da pressão sanguínea quando a válvula aórtica se fecha [Politi et al. 2016].

As *features* de um sinal PPG podem ser utilizadas para identificar diferentes indivíduos, ao mesmo tempo, similares o suficiente para reconhecer uma mesma pessoa. Os sinais PPG têm diversas vantagens para autenticação de usuários quando comparados com outras abordagens biométricas. Eles possuem baixo custo de desenvolvimento e são acessíveis a várias partes do corpo humano (dedo, lóbulo da orelha, pulso ou braço) [Gu et al. 2003]. Por conta disso, muitos trabalhos concentram-se em pesquisar sobre o uso dos sinais PPG como identificadores biométricos. Muitos deles desenvolveram esquemas para sistemas de autenticação biométrica, como ilustrado na Figura 4.13. Esses esquemas geralmente apresentam as mesmas etapas, que em sua maioria são a aquisição e filtragem do sinal, tratamento de ruídos, extração de *features*, aplicação de alguma técnica de aprendizado de máquina ou estatística e a identificação propriamente dita dos indivíduos. A seguir serão descritos alguns trabalhos encontrados na literatura que abordam extração de *features* de sinais PPG.

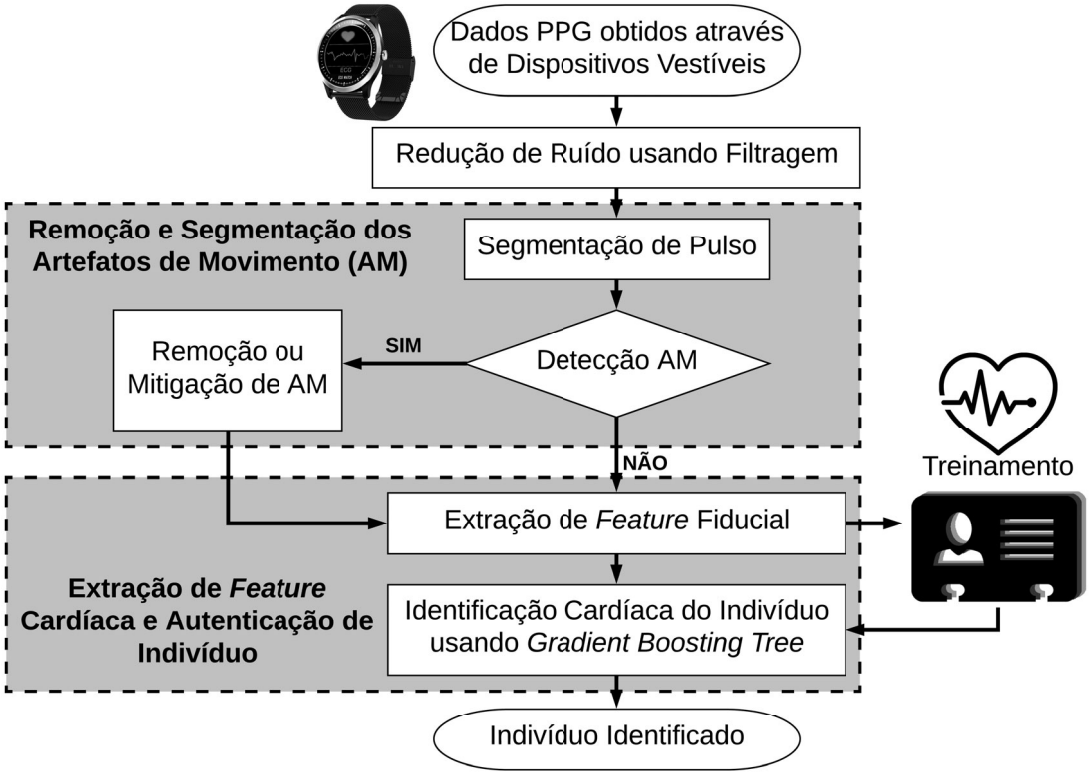

Figura 4.13: Esquema de sistemas de autenticação biométrica (Adaptado de [Zhao et al. 2018])

[Sancho et al. 2018] propuseram oferecer uma excelente discriminação entre indivíduos através da análise de um sinal PPG normal e de outro contaminado por artefato

de movimento. Eles consideraram como característica única o período de tempo dos ciclos completos do sinal PPG. [Salanke et al. 2013] também consideraram os ciclos PPG para fins de autenticação biométrica. Os ciclos foram normalizados dividindo-se a amplitude do ciclo pela amplitude do pico sistólico e, em seguida, eles foram alinhados alocando seus picos sistólicos no mesmo ponto. [Bonissi et al. 2013] adotaram como características únicas um número variável de pulsações distintas da amostra de sinal. Os autores consideraram os valores máximos de correlação cruzada entre cada batimento cardíaco e o batimento cardíaco médio. Se o valor de correlação de um batimento cardíaco for menor que um limite empiricamente estimado, o sinal relacionado é removido do *template* de *features*.

Dada a variabilidade na forma PPG em diferentes estados, a detecção fiducial no sinal PPG bruto pode ser malsucedida ou incorreta. Consequentemente, muitos pesquisadores estenderam a ideia para a primeira derivada (FD) e a segunda derivada (SD) de sinais PPG brutos e usaram pontos semelhantes em FD e SD como recursos para autenticação. Por exemplo, [Orjuela-Cañón et al. 2013] usou padrões de ataque e de pico nos sinais PPG. [Sarkar et al. 2016] demonstraram que os sinais PPG também têm o potencial de serem usados para autenticação biométrica, mostrando um exemplo da morfologia do sinal para um único batimento que compreende duas fases principais: a fase anacrótica, que significa o surgimento de a pressão sistólica e a borda ascendente do sinal, e a fase catacrótica, que reflete a diástole e a reflexão da onda a partir da periferia. O pico diastólico e o entalhe dicrótico aparecem nesta fase. A base da pulsação mostra o ponto mais baixo da diástole e o ponto inicial da sístole.

Muitos dos métodos anteriores focaram em abordagem fiducial, mas a detecção de pontos fiduciais em qualquer condição é propensa a erros [Yadav et al. 2018]. Consequentemente, muitos outros trabalhos preferiram se concentrar na abordagem não-fiducial. [Kavsaoğlu et al. 2014] analisaram o mais completo conjunto de características únicas dos sinais PPG. O conjunto é composto por quarenta características envolvendo pico sistólico, pico diastólico, entalhe dicrótico, intervalo de pulso, pico a pico, índice de aumento, índice de aumento alternativo, tempo de pico sistólico, tempo de entalhe dicrótico, tempo de pico diastólico, tempo entre os picos sistólico e diastólico, largura de pulso com semi-altura do pico sistólico, razão de área de ponto de inflexão, curva de saída de pico sistólico, curva descendente de pico diastólico, entre outros.

[Orjuela-Cañón et al. 2013] usaram uma base de dados composta por sinais de sete voluntários, sendo quatro homens e três mulheres, que ficaram em repouso por cinco minutos na posição supina. Os sinais ECG e PPG foram coletados simultaneamente através de um canal para o ECG e dois canais para o PPG. Os autores apresentaram uma proposta baseada no reconhecimento de padrões, utilizando um *Multilayer Perceptron* (MLP) para aprender as informações temporais sobre o início e o pico de pulsos. Esses pulsos estão localizados no meio do segmento. Em seguida, as janelas temporais são extraídas para treinar a rede neural. Os MLPs possuem apenas conexões *feed forward* e são treinados de forma supervisionada. Para validação dos modelos, implementou-se o método de validação cruzada *Leave One Out* (LOO). Neste caso, seis dos sete sinais foram utilizados no treinamento. Em seguida, calculou-se a validação usando apenas o sinal não incluído no treinamento. Os resultados da classificação alcançaram 98,1 % no pior dos casos.

[Kavsaoğlu et al. 2014] analisaram uma base de dados composta por 30 indivíduos

saudáveis, sendo 17 homens e 13 mulheres, que estavam sentados durante a coleta de dados. Um sinal de 15 períodos foi coletado de cada indivíduo em dois intervalos de tempo diferentes. O primeiro conjunto de dados com *features* dos primeiros sinais recebidos dos indivíduos, o segundo conjunto com *features* de sinais recebidos em um horário logo após o primeiro e o terceiro conjunto de dados sendo a combinação dos dois conjuntos anteriores. A fórmula de diferenciação fornece as três *features* dos sinais digitais unidimensionais: tanto a primeira quanto a segunda derivada devem ser zero onde a função é constante. A primeira derivada deve ser constante e a segunda derivada deve ser zero para os feixes crescentes e decrescentes. Foram obtidas identificações de 90,44%, 94,44% e 87,22% para o primeiro, o segundo e o terceiro conjunto de dados, respectivamente.

[Karimian et al. 2017] registraram sinais PPG brutos de 42 indivíduos saudáveis, os quais estavam com respiração espontânea ou controlada. Um filtro de banda passante *Butterworth* de terceira ordem com frequência de corte de 1Hz-5Hz foi empregado para reduzir o efeito de ruído. Os autores criaram segmentos PPG identificando os picos sistólicos de cada batimento cardíaco através de um algoritmo *Pan Tompkins* modificado. Os autores aplicaram *support vector machine* para aprendizado de máquina supervisionado (AMS), e *k-nearest neighbours* e *self-organization map*, para aprendizado de máquina não supervisionado (AMNS). Eles avaliaram abordagens não-fiduciais e fiduciais para extração de *features*. Os resultados demonstraram que o desempenho do AMNS é melhor, especialmente no caso de *features* fiduciais, comparado ao aprendizado de máquina não supervisionado (AMS). A abordagem não fiducial teve melhor desempenho em termos de acurácia e *equal error rate* (EER), de modo que obteve 99,5% de acurácia para AMS e 99,84% de acurácia para AMNS com EER igual a 1,31%.

Dentre as técnicas mencionadas, algoritmos baseados em PPG (para dispositivos vestíveis) mostram um grande potencial, precisando considerar as dificuldades associadas ao uso desses dispositivos. Em primeiro lugar, as gravações de PPG desses dispositivos podem frequentemente ter ruídos devido aos movimentos contínuos dos usuários. Em segundo lugar, a ocorrência de eventos nas artérias podem registrar ruídos. Assim, existe a necessidade de desenvolver algoritmos que respondam aos fatores acima de detecção de ruídos [Shashikumar et al. 2017]. Nos últimos anos, *Deep Learning* foi utilizado com sucesso no campo do processamento de sinais biométricos. Pesquisas na área de processamento de sinais vitais envolvem o estudo de sinais como ECG, eletroencefalograma (EEG) e PPG para prever ampla gama de eventos fisiológicos no corpo humano. Algumas das aplicações incluem reconhecimento de emoções [Jirayucharoensak et al. 2014], detecção de crises [Turner et al. 2014] e detecção do estágio do sono [Längkvist et al. 2012].

Deep Learning também tem sido usada para melhorar a robustez nos procedimentos atuais de monitoramento de sinais PPG em ambientes clínicos, de *e-health* e *fitness*, fazendo uso de biossensores vestíveis. Através desses dispositivos, [Jindal et al. 2016] apresentaram uma nova técnica de identificação biométrica utilizando sinais PPG por meio de *Deep Belief Networks* e *Restricted Boltzman Machines*. De acordo com [Miotto et al. 2017], as abordagens de *Deep Learning* podem ser o veículo para traduzir grandes dados biométricos em saúde humana. Entretanto, [Miotto et al. 2017] também notaram as limitações e as necessidades para desenvolvimento de métodos melhorados, especialmente em termos de facilidade de entendimento para especialistas. Portanto, estes autores sugerem o desenvolvimento de arquiteturas holísticas e significativas para unir modelos de *Deep Learning* e

interpretabilidade humana.

Alguns dos trabalhos que analisaram sinais PPG reportados neste JAI utilizaram bases de dados criadas por seus próprios autores. A maioria deles informa a quantidade e a idade dos indivíduos que participaram no processo de coleta de dados, assim como também o equipamento utilizado. Entretanto, alguns trabalhos também utilizaram base de dados públicas, disponíveis na Internet [Hatzinakos and Yadav 2019]. Sobre a extração de *features* de sinais PPG, pode-se concluir que a maioria dos trabalhos realizou duas fases: filtragem e identificação. Há várias fontes de artefatos que interferem na aquisição de sinais PPG, incluindo mudança de linha de base, artefato de movimento e respiração [Karimian et al. 2017]. Portanto, a fase de filtragem é essencial para remover/minimizar o ruído dos sinais PPG coletados. Depois da remoção de ruído, os autores utilizaram técnicas para identificar e correlacionar os usuários. As principais técnicas para identificação foram técnicas de aprendizagem de máquina (supervisionadas ou não supervisionadas), redes neurais ou até mesmo simplesmente a primeira e a segunda derivada do sinal PPG.

4.3.4.2. *Features* consideradas para sinais ECG

As batidas do coração geram ondas de polarização e despolarização nas fibras musculares. O eletrocardiograma (ECG) é feito de uma forma não evasiva, o qual representa simplesmente o registro da atividade elétrica cardíaca baseada nas diferenças de potencial resultantes [Biel et al. 2001]. Sua amostra está associada ao ciclo cardíaco, conforme ilustrado na Figura 4.14. O ECG é bastante útil para várias aplicações biomédicas, tais como a medição da taxa de frequência cardíaca, exame de ritmo das batidas do coração em busca de arritmias, diagnóstico de anormalidades do coração, reconhecimento de emoção e mais recentemente identificação biométrica.

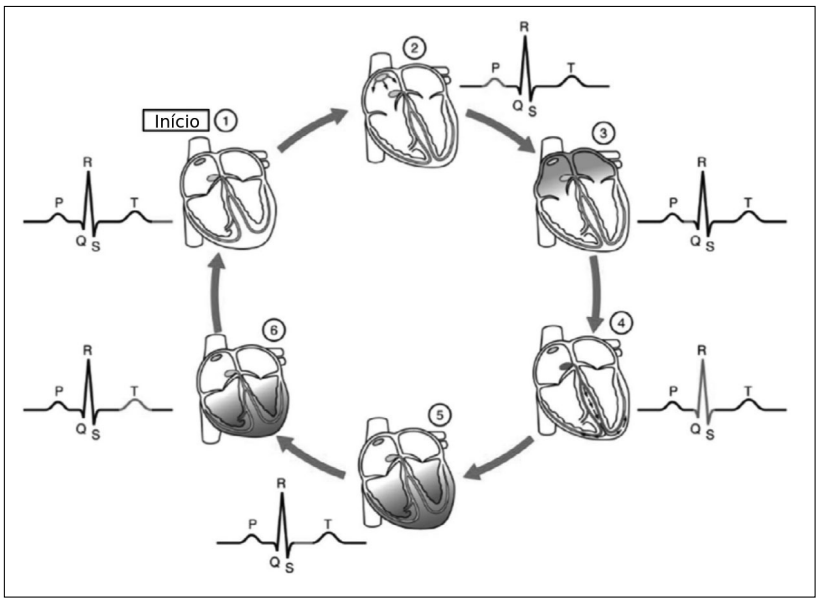

Figura 4.14: Etapas de funcionamento do coração e forma de onda captada pelo ECG

Para a extração de *features* do sinal de ECG é necessário que o sinal elétrico

coletado seja tratado previamente, passando por um processo de filtragem para retirada de ruídos, normalização e amostragem. Como explicado por [Odinaka et al. 2012], o ECG apresenta três componentes predominantes: onda P, complexo QRS e onda T como representadas na Figura 4.15. Primeiro, a despolarização do átrio gera um pulso registrado como onda P. A série de pulsos seguinte à onda P é o complexo QRS e está associada com a atividade ventricular. Finalmente, a onda T está associada à repolarização ventricular [Rezgui and Lachiri 2016]. Este complexo P-QRS-T é o mais utilizado para identificação de pessoas. Ele basicamente corresponde às localizações, durações, amplitudes e formas de onda do sinal coletado do coração (ou seja, ECG). Tipicamente, um sinal ECG possui um total de cinco deflexões principais, as ondas P, Q, R, S e T, mais uma deflexão menor, chamada de onda I, conforme descrito a Figura 4.15. A literatura apresenta três tipos de *features*: fiduciais, não fiduciais e híbridas. As *features* fiduciais extraem características no domínio do tempo das formas de onda ECG, as *features* não fiduciais aplicam uma função de transformação aos pontos característicos, e as *features* híbridas são a combinação das *features* fiduciais com as *features* não fiduciais.

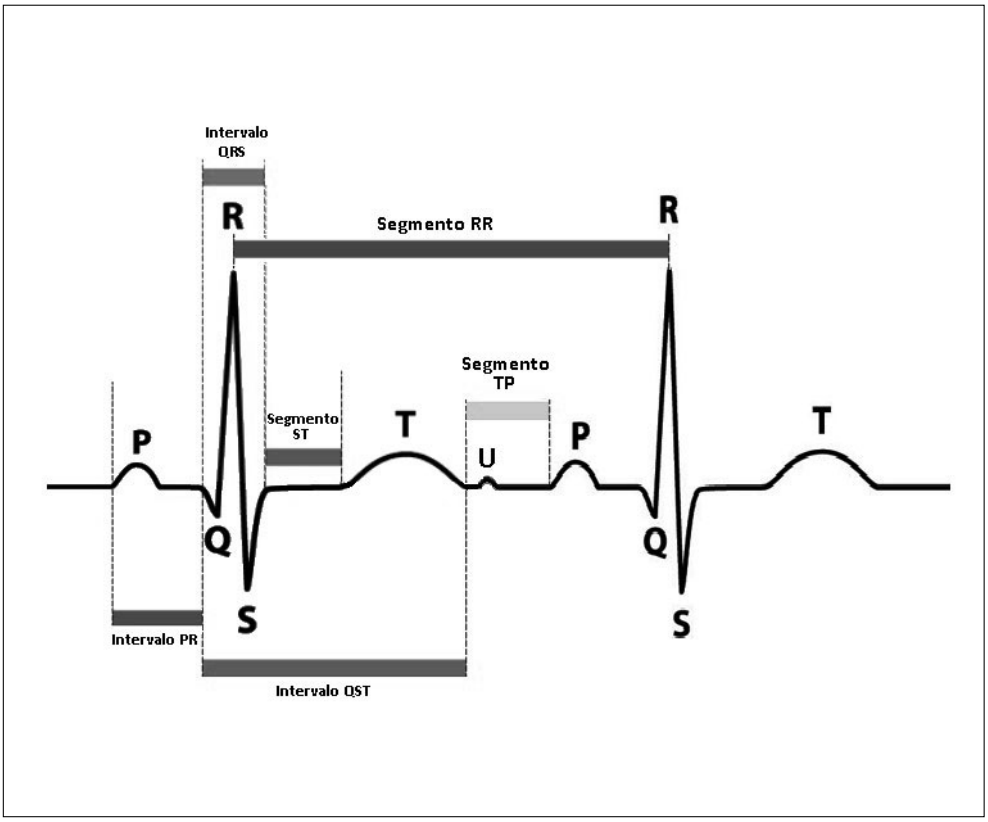

Figura 4.15: Pontos fiduciais utilizados como *features* no ECG

Segundo [Odinaka et al. 2012], há pesquisas que usam ECG como identificador biométrico: [Biel et al. 2001], [Irvine et al. 2001] e [Kyoso and Uchiyama 2001]. Estes trabalhos consideraram a hipótese de que o ECG possui informações suficientes para aplicabilidade no reconhecimento humano. Especificamente, [Odinaka et al. 2012] pesquisou cinquenta estudos dedicados à identificação humana, onde 66% dos artigos pesquisados empregaram características não-fiduciais, 26% aplicaram características fiduciais, e 8%

dos trabalhos de pesquisa usaram a abordagem híbrida. Quanto ao método de classificação, 44% dos trabalhos de pesquisa selecionaram os algoritmos *k-Nearest Neighbour* (k-NN) ou *Nearest Center* (NC), 16% implementaram Redes Neurais (ANN) e 16% utilizaram *Linear Discriminant Analysis* (LDA). Finalmente, 12% das pesquisas atingiram uma acurácia superior a 99% e 20% dos artigos pesquisados atingiram 100% de acurácia. Segundo [Odinaka et al. 2012], as características fiduciais, não-fiduciais ou híbridas não influenciam diretamente na acurácia.

[Camara et al. 2018] consideraram um cenário de uma torre de controle de tráfego aéreo. Nesse conceito, os pesquisadores assumiram que os controladores exigiam monitoramento permanente para evitar incidentes de segurança, como um intruso tentando usar o sistema de controle, um controlador assumindo a posição de um colega e a alta variação da frequência cardíaca do controlador devido a uma situação estressante. Os autores consideraram um dispositivo médico implantável para capturar o sinal de ECG e uma etapa de filtragem para limpar a corrente contínua (CC). Por simplicidade, os pesquisadores optaram por trabalhar com características não-fiduciais do ECG. Nesse sentido, o módulo de extração de recursos analisa a janela de ECG e a envia para uma Transformada *Walsh-Hadamard* (HT). [Camara et al. 2018] consideraram o HT menos computacionalmente complexo que as transformadas de *Fourier* ou *Wavelet*. O modelo de aprendizado de máquina implementou um algoritmo k-NN, usando o conjunto de dados *MIT-BIH Normal Sinus Rhythm* [Goldberger et al. 2000a]. Para a estratégia de monitoramento contínuo, o sistema atingiu 96% de acurácia.

[Zhang and Wu 2016] e [Tomlinson et al. 2019] consideraram um cenário de autenticação usando o ECG. O primeiro trabalho coleta ECG de eletrodos de dois dedos associados a um aplicativo de *smartphone*. Nos dois casos, a aplicação do sistema considera três etapas: etapa de filtragem de pré-processamento, etapa de extração de *features* e etapa de classificação. A filtragem elimina o ruído associado à linha de energia, interferência, movimento muscular e ruído de alta frequência. O módulo de detecção funciona como uma pré-etapa para a extração de *features*. Os autores em [Zhang and Wu 2016] consideraram o complexo de computação de extração de *features* não fiduciais e, assim, decidiram implementar o modelo usando formas de onda divididas por fiduciais (WF). A etapa de classificação refere-se a dois métodos biométricos: autenticação e identificação. Durante a autenticação, o sistema compara a biometria do usuário com um modelo armazenado que calcula a distância euclidiana como uma métrica de comparação. Para identificação, o sistema realiza uma classificação usando *Support Vector Machine* (SVM) e Redes Neurais (ANN). Para ambos os casos, um mecanismo de votação exigiu que mais da metade dos eleitores validassem o assunto do teste. Em comparação com outros trabalhos relacionados, a pesquisa de [Zhang and Wu 2016] atingiu 97,55% de acurácia e executou a autenticação em quatro segundos.

[Zhang et al. 2018] propuseram um sistema que combina *features* fiduciais e não fiduciais (abordagem híbrida) para aumentar a acurácia ao autenticar um grande número de indivíduos. Os autores consideraram os picos do PQRST como as principais *features*. Especificamente, os segmentos PQ, QR, RS e duração ST, as amplitudes PQ, PT e SQ determinadas por transformada *wavelet*. Para *features* não fiduciais, os autores definiram o sinal do ECG como uma matriz X, obtiveram a matriz Gramiana multiplicando $X^T X$ e finalmente obtiveram as características dos autovalores e autovetores da matriz Gramiana.

A pesquisa considerou um segundo conjunto de *features* não fiduciais como o espectro do sinal ECG gerado pela Transformada Rápida de *Fourier*. O reconhecimento do padrão ECG considerou o treinamento incremental de um algoritmo *Linear Discriminant Analysis* (LDA), usando as *features* fiduciais e não fiduciais expostas. [Zhang et al. 2018] consideraram o conjunto de dados MIT-BH que incluiu 100 amostras contendo 200 arquivos de sinal ECG por arquivo de amostra, ou seja, 20.000 sinais ECG. A pesquisa concluiu que a identificação baseada em características fiduciais e Transformada Rápida de *Fourier* apresentou baixa acurácia, na ordem de 70%-75%. Por outro lado, a implementação de uma abordagem híbrida alcançou 99%. Finalmente, os autores mostraram que o aumento do número de *features* leva a um aumento no esforço computacional, e o esquema proposto melhora a eficiência.

A seleção de *features* e a extração combinada com o aprendizado de máquina apresentam um papel relevante no reconhecimento de indivíduos. Conforme discutido por [Biel et al. 2001], as *features* do ECG contêm uma quantidade significativa de informações, mas algumas características são altamente correlacionadas. Entretanto, como discutido por [Odinaka et al. 2012], o tipo de *feature* (fiducial ou não-fiducial) não afeta a acurácia do modelo. No entanto, esta conclusão entra em conflito com a conclusão de [Zhang et al. 2018], que claramente influencia o modelo para a aplicação de *features* híbridas supostamente devido ao aprimoramento da acurácia. Portanto, é preciso conduzir a presente pesquisa por meio de simulações para concluir a melhor combinação entre o algoritmo de aprendizado de máquina *versus* o tipo de *features* no contexto de dispositivos vestíveis. Além disso, a identificação correta de um número significativo de indivíduos é uma condição *sine qua non* para a avaliação do modelo.

[Camara et al. 2018] consideraram os avanços da Internet das Coisas (IoT) e dos dispositivos médicos implantáveis da próxima geração. Nesse sentido, os autores observaram que a mineração de fluxo de dados é uma área de pesquisa promissora para lidar com a autenticação contínua. Especificamente, o ECG muda com o tempo e, portanto, o sistema precisa de atualizações. Nesse contexto, a pesquisa considera ampliar os conceitos para investigar outros sinais fisiológicos, como PPG e EEG (eletroencefalograma).

[Zhang and Wu 2016] provaram o conceito de usar um *smartphone* para reconhecimento de identidade baseado em um sinal ECG. No entanto, o teste considerou três conjuntos de dados ECG abertos e, portanto, os resultados práticos podem ser diferentes. Considerando que os dispositivos portáteis, como o *Apple Watch* [Apple 2019], já fornecem ECG, outras empresas seguirão a tendência em breve. Nesse sentido, o uso do ECG como método de autenticação se tornará frequente. Assim, o conceito de [Zhang and Wu 2016] precisa de mais investigações.

[Rezgui and Lachiri 2016] realizaram pesquisas sobre a aplicação do ECG para identificação biométrica. Na metodologia proposta, os autores consideraram um detector QRS chamado ECGPUWAVE como extrator de *features*. Este *software* implementa o algoritmo proposto por [Pan and Tompkins 1985] com melhorias propostas por [Laguna 1990]. Por outro lado, [Venkatesh and Jayaraman 2010] usaram *Dynamic Time Warping* (DTW), *Fisher Linear Discriminant Analysis* (FLDA) e *K-nearest neighbour* (k-NN). A extração de *features* considerou um sinal ECG filtrado com um minuto de duração. Primeiramente, o método identificou o complexo QRS, o intervalo R-R, a frequência cardíaca, o desvio

padrão e o número de picos na amostra considerada. Em uma segunda análise, o método identificou as ondas P, T, Q e S. Finalmente, após a redução de dimensão, o vetor de *features* considerou os intervalos de onda P, de T, de ST, o de PR interno, de QRS e de QT.

[Belgacem et al. 2012] consideraram Transformada *Wavelet* Discreta (TWD) para extração de *features* e *Random Forest* (RF) como método de classificação para identificar indivíduos com base em sinais ECG. *Wavelets* são usadas para representar sinais e outras funções de maneira normalizada, isto é, com média zero. Primeiramente, o procedimento de extração de *features* considerou um ciclo cardíaco médio obtido pela sobreposição do ciclo de cada indivíduo a partir da amostra de dados. Finalmente, as *features* são obtidas como os coeficientes do TWD dos batimentos médios. Um método de extração de *features* similar, *i.e.*, Transformada *Wavelet* Discreta, foi usado por [Dar et al. 2015]. Entretanto, os métodos mais recentes diferem em propor uma estratégia de redução de *features* aplicando *Greedy Best First Search* para subconjuntos de um subconjunto de características altamente correlacionadas.

[Karpagachelvi et al. 2010] avaliaram 17 artigos sobre técnicas de extração de *features* de ECG. Neste contexto, a transformada de *wavelet* e suas variações, tais como *wavelets* ortogonais e bi-ortogonais, *wavelets* discretas e *wavelets* quadráticas, receberam atenção de vários trabalhos. Além disso, métodos propondo algoritmos inovadores para detecção de onda P, complexo QRS, onda T e a detecção do intervalo R-R estavam em evidência no *survey* de [Karpagachelvi et al. 2010]. Métodos estatísticos, filtros combinados, coeficientes de *cepstrum* e teoria do caos eram menos frequentes.

Para [Page et al. 2015], o ECG, juntamente com um marcador biométrico secundário (ex.: impressão digital), desempenham um papel fundamental na segurança de dispositivos vestíveis. Portanto, estes autores, através de técnicas de *Deep Learning*, implementaram um sistema de reconhecimento de padrões de ECG, para fins de autenticação biométrica, confiável, robusto e rápido, utilizando redes neurais para identificar segmentos QRS complexos do sinal de ECG e, em seguida, executar a autenticação do usuário nesses segmentos. [Wieclaw et al. 2017] também aplicaram redes neurais profundas (DNN) para identificação humana com base no sinal de ECG bruto. Os resultados do estudo apontaram que o número de usuários identificados, bem como o número de neurônios e camadas ocultas, têm um impacto significativo na precisão da identificação em comparação a outros fatores. A precisão da identificação pode ser potencialmente melhorada usando outra solução, por exemplo, outras arquiteturas DNN. Isso é reforçado por [Labati et al. 2018], que afirmam que os sistemas biométricos baseados em ECG são geralmente menos precisos do que os baseados em outras características fisiológicas. Para [Labati et al. 2018], métodos como as CNNs podem extrair automaticamente características distintas de sinais ECG e demonstrar sua eficácia para outros sistemas biométricos. Para tal fim, estes autores apresentaram Deep-ECG, uma abordagem biométrica baseada em CNN para sinais de ECG, sendo o primeiro estudo na literatura que utiliza uma CNN para biometria de ECG. O Deep-ECG extrai *features* significativas de uma ou mais derivações usando uma CNN profunda, obtendo uma precisão notável para identificação, verificação e nova autenticação periódica.

Com base na análise de tais trabalhos, cujo objetivo é analisar o uso de sinais ECG como identificadores biométricos, geralmente buscam detectar a onda P, o complexo QRS,

a onda T e o intervalo R-R, através de técnicas de aprendizado de máquina e transformada *wavelet*. Também são utilizados métodos estatísticos e filtros combinados, porém estes com menor frequência, pois alguns trabalhos têm buscado elaborar algoritmos inovadores para detecção e extração das *features* dos sinais ECG.

4.3.5. Discussão

O monitoramento de sinais ECG pode ser usado como uma ferramenta essencial para monitorar condições de saúde de pacientes, assim como para identificação de indivíduos. As principais limitações dos sistemas biométricos estão relacionadas com: *i*) condições ambientais variáveis (*i.e.*, ruído, mudanças na iluminação, posicionamento da impressão digital ou da face em relação ao sensor), as quais afetam fortemente a acurácia do sistema, especialmente quando a aquisição não é realizada em condições restritas; *ii*) grandes variações intra-classe causadas pela aquisição em diferentes condições ou efeitos de envelhecimento; *iii*) não-universalidade de alguma credencial biométrica, devido a doença ou deficiência, *iv*) ataques de fraudes que são realizados falsificando um traço biométrico e, em seguida, apresentando essas informações falsificadas ao sistema biométrico [Lumini and Nanni 2017].

Nesse contexto, interferências afetam fortemente a performance dos sistemas biométricos existentes [Nakayama et al. 2019]. Por exemplo, um sistema pode rejeitar as amostras fornecidas devido à baixa qualidade ou imagens ruidosas [Lumini and Nanni 2017]. Desempenho de reconhecimento é uma medida de o quanto o sistema está apto para combinar corretamente as informações biométricas de uma mesma pessoa. Em alguns casos, o desempenho de uma simples modalidade biométrica é insuficiente e, por isso, combinar biomarcadores tem se tornado um interesse acadêmico. Essa combinação é chamada *"fusão biométrica"*, a qual pode ser classificada em dois grupos: sistemas biométricos unimodais e sistemas biométricos multimodais.

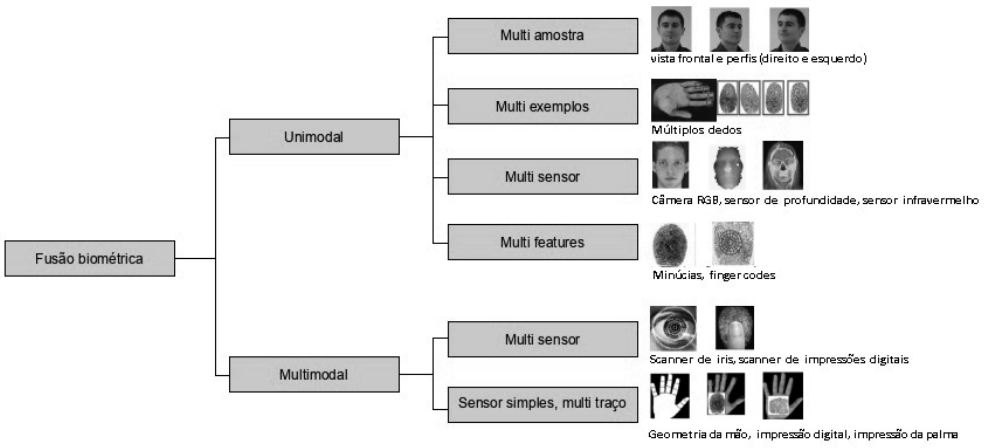

Figura 4.16: Fontes possíveis de informação em um sistema com fusão biométrica (Adaptado de [Lumini and Nanni 2017])

Os sistemas biométricos multimodais adquirem e usam vários traços biométricos para autenticação de pessoas. Algumas possíveis amostras de fontes de informação, em um sistema unimodal e multimodal, são apresentadas por [Lumini and Nanni 2017]. A

multimodalidade tem diversas vantagens sobre a unimodalidade, devido à sua capacidade de reduzir a taxa de falha de registro (do inglês *Failure-to-Enroll Rate* (FTER)) e a taxa de falha de captura (do inglês *Failure-to-Capture Rate* (FTCR)) e garantir uma cobertura populacional suficiente. Por exemplo, este processo estima que 2% da população pode não estar apta para fornecer uma impressão digital, devido a condições médicas/genéticas/acidentais/temporárias. Os sistemas multimodais são também resistentes a ataques fraudulentos porque é mais difícil para o atacante fraudar múltiplas fontes biométricas simultaneamente. O futuro dos sistemas biométricos está relacionado aos sistemas multimodais. A Figura 4.16 representa algumas possíveis fontes de informação em um sistema de fusão biométrica.

Tabela 4.1: Comparação entre sinais biométricos

Sistema biométrico	**Prós**	**Contras**
Mão	O pequeno *template* torna os atributos da região da mão uma boa opção para muitos tipos de aplicações, comparados com assinaturas biométricas mais complexas.	Pode comprometer facilmente a eficácia do sistema.
Ocular	É mais preciso, altamente confiável, bem protegido, estável e quase impossível de forjar as assinaturas biométricas.	Alto custo de sensores de imagem; Requer cuidados com fontes de luz ambiente.
Facial	Aquisição de imagem não intrusiva e sem contato, resultando em maior aceitação pública.	Esses sistemas não podem garantir identificação confiável na presença de ruídos.
ECG	*Features* ECG não podem ser copiadas ou manipuladas.	É necessário o uso de vários eletrodos durante a aquisição dos sinais ECG, causando desconforto no indivíduo. Muda de acordo com a frequência cardíaca (repouso ou exercício)
PPG	Sua coleta requer apenas LED e Foto-Diodo, ou seja, não requer nenhum tipo de gel, estímulo externo ou vários eletrodos; pode ser coletado de qualquer parte do corpo; é econômico, comparado aos outros traços biométricos.	Geralmente é prejudicado por ruídos durante a aquisição (artefatos de movimento, movimentos de sensor, respiração, contração ventricular prematura e luz ambiente); muda junto com a frequência cardíaca (repouso ou exercício); as emoções influenciam o funcionamento do sistema nervoso autônomo e do coração.

Uma outra discussão pertinente é em relação para as etapas de separação de *features* e classificação. Alguns trabalhos separam tais etapas e realizam de uma forma desacoplada, como vários artigos que usaram técnicas mais tradicionais de aprendizado de máquina

supervisionadas. Enquanto outros trabalhos já tratam ambas as etapas e executam de uma vez só, de forma integrada, como vistos nas redes neurais como *Convolutional Neural Network* e *Deep Learning*. Ambas as estratégias são válidas, no entanto separar as etapas permite ter uma maior discussão e entendimento sobre o próprio motivo de tal algoritmo classificar um sinal biométrico. Quando é usada uma integração de etapas por aplicação de redes neurais ou *Deep Learning*, nota-se que estes algoritmos trazem uma resposta, mas que continuam sendo caixas pretas, o que inviabiliza um pouco algumas afirmações como: Qual foi o processo para chegar a resposta? Ou quais *features* são mais úteis para identificar alguém?

A Tabela 4.1 mostra uma comparação entre os sistemas biométricos, destacando os prós e contras do uso de cada um deles. O sistema biométrico que faz uso da mão e o que faz uso facial, apesar de serem não intrusivos, não passam muita segurança quanto a probabilidade de serem forjados. Já o sistema que considera os olhos como identificador biométrico, apesar de ser altamente confiável e protegido, acaba sendo custoso devido aos sensores de imagem exigidos. Entre os sinais ECG e PPG, apesar de o PPG ser mais fácil e mais confortável de ser coletado, ele é mais prejudicado por ruídos durante a aquisição que o ECG. Sinais ECG são também mais fáceis de serem interpretados, de acordo com a natureza da sua forma de onda. Por este fato, este sinal será o foco principal deste JAI.

4.4. Biometria: Aspectos Técnicos de Aprendizado de Máquina

Nessa seção serão abordadas as diferentes técnicas de aprendizado de máquina utilizadas em sistemas de biometria. O objetivo é mostrar que essa é uma área de pesquisa com muitas oportunidades e uma grande variedade de técnicas que, quando dominadas, podem ser utilizadas em outras aplicações além da biometria.

4.4.1. *Artificial Neural Networks* (ANN)

As redes neurais artificiais (ANN) são algoritmos de aprendizado de máquina capazes de classificar dados lineares e não lineares. A arquitetura típica é inspirada nas redes neurais biológicas e apresenta um determinado número conectado de neurônios dispostos em diferentes camadas. A estrutura de dados representa um neurônio artificial, geralmente configurado com ponteiros conectados a outros neurônios e um valor de peso (número real) para ponderar cada conexão.

Multilayer Perceptron (MLP) refere-se a uma rede neural configurada com um número variável de neurônios dispostos em uma camada de entrada, uma ou mais camadas ocultas, e uma camada de saída, como vistos na Figura 4.17. Especificamente, o MLP propaga um estímulo injetado nos neurônios na camada de entrada, através dos neurônios conectados nas camadas ocultas, e reflete na camada de saída. *Back propagation* é uma técnica de treinamento comum para o MLP, o qual é executado em duas fases:

- **Processamento Direto:** Inicialmente, cada neurônio recebe um valor de peso fixo. O algoritmo transfere o sinal injetado da camada de entrada para a camada de saída usando os pesos para ponderar o resultado.
- **Processamento Reverso (*Back Propagation*):** O algoritmo calcula o erro entre as saídas obtidas e as saídas desejadas, e retro-propaga o erro na rede ajustando os

pesos do neurônio no caminho de volta.

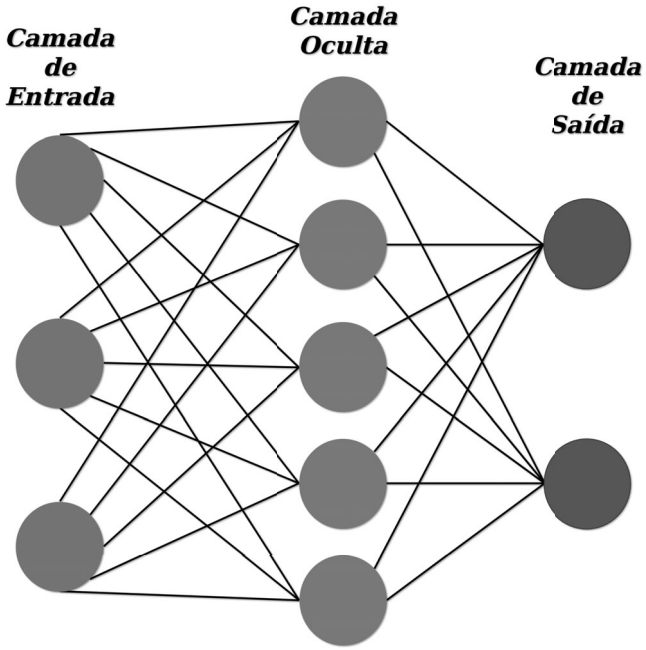

Figura 4.17: Exemplo de rede neural

O processo de treinamento repete as fases de processamento direto e reverso por um determinado número de iterações. Cada iteração se concentra em minimizar o erro entre a saída real e a saída desejada. O processo de treinamento termina quando o erro cai abaixo de um determinado limite ou quando o algoritmo atinge o número máximo de iterações estabelecidas.

Convolutional Neural Network (CNN) é um tipo de rede neural artificial (ANN) que apresenta algumas características distintas. CNN apresenta uma ou mais camadas de unidades de convolução, que reduz as unidades em mapeamentos muitos-para-um. Essa redução de parâmetros torna o modelo menos complexo, e tais unidades de convolução ao juntar algumas das unidades permite a criação de pequenas vizinhanças que compartilham informações. Devido a sua menor complexidade, CNN acaba precisando de menos amostras, o que torna o tempo de treinamento menor e deixa o modelo mais rápido.

Deep Learning é uma técnica de rede neural que consiste em transformar um dado de entrada em várias camadas de representações abstratas. Quanto mais camadas tiver na rede, maior será o número de *features* que vai aprender. A camada de saída reunirá todas estas e *features* e fará a previsão. Um dos impedimentos para se usar *deep learning* é que dependendo do número de neurônios, aumenta também o número de *features* e consequentemente a necessidade de aumentar a base de dados de treinamento.

4.4.2. *k-Nearest Neighbor* (k-NN)

k-NN classifica os vetores de características de acordo com os rótulos das amostras de treinamento mais recentes no espaço de recursos. Para um vetor de característica desconhecida, as distâncias deste vetor para todos os vetores no conjunto de treinamento

são calculadas usando uma medida de distância, *e.g.*, distância euclidiana, entre um ponto de dados particular e seus *k*-vizinhos. Em seguida, um vetor de recurso desconhecido é atribuído à classe na qual as amostras *k* mais próximas pertencem. Assim, um tipo de abordagem por maioria de votos é aplicado. O valor de *k* é um inteiro positivo e é conhecido por ser um fator que influencia fortemente a precisão da classificação.

k-NN tem a vantagem de não fazer uma suposição inicial sobre o conjunto de dados, pois apenas agrupa os pontos de dados baseados em uma vizinhança. No entanto, o algoritmo armazena todos os dados de treinamento e só libera-os quando todos os dados são classificados. Normalmente, mas nem sempre, o algoritmo consegue uma melhor precisão com *k* valores mais altos. O algoritmo k-NN herda formas de tratar características de aplicações, como previsão meteorológica [Yesilbudak et al. 2017], detecção de quedas de idosos [Tsinganos 2017], detecção de crime [Tayal et al. 2015], além de um uso amplo na maioria dos problemas de reconhecimento de padrões, como também é empregado em alguns estudos recentes de classificação de ECG ou de detecção de convulsões epilépticas [Shanir et al. 2017].

4.4.3. *Support Vector Machine* (SVM)

SVM é uma ferramenta amplamente usada para resolver problemas de classificação binária devido ao seu excelente desempenho de generalização. A ideia principal do SVM é encontrar uma margem máxima entre os dados de treinamento e o limite de decisão. Os vetores de suporte, que são as amostras de treinamento mais próximas do limite de decisão que são usados para a maximização da margem. O SVM pode ser considerado como um classificador linear ou não linear de acordo com o tipo de sua função *kernel*. Enquanto uma função de *kernel* linear torna o SVM um classificador linear, outras funções do *kernel*, como base radial de *gaussian*, polinômio e sigmoide, fazem dele um classificador não linear. O SVM é utilizado na maioria dos estudos de classificação do ECG.

4.4.4. *Naïve Bayes* (NB)

NB é um método de classificação probabilístico e estatístico baseado nas regras do Teorema de *Bayes*. A definição do teorema deriva-se da definição probabilística condicional [Goodfellow et al. 2016], que estabelece a probabilidade de um evento *A* de ocorrer baseado em uma ocorrência prévia de um evento *B*, como mostrado na Eq. 1. Esta teoria é uma abordagem estatística fundamental na qual a ideia por trás é que, se a classe for conhecida, os valores dos outros recursos podem ser previstos. No caso em que a classe não é conhecida, a regra de *Bayes* pode ser usada para prever o rótulo da classe de acordo com os valores de recurso fornecidos.

$$P(A|B) = \frac{P(A) * P(B|A)}{P(B)} \tag{1}$$

Onde,

- $P(A|B)$, é a probabilidade condicional de B ocorrer sabendo que A já ocorreu.
- $P(A)$, é a probabilidade do evento A de acontecer.

- $P(B|A)$, é a probabilidade condicional de A ocorrer sabendo que B já ocorreu.
- $P(B)$, é a probabilidade de evento B de ocorrer. pode ser tanto descoberto a priori ou calculado por $P(B) = \sum_A P(B|A) * P(A)$.

O algoritmo inicializa as probabilidades para as variáveis de resultado e as ajusta em cada interação baseada no que aconteceu com as outras variáveis do conjunto de dados. Em classificadores *bayesianos*, os modelos probabilísticos dos recursos são criados para prever o rótulo de classe de uma nova amostra. Eles são um dos métodos mais utilizados para problemas de reconhecimento de padrões.

4.4.5. *Bagging*

Também chamado de *Bootstrap Aggregating*, é um algoritmo de *ensemble* metaheurístico. Como modelo de *ensemble*, ele tenta diminuir a variância das diferentes classes, ajudando assim a fugir de problema do *overfitting* (sobre-ajuste). Para os métodos de *ensemble* como o *bagging*, quanto maior a diversidade do conjunto de dados, melhor será seu desempenho. Apesar de ter sido criado para evitar *overfitting*, há outros algoritmos bem mais aleatórios, como o RF, mais eficazes nesse processo.

4.4.6. *K-means clustering*

K-Means é um clusterizador que divide n-instâncias do conjunto de dados em *k-clusters*. A associação de cada dado é feita de acordo com a distância mais próxima do centro de cada *cluster*. Portanto, cada *cluster* agrega os conjuntos de dados mais próximos. No final, o *K-Means* divide todo o conjunto de dados usados em um diagrama de Voronoi. É importante ressaltar que *K-Means* é uma técnica não supervisionada, diferente de todos os outros modelos de aprendizado de máquina apresentados aqui. Por sua natureza não supervisionada, ele não precisa de pontos rotulados. Portanto, *K-Means* é ótimo para ser usado em cenários onde não sabemos muito a respeito do conjunto de dados processado, sendo assim muito útil para utilizá-lo inicialmente em grandes *datasets* como demografia da população, tendências nas redes sociais, detecção de anomalia, entre outros.

4.4.7. *Decision Tree (DT)*

A DT tornou-se um popular método de classificação de aprendizado de máquina devido à sua versatilidade para aplicações em muitos problemas, desde a identificação de objetos até diagnósticos médicos como análise de digitais, íris ou até ECG. O conceito é usar a estrutura em árvore para dividir as *features* em classes diferentes com base em critérios probabilísticos e em limites numéricos. *features* ou atributos definem a classe. As estruturas de DT são chamadas de árvores de classificação ou regressão. Enquanto as folhas das árvores de classificação representam rótulos de classe, as folhas das árvores de regressão representam valores contínuos. Existem muitos algoritmos para desenvolver um DT, como ID3 (*Iterative Dichotomiser 3*), C4.5 (alternativa para ID3), *Cart* (Árvore de Classificação e Regressão) e *Chaid* (*Chi-Squared Automatic Interaction Detector*).

DT tem a vantagem de ser fácil de implementar e interpretar quando comparado a outros métodos de classificação. Entretanto, dependendo das *features* escolhidas e da forma como os dados são divididos na árvore, o modelo pode perder a capacidade de

generalização devido ao *overfitting*. Há duas maneiras comuns de lidar com o *overfitting*: limitar o número de divisões ou permitir a divisão apenas se houver um número mínimo de pontos de dados na ramificação da árvore.

Um aspecto essencial da configuração do DT é como definir a importância de cada *feature* para maximizar os resultados da classificação. O algoritmo pega a característica que melhor representa a classe e a posiciona na raiz. Existem alguns índices propostos na literatura para identificar as características mais relevantes: Coeficiente de *Gini* e Índice de Entropia. o Coeficiente de *Gini* é uma medida da importância da variável para o conjunto de dados e o índice de entropia é uma medida de incerteza associada com a variável. A plataforma *Knime* usou a metodologia discutida por [Shafer et al. 1996] para implementar DT usando o Índice de *Gini*, calculado de acordo com a Eq. 2.

$$Gini(s) = 1 - \sum_{j} p_j^2 \tag{2}$$

onde,

- s representa o conjunto de dados
- p_j representa a frequência relativa da classe j no conjunto de dados s

Além das abordagens de árvores de decisão comuns, existem algumas estruturas de árvores de decisão mais específicas que são usadas frequentemente para classificação de ECG. Uma abordagem mais complexa é a utilização da floresta aleatória, onde várias árvores de decisão são treinadas com subconjuntos de dados e será explicada a seguir.

4.4.8. *Random Forest* (RF)

Um conjunto de árvores de decisão (DT) pode receber a nomeação de RF, o qual treina cada DT com dados selecionados aleatoriamente. Essa metodologia garante que cada árvore seja ligeiramente diferente uma da outra. Assim, cada árvore pode retornar um resultado distinto para um conjunto de dados. O algoritmo de RF classifica os dados com base em um sistema de votação envolvendo os resultados de árvores individuais, como visto na Figura 4.18. O sistema de votação pode calcular o voto direto ou ponderado. Especificamente, o voto direto conta quantas árvores classificaram uma determinada *feature* sob uma classe específica. A votação ponderada retorna a proporção de elementos pertencentes a uma determinada classe.

O RF executa melhor que DT em dois aspectos críticos: detecção de anomalia e *overfitting*. Devido ao processo de treinamento, os *outliers* estarão presentes em algumas das árvores, mas não em todas elas. Assim, o sistema de votação garante que os resultados anômalos sejam isolados. O sistema de votação também minimiza o efeito do *overfitting* em relação ao DT individual. No entanto, tanto RF quanto DT tem problemas para extrapolar dados. Especificamente, os valores de atributo no conjunto de validação devem estar dentro dos limites de valor do conjunto de treinamento. Os atributos não treinados ou fora do limite levam a resultados imprevisíveis quando incluídos no conjunto de validação.

O algoritmo de RF aceita que o número de árvores cresça como um parâmetro configurável. Não há um melhor valor e o limite deve ser a capacidade de armazenamento

para salvar a DT. No entanto, um número maior de árvores de decisão não reflete necessariamente nos resultados da classificação. Uma abordagem é começar com poucas árvores e aumentar gradualmente seu número até que os benefícios não valham os aumentos.

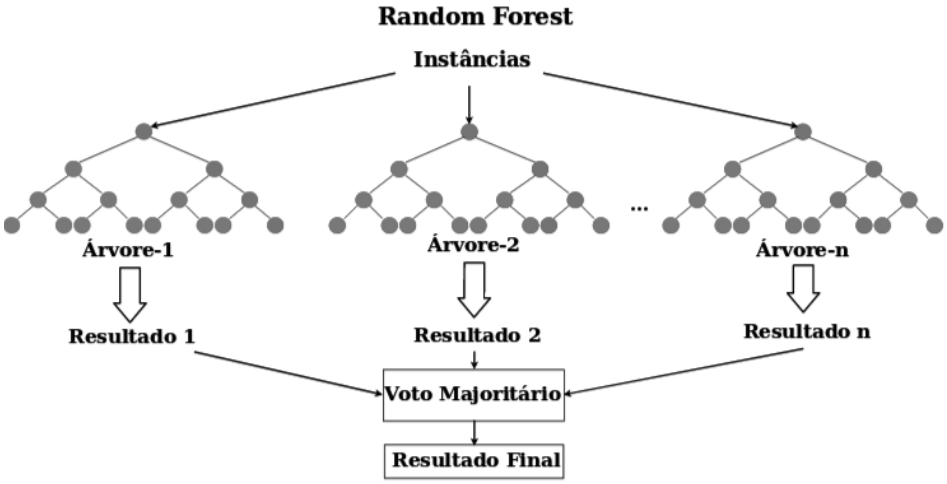

Figura 4.18: *Random Forest*

4.5. Um Estudo de Caso: na prática

Como forma de validar a utilização de sinais biométricos para autenticação, será utilizado um dos vários bancos de dados públicos disponíveis na base do site *Physionet*[1] [Goldberger et al. 2000b]. A maioria das bases de dados foi coletadas com objetivos clínicos, avaliando pessoas com problemas cardíacos e pessoas saudáveis. Para a parte prática deste JAI, será considerado o seguinte roteiro de atividades:

1. **Escolha da Base de Dados:** O participante analisará as bases públicas disponíveis no *Physionet*. Serão observados os desafios que o pesquisador enfrentar ao trabalhar com dados biométricos. Para a validação dos modelos desenvolvidos é preciso escolher uma base de dados com uma quantidade suficiente de amostras. Bases com poucas instâncias podem nos levar a conclusões divergentes daquelas encontradas em aplicações reais, com milhares ou milhões de amostras. No caso de uma base com muitas amostras, ainda será necessário avaliar algumas questões como: qual é a qualidade dessas amostras? Como o sinal foi capturado? Qual é a amostragem do sinal ou sua resolução (casas decimais)? Há ruído no sinal capturado?

2. **Seleção das *features* e aplicação de técnica de aprendizado de máquina:** Serão revisados de modo prático as vantagens e desvantagens das tecnologias de aprendizado disponíveis. Aspectos como quantidade dos dados e características das *features* utilizadas podem influenciar em um melhor ou pior resultado com uma determinada técnica. Será realizado comparativos entre resultados obtidos através de diferentes técnicas. Há ferramentas abertas como o *knime* que permitem a execução de diversas técnicas de aprendizado de máquina sobre a mesma base de dados, possibilitando

[1]Banco de dados de sinais biométricos, https://physionet.org

a definição de qual técnica pode fornecer o melhor resultado para um determinado *dataset*.

3. **Avaliação dos resultados:** Após a escolha do *dataset*, das *features* que serão analisadas e da execução do algoritmo de aprendizado de máquina, serão estimuladas avaliações dos resultados encontrados. Variações na quantidade de *features* ou utilização de *datasets* diferentes podem nos levar a resultados diferentes. É necessário entender o que motiva esse tipo de resultado. Uma análise estatística e de vários cenários são essenciais para a validação do sistema. Figura 4.19 resume este roteiro de atividades.

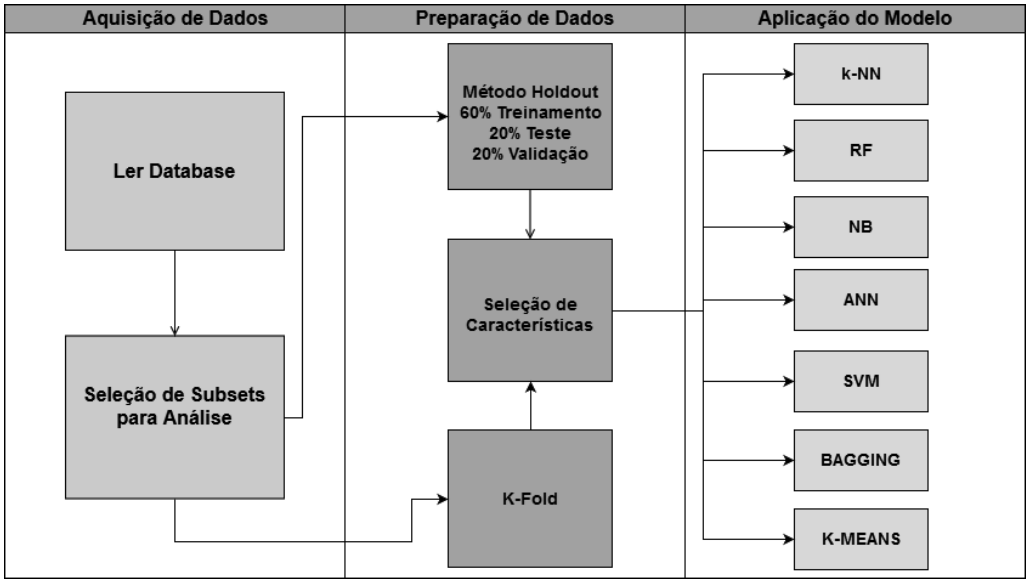

Figura 4.19: Roteiro de atividades

4.5.1. Características das Base de dados

O conjunto de dados usado foi proveniente de dois *datasets*, provenientes do Physionet: *Stress Recognition in Automobile Drivers*[2] (Reconhecimento de Stress em Motoristas de Automóveis) e *ECG-ID Database*[3] (Base de Dados ECG-ID). Ambos *datasets* serão usados na etapa de avaliação. Mais especificamente:

1. ***Dataset I - Stress Recognition in Automobile Drivers*:** O Reconhecimento de Stress em motoristas de automóveis [Healey and Picard 2005] é um *dataset* usado para tentar identificar o grau de stress de motoristas dirigindo. A coleta foi feita com 24 motoristas saudáveis, por pelo menos 50 minutos cada. O *dataset* apresenta uma coleção de sinais biométricos distintos disponíveis, como o ECG, EMG, respiração e resposta galvânica da pele (medidos nas mãos e pés). A coleta foi realizada enquanto os motoristas seguiam uma rota pré-determinada de rodovias na região

[2]*Dataset I - Stress Recognition in Automobile Drivers*, https://physionet.org/pn3/drivedb/
[3]*Dataset II* - ECG-ID, https://physionet.org/pn3/ecgiddb/

Tabela 4.2: Todas as 30 features mapeadas pelo Siemens Megacart

N.	*Features*/Características
1	início da onda P
2	duração da onda P (ms)
3	início da onda QRS
4	duração da onda QRS (ms)
5	duração da onda Q (ms)
6	duração da onda R (ms)
7	duração da onda S (ms)
8	duração da onda R' (ms)
9	duração da onda S' (ms)
10	duração da onda P+ (ms)
11	deflação da onda QRS (ms)
12	amplitude da onda P+ (μV)
13	amplitude da onda P- (μV)
14	amplitude de pico a pico da onda QRS (μV)
15	amplitude da onda Q (μV)
16	amplitude da onda R (μV)
17	amplitude da onda S (μV)
18	amplitude da onda R' (μV)
19	amplitude da onda S' (μV)
20	amplitude do segmento ST (μV)
21	amplitude do segmento 2/8 ST (μV)
22	amplitude do segmento 3/8 ST (μV)
23	amplitude da onda T+ (μV)
24	amplitude da onda T- (μV)
25	área da onda QRS (μV * ms)
26	morfologia da onda T [-2,2]
27	existência de corte da onda R
28	grau de confiança da onda Delta [0,100]%
29	inclinação do segmento ST [-90,90] graus
30	início da onda T

metropolitana de Boston. O principal objetivo do estudo foi investigar a viabilidade de reconhecimento automatizado de estresse baseado nos sinais registrados. O resultado demonstrou que a maioria dos motoristas estudados apresentou uma boa correlação entre o nível do registro galvânico e métricas do batimento cardíaco com o nível de stress das pessoas. O *dataset* está dividido nos 2 experimentos realizados por [Healey and Picard 2005].

2. ***Dataset II*** **- ECG-ID** O outro *dataset* foi uma investigação sobre a possibilidade de identificar pessoas a partir do sinal biométrico do ECG. O estudo envolveu 90 voluntários e apresenta 310 gravações distintas de voluntários com idades variando entre 13 e 75 anos. Devido a natureza ruidosa da coleta do sinal ECG, o autor do *dataset* disponibilizou 2 tipos de sinais: sinal original e sinal filtrado para análise.

4.5.2. Selecionando *features*

Tabela 4.2 reúne as principais *features* presentes nos sinais ECG, ambos disponíveis nos dois *datasets* que serão trabalhados.

4.5.3. Métricas de desempenho

A escolha das métricas foi feita de acordo com os resultados apresentados em uma matriz de confusão para avaliar o desempenho dos algoritmos. A matriz de confusão tabula os resultados previstos em relação às observações dos resultados reais, como mostra a Tabela 4.3. Com base na matriz de confusão, tem-se 2 linhas e 2 colunas. A primeira coluna apresenta os valores negativos (sejam os verdadeiros e os falsos) e a segunda coluna apresenta os valores positivos (sejam os verdadeiros e os negativos). A primeira linha apresenta os valores reais observados negativos (indicados como verdadeiros negativos e falsos positivos). A segunda linha apresenta os valores, de fato, positivos (indicados como falsos negativos e verdadeiros positivos).

Tabela 4.3: Exemplo de uma matriz de confusão

		Valores Preditos	
		A	B
Valores Reais	A	verdadeiro negativo (TN)	falso positivo (FP)
	B	falso negativo (FN)	verdadeiro positivo (TP)

A escolha de cada métrica depende de acordo com o que quer avaliar. A matriz de confusão oferece uma forma visual para enxergar como deriva cada métrica de desempenho que será usada na seção prática. Todos os algoritmos serão avaliados. As métricas de desempenho são acurácia, *recall*, precisão e *F1 Score*. Todas estas métricas avaliam quantitativamente o quanto cada classificador atingiu durante os testes e valores maiores representam melhores desempenhos.

A acurácia é aplicada para medir o desempenho de cada classificador, o qual tem sido usada na avaliação dos algoritmos de aprendizagem de máquina. A acurácia calcula a porcentagem de acertos que o classificador alcançou durante identificação do sinal ECG, sendo calculada pela Eq. (3). O TP refere-se aos verdadeiros positivos, TN aos verdadeiros negativos, FP aos falsos positivos, e FN aos falsos negativos. Uma outra interpretação para esta equação seria a razão entre o número de predições corretas sobre o número total de predições realizadas. Em outras palavras, acurácia pode ser também definido como a fração das predições que o modelo de aprendizado de máquina acertou prever.

$$Acurácia = \frac{(TP+TN)}{(TP+FP+TN+FN)} \tag{3}$$

A métrica de precisão tenta responder o seguinte questionamento: qual é a proporção de identificações positivas que estão realmente corretas? A precisão pode ser calculada de acordo com a Eq. (4), onde TP refere-se aos verdadeiros positivos e FP aos falsos positivos. Uma outra forma de especificar a precisão é que esta seja a proporção de verdadeiros positivos pelo número total de valores positivos preditos.

$$Precisao = \frac{(TP)}{(TP+FP)} \tag{4}$$

O *Recall* tenta responder o seguinte questionamento: qual é a proporção de atuais positivos foram identificados corretamente? *Recall* pode ser calculado de acordo com a Eq. (5), onde TP se refere aos verdadeiros positivos e FN aos falsos negativos. Em outros termos, *recall* pode ser interpretado como a forma que os modelos podem calcular os atuais positivos e marcar como positivos (TP).

$$Recall = \frac{(TP)}{(TP+FN)} \tag{5}$$

F1 Score é uma outra métrica um pouco mais distinta. A Eq. (6) apresenta a forma de calculá-la e depende tanto dos valores de precisão quanto de *recall*. *F1 Score* é empregada quando há valores bem diferentes entre precisão e *recall*, tentando achar um certo equilíbrio ao utilizar a média harmônica. Dentre as quatro métricas de desempenho usadas, o *F1 Score* consegue ser a mais apropriada para conjuntos de dados desbalanceados que apresentam distribuições de classes bem distintas.

$$F1\ Score = 2 \times \frac{\text{Precisao} \times \text{Recall}}{\text{Precisao} + \text{Recall}} \tag{6}$$

4.5.4. Algoritmos de Aprendizagem de Máquina

A análise faz uso de vários algoritmos de aprendizado de máquina supervisionados e não supervisionados. No total, empregou-se sete algoritmos de classificação e um *clusterizador*, todos bem diversificados e conhecidos na literatura. Especificamente, considerou-se *Naïve Bayes*, *Random Forest*, *Bagging*, *k-Nearest Neighbor*, *Support Vector Machine*, *K-Means*, *Artificial Neural Network*.

4.5.5. Sobre o ambiente de trabalho e avaliação

Durante as análises, essas características foram combinadas conforme resultados de correlação obtidos na ferramenta Weka[4]. Weka é um conjunto de ferramentas que possuem diversos algoritmos de aprendizado de máquina para as mais distintas funções de mineração de dados, seja estas de classificação, preparação, regressão, *clusterização*, entre outros.

Para a identificação através de algoritmos de aprendizado de máquinas, baseamos a avaliação prática nos métodos *holdout* e *k-fold*. Ambos os métodos são usados para realizar o particionamento dos dados. O objetivo com estes métodos é dividir os dados em conjuntos mutualmente exclusivos e depois utilizar alguns destes subconjuntos para estimação dos parâmetros, ou seja, fazer uma previsão que estima o quão acurado é um determinado modelo (técnica de aprendizado de máquina) na prática. É importante que estes resultados sejam bem avaliados e que consigam determinar com precisão sobre o que tentam classificar, sem que estes dados estejam enviesados por *overfitting* (sobre-ajuste).

[4]Weka 3, https://www.cs.waikato.ac.nz/ ml/weka/. Último acesso em Abril/2019.

Ou seja, é importante que os modelos tenham bons desempenhos para o conjunto de dados e que façam boas estimações sem estarem enviesados/viciados.

Para evitar o *overfitting*, tentamos usar dois métodos recomendados de particionamento. No método *holdout* dividimos os dados em treinamento (60 %), teste (20 %) e validação (20 %). *k-fold* usa apenas uma amostra de dados (dados de treinamento) e tem um único parâmetro chamado *k* [Pacheco et al. 2018]. O parâmetro refere-se ao número de grupos que uma determinada amostra de dados deve ser dividida. Nós executamos a validação cruzada de *k-fold* e *holdout* nas sessões práticas.

O objetivo de toda a avaliação é mostrar de forma prática como pode ser realizada a identificação de pessoas com alguma técnica de aprendizado de máquina, usando sinais vitais como o ECG, registrando assim uma demonstração de tudo o que foi explicado neste JAI. Para maiores detalhes das etapas práticas e procedimentos a serem adotados na apresentação prática, estará disponibilizado um outro material que permitirá o acompanhamento da seção prática, através do *link*[5].

4.6. Considerações Finais e Direções Futuras

Esta seção está organizada de acordo com as conclusões tiradas e desafios/*open issues* feitos acerca do tema. Ao longo deste capítulo realizamos uma revisão da evolução tecnológica que a linha de pesquisa biométrica, como técnica de segurança, sofreu nas últimas décadas. Independente do sinal biométrico utilizado (digital, mão, rosto, íris, ECG, etc), foi possível observar que a acurácia e qualidade do sistema dependem de diversos fatores como a qualidade do sensor utilizado para a aquisição dos dados, técnica de pré-processamento do sinal, escolha das *features*, técnicas de aprendizado de máquina aplicadas e outros. Para a simulação e estudos científicos, há dificuldades em relação às base de dados públicas disponíveis que possam refletir um cenário realístico no número de indivíduos para testes.

Para traços biométricos estabelecidos e utilizados ao longo de décadas, como as digitais, existem bases de dados disponíveis coletadas através de situações reais. Para o sinal biométrico ECG, o qual tem sido bastante utilizado em novas pesquisas, apesar de trabalhos como o [Merone et al. 2017], onde é feito um mapeamento sistemático das bases de dados mais utilizadas, percebemos que ainda falta uma padronização que permita testes mais robustos, com milhares de indivíduos para teste, algo possível para digitais, por exemplo. Assim, novos sinais biométricos como o ECG, EEG, PPG e EMG ainda precisam ser validados com bases de testes maiores e mais robustas. Esta é uma das grandes dificuldades: validar esses modelos com uma quantidade maior de indivíduos e com uma padronização em relação ao *hardware* utilizado para permitir uma comparação e avaliação de desempenho fidedigna.

Além disso, entende-se que, devido à grande quantidade de *features* disponíveis para cada sinal e à variação de técnicas de aprendizado de máquina que podem ser utilizadas em conjunto com essas *features*, é difícil que ocorra uma padronização e resposta exata para qual a melhor característica a ser utilizada de um sinal ou qual a melhor técnica de aprendizado de máquina. Muitos aspectos precisam ser levados em consideração,

[5]Material complementar do JAI, https://github.com/TheHealthsenseProject/JAI. Último acesso em Maio/2019.

tais como a sensibilidade do algoritmo de classificação em relação ao ruído no sinal capturado, expectativa no tempo de processamento, domínio do sinal e outros. As métricas de desempenho também devem ser escolhidas criteriosamente, por representarem aspectos diferentes da qualidade de um sistema de autenticação.

Pode-se observar que vários classificadores são utilizados, como o ANN, k-NN, SVM, RF. De um modo geral, as variações de redes neurais (ANN) têm sido mais utilizadas, assim como o SVM e o k-NN. Os algoritmos ligados à árvores de decisão, como o *Random Forest*, são muito utilizados também devido à sua menor complexidade e maior facilidade de compreensão para quem inicia nessa linha de pesquisa. Sendo assim, entende-se que o estudo de técnicas de biometria proporciona para o estudante de computação uma visão transversal e prática de diversas disciplinas, como eletrônica (sensores para aquisição de dados), processamento de Sinais (tratamento dos ruídos e extração/Seleção de *features*), redes (transmissão de dados e processamento distribuído) e inteligência Computacional (utilização de aprendizado de máquina para identificação de padrões).

Acreditamos que ainda há grande oportunidade para avançarmos na utilização de novos sinais biométricos, principalmente em relação ao ECG, PPG, e EEG. Ainda precisam ser endereçados aspectos na aquisição dos dados, aprendizado de máquina, utilização multimodal de sinais, publicidade, falsificação e segurança dos dados. Inicialmente, no caso do ECG, os dados eram capturados através de dispositivos médicos e em um ambiente controlado dentro de uma clínica ou hospital. Como a finalidade dos dados era prioritariamente a identificação de doenças cardíacas, essa metodologia era razoável. Com o avanço da Eletrônica, a aquisição dos sinais passou a ser distribuída, através de dispositivos vestíveis e *gadgets* tecnológicos, aumentando significativamente o conforto e aceitabilidade pelo usuário. Esse tipo de avanço possibilitou um maior interesse das pessoas por monitorar seus sinais cardíacos, obtendo ganhos de saúde ao monitorar o ritmo do coração ao longo do dia.

As pesquisas devem continuar a explorar melhores técnicas de aquisição de sinais, melhorando a aceitabilidade dos novos sistemas, como o sinal de ECG por exemplo. Além disso, também será foco o endereçamento para o uso de múltiplos sinais, conforme a Figura 4.16, onde é visualizada a comparação entre multimodal e unimodal. A utilização do rosto/face como método de autenticação estava apenas em laboratório até poucos anos atrás, mas hoje já está em uso por vários fabricantes de celulares, por exemplo. Espera-se que, em breve, outros sinais passem a ser utilizados, como o PPG e o ECG.

Aspectos ligados a proteção dos dados também devem ser levados em consideração, pois acreditamos que a preocupação com a privacidade fará com que tanto a indústria como a academia desloque mais esforços para aumentar o controle dos dados sensíveis produzidos e seu armazenamento. Técnicas de criptografia passarão a ser itens obrigatórios no armazenamento de dados em dispositivos IoT, além da utilização de biometria em serviços que, até então, não existia a preocupação com o acesso malicioso.

Um dos primeiros desafios que precisam ser endereçados, principalmente ao levar em conta a iminente utilização da biometria em dispositivos IoT, com limitações de *hardware*, é o aumento da qualidade nos sensores. Possibilitando a supressão do efeito de várias fontes de ruídos sem degradar as informações contidas no sinal biométrico que possibilitam identificar um indivíduo. Os sistemas biométricos se beneficiarão dos avanços

nos sensores, principalmente com novas tecnologias ópticas para coleta de sinais, as quais já vem melhorando a coleta de sinais PPG, por exemplo. Assim, outros esforços vêm sendo direcionados a alguns desafios.

Existe ainda uma dificuldade de encontrar a melhor representação de *features* de um traço biométrico. Por exemplo, para o ECG, como vimos na Figura 4.5 e na Tabela 4.2, há um número grande de *features* que podem ser utilizadas. O ideal é a escolha do conjunto de discriminantes mais representativos. Por intuição, isso seria relativamente fácil de se atingir ao aumentar o número de *features*, mas não há garantia que isso vá aumentar a acurácia, exceto se, de fato, existir. Portanto, é necessário uma avaliação profunda sobre quais *features* devem ser selecionadas.

Uma outra dificuldade se apresenta em escolher o melhor algoritmo para ser usado como classificador. É importante mencionar que não há um classificador que possa ser aplicado universalmente para todos os traços biométricos. Portanto, há a necessidade de analisar cuidadosamente o algoritmo de aprendizado de máquina com o conjunto de dados (tipos de sinais biométricos) a ser trabalhado.

Apesar de todas as dificuldades, acreditamos na necessidade e importância de se estudar com mais profundidade sobre a autenticação usando sinais biométricos, que tende a se tornar cada vez mais popular na sociedade. Neste capítulo e na apresentação durante a Jornada de Atualização em Informática (JAI), demos um enfoque maior ao ECG como estudo de caso prático, por entendermos que o ECG, dentre os novos sinais biométricos, é o que possui maior potencial para ser utilizado brevemente na indústria, tornando-se assim uma alternativa viável e com grande valor agregado por possibilitar o monitoramento dos sinais do coração e prover segurança ao mesmo tempo.

Agradecimentos

Este trabalho foi desenvolvido através do projeto denominado *HealthSense: Assessing and Protecting Privacy in Wireless Wearable Sensor-generated Medical Data*, através do apoio da Rede Nacional de Ensino e Pesquisa (Brasil) e da *National Science Foundation* (EUA). No Brasil, o projeto está sendo executado pela Universidade Federal do Paraná (UFPR) e pela Universidade Federal do Pará (UFPA).

Referências

[Abate et al. 2007] Abate, A. F., Nappi, M., Riccio, D., and Sabatino, G. (2007). 2d and 3d face recognition: A survey. *Pattern Recognition Letters*, 28(14):1885 – 1906. Image: Information and Control.

[Al-Waisy et al. 2018] Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., and Nagem, T. A. (2018). A multi-biometric iris recognition system based on a deep learning approach. *Pattern Analysis and Applications*, 21(3):783–802.

[Allen 2007] Allen, J. (2007). Photoplethysmography and its application in clinical physiological measurement. *Physiological measurement*, 28(3):R1.

[Apple 2019] Apple (2019). Apple watch. `https://www.apple.com/watch`. Acessado em: Janeiro de 2019.

[Baynes 2019] Baynes, C. (2019). Chinese police to use facial recognition technology to send jaywalkers instant fines by text. https://www.independent.co.uk/news/world/asia/china-police-facial-recognition-technology-ai-jaywalkers-fines-text-wechat-weibo-cctv-a8279531.html. Acessado em: Maio de 2019.

[Belgacem et al. 2012] Belgacem, N., Nait-Ali, A., Fournier, R., and Bereksi-Reguig, F. (2012). Ecg based human authentication using wavelets and random forests. *Int. J. Cryptogr. Inf. Secur*, 2(3):1–11.

[Biel et al. 2001] Biel, L., Pettersson, O., Philipson, L., and Wide, P. (2001). Ecg analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, 50(3):808–812.

[Bledsoe 1966] Bledsoe, W. (1966). Man-machine facial recognition. *Technical Report, PRI 22 - Panoramic Research, Inc.*, 73.

[Bonissi et al. 2013] Bonissi, A., Labati, R. D., Perico, L., Sassi, R., Scotti, F., and Sparagino, L. (2013). A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on*, pages 28–33. IEEE.

[Bosche et al. 2018] Bosche, A., Crawford, D., Jackson, D., Schallehn, M., and Schorling, C. (2018). 2018 roundup of internet of things forecasts and market estimates. https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/. Acessado em: Abril de 2019.

[Camara et al. 2018] Camara, C., Peris-Lopez, P., Gonzalez-Manzano, L., and Tapiador, J. (2018). Real-time electrocardiogram streams for continuous authentication. *Applied Soft Computing Journal*.

[Chen et al. 2005] Chen, H., Valizadegan, H., Jackson, C., Soltysiak, S., and Jain, A. K. (2005). Fake hands: spoofing hand geometry systems. *Biometric Consortium*.

[Clark and Kruse 1990] Clark, V. L. and Kruse, J. A. (1990). Clinical methods: the history, physical, and laboratory examinations. *Jama*, 264(21):2808–2809.

[Columbus 2018] Columbus, L. (2018). 2018 roundup of internet of things forecasts and market estimates. https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#51e137ea7d83. Acessado em: Abril de 2019.

[Daluz 2014] Daluz, H. (2014). *Fundamentals of Fingerprint Analysis*. Taylor & Francis.

[Dar et al. 2015] Dar, M. N., Akram, M. U., Usman, A., and Khan, S. A. (2015). Ecg biometric identification for general population using multiresolution analysis of dwt based features. In *Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on*, pages 5–10. IEEE.

[Daugman 2010] Daugman, J. (2010). How iris recognition works. *IEEE Trans. Circuits Syst. Video Technol. 14*, pages 21–30.

[Dhanvijay and Patil 2019] Dhanvijay, M. M. and Patil, S. C. (2019). Internet of things: A survey of enabling technologies in healthcare and its applications. *Computer Networks*, 153:113 – 131.

[Dodds 2019] Dodds, L. (2019). Chinese businesswoman accused of jaywalking after AI camera spots her face on an advert. `https://www.telegraph.co.uk/technology/2018/11/25/chinese-businesswoman-accused-jaywalking-ai-camera-spots-face/`. Acessado em: Maio de 2019.

[Duta 2009] Duta, N. (2009). A survey of biometric technology based on hand shape. *Pattern Recognition*, 42(11):2797–2806.

[Ericsson 2018] Ericsson (2018). Iot connections outlook. `https://www.ericsson.com/en/mobility-report/reports/november-2018/iot-connections-outlook`. Acessado em: Abril de 2019.

[Gangwar and Joshi 2016] Gangwar, A. and Joshi, A. (2016). Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition. In *2016 IEEE International Conference on Image Processing (ICIP)*, pages 2301–2305. IEEE.

[Goldberger et al. 2000a] Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., and Stanley, H. E. (2000a). Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiological signals. *circulation*, 10(23):e215–e220.

[Goldberger et al. 2000b] Goldberger, A. L., Amaral, L. A. N., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., Stanley, H. E., and et al. (2000b). Physiobank, physiotoolkit, and physionet. *Circulation*, 101(23).

[Goodfellow et al. 2016] Goodfellow, I., Bengio, Y., and Courville, A. (2016). *Deep Learning*. MIT Press. `http://www.deeplearningbook.org`.

[Gu et al. 2003] Gu, Y., Zhang, Y., and Zhang, Y. (2003). A novel biometric approach in human verification by photoplethysmographic signals. In *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on*, pages 13–14. IEEE.

[Hatzinakos and Yadav 2019] Hatzinakos, D. and Yadav, U. (2019). Photoplethysmograph (PPG) based Biometric Recognition. `https://www.comm.utoronto.ca/~biometrics/PPG_Dataset/index.html`. Acessado em: Janeiro de 2019.

[Healey and Picard 2005] Healey, J. A. and Picard, R. W. (2005). Detecting stress during real-world driving tasks using physiological sensors. *IEEE Transactions on Intelligent Transportation Systems*, 6(2):156–166.

[Insider 2019] Insider, B. (2019). Password-free smartphones are no longer the stuff of science fiction — they're everywhere. https://www.businessinsider.com/smartphone-biometrics-are-no-longer-the-stuff-of-science-fiction-2017-12. Acessado em: Abril de 2019.

[Irvine et al. 2001] Irvine, J., Wiederhold, B., Gavshon, L., Israel, S., McGehee, S., Meyer, R., and Wiederhold, M. (2001). Heart rate variability: a new biometric for human identification. In *Proceedings of the International Conference on Artificial Intelligence (IC-AI'01)*, pages 1106–1111.

[Jain and Duta 1999] Jain, A. K. and Duta, N. (1999). Deformable matching of hand shapes for user verification. In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, volume 2, pages 857–861. IEEE.

[Jain et al. 2016] Jain, A. K., Nandakumar, K., and Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80 – 105.

[Jindal et al. 2016] Jindal, V., Birjandtalab, J., Pouyan, M. B., and Nourani, M. (2016). An adaptive deep learning approach for ppg-based identification. In *2016 38th Annual international conference of the IEEE engineering in medicine and biology society (EMBC)*, pages 6401–6404. IEEE.

[Jirayucharoensak et al. 2014] Jirayucharoensak, S., Pan-Ngum, S., and Israsena, P. (2014). Eeg-based emotion recognition using deep learning network with principal component based covariate shift adaptation. *The Scientific World Journal*, 2014.

[Jung and Heo 2018] Jung, H. and Heo, Y. (2018). Fingerprint liveness map construction using convolutional neural network. *Electronics Letters*, 54(9):564–566.

[Karimian et al. 2017] Karimian, N., Tehranipoor, M., and Forte, D. (2017). Non-fiducial ppg-based authentication for healthcare application. In *Biomedical & Health Informatics (BHI), 2017 IEEE EMBS International Conference on*, pages 429–432. IEEE.

[Karpagachelvi et al. 2010] Karpagachelvi, S., Arthanari, M., and Sivakumar, M. (2010). ECG feature extraction techniques - A survey approach. *CoRR*, abs/1005.0957.

[Kate Conger 2019] Kate Conger, Richard Fausset, S. F. K. (2019). San Francisco Bans Facial Recognition Technology. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acessado em: Maio de 2019.

[Kavsaoğlu et al. 2014] Kavsaoğlu, A. R., Polat, K., and Bozkurt, M. R. (2014). A novel feature ranking algorithm for biometric recognition with ppg signals. *Computers in biology and medicine*, 49:1–14.

[Kinetz 2019] Kinetz, E. (2019). China deploys fully automated airport check-ins using facial recognition. https://www.pressherald.com/2018/10/16/fully-automated-airport-check-ins-using-facial-recognition-arrive-in-china/. Acessado em: Maio de 2019.

[Krizhevsky et al. 2012] Krizhevsky, A., Sutskever, I., and Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105.

[Kukula and Elliott 2006] Kukula, E. and Elliott, S. (2006). Implementation of hand geometry: an analysis of user perspectives and system performance. *IEEE Aerospace and Electronic Systems Magazine*, 21(3):3–9.

[Kyoso and Uchiyama 2001] Kyoso, M. and Uchiyama, A. (2001). Development of an ecg identification system. In *Engineering in medicine and biology society, 2001. Proceedings of the 23rd annual international conference of the IEEE*, volume 4, pages 3721–3723. IEEE.

[Labati et al. 2018] Labati, R. D., Muñoz, E., Piuri, V., Sassi, R., and Scotti, F. (2018). Deep-ecg: Convolutional neural networks for ecg biometric recognition. *Pattern Recognition Letters*.

[Laguna 1990] Laguna, P. (1990). New electrocardiographic signal processing techniques: Application to long-term records. *PhD. Disertation, Science Faculty, University of Zaragoza*.

[Längkvist et al. 2012] Längkvist, M., Karlsson, L., and Loutfi, A. (2012). Sleep stage classification using unsupervised feature learning. *Advances in Artificial Neural Systems*, 2012:5.

[Liu 2010] Liu, M. (2010). Fingerprint classification based on adaboost learning from singularity features. *Pattern Recogn.*, 43(3):1062–1070.

[Liu et al. 2016] Liu, N., Zhang, M., Li, H., Sun, Z., and Tan, T. (2016). Deepiris: Learning pairwise filter bank for heterogeneous iris verification. *Pattern Recognition Letters*, 82:154–161.

[Lumini and Nanni 2017] Lumini, A. and Nanni, L. (2017). Overview of the combination of biometric matchers. *Information Fusion*, 33:71 – 85.

[Mauceri 1965] Mauceri, A. (1965). Feasibility study of personal identification by signature verification. *Technical Report SID65-24 North American Aviation*.

[Merone et al. 2017] Merone, M., Soda, P., Sansone, M., and Sansone, C. (2017). Ecg databases for biometric systems: A systematic review. *Expert Systems with Applications*, 67:189 – 202.

[Miotto et al. 2017] Miotto, R., Wang, F., Wang, S., Jiang, X., and Dudley, J. T. (2017). Deep learning for healthcare: review, opportunities and challenges. *Briefings in bioinformatics*, 19(6):1236–1246.

[Nakayama et al. 2019] Nakayama, F., Lenz, P., Cremonezi, B., dos Santos, A., Nogueira, M., Chowdhoury, K., Banou, S., Rosario, D., and Cerqueira, E. (2019). Autenticação contínua e segura baseada em sinais ppg e comunicação galvânica. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*.

[Nguyen et al. 2017] Nguyen, K., Fookes, C., Ross, A., and Sridharan, S. (2017). Iris recognition with off-the-shelf cnn features: A deep learning perspective. *IEEE Access*, 6:18848–18855.

[Odinaka et al. 2012] Odinaka, I., Lai, P.-H., Kaplan, A. D., O'Sullivan, J. A., Sirevaag, E. J., and Rohrbaugh, J. W. (2012). Ecg biometric recognition: A comparative analysis. *IEEE Transactions on Information Forensics and Security*, 7(6):1812–1824.

[Oinonen et al. 2010] Oinonen, H., Forsvik, H., Ruusuvuori, P., Yli-Harja, O., Voipio, V., and Huttunen, H. (2010). Identity verification based on vessel matching from fundus images. In *Proceedings of the 17th IEEE International Conference on Image Processing ICIP, Hong Kong, September 26-29, 2010*, pages 4089–4092. Contribution: organisation=sgn,FACT1=1.

[Orjuela-Cañón et al. 2013] Orjuela-Cañón, A. D., Delisle-Rodríguez, D., López-Delis, A., de la Vara-Prieto, R. F., and Cuadra-Sanz, M. B. (2013). Onset and peak pattern recognition on photoplethysmographic signals using neural networks. In *Iberoamerican Congress on Pattern Recognition*, pages 543–550. Springer.

[Pacheco et al. 2018] Pacheco, F., Exposito, E., Gineste, M., Baudoin, C., and Aguilar, J. (2018). Towards the deployment of machine learning solutions in network traffic classification: A systematic survey. *IEEE Com. Surveys & Tuts,*.

[Page et al. 2015] Page, A., Kulkarni, A., and Mohsenin, T. (2015). Utilizing deep neural nets for an embedded ecg-based biometric authentication system. In *2015 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pages 1–4. IEEE.

[Pan and Tompkins 1985] Pan, J. and Tompkins, W. J. (1985). A real-time qrs detection algorithm. *IEEE Trans. Biomed. Eng*, 32(3):230–236.

[Politi et al. 2016] Politi, M. T., Ghigo, A., Fernández, J. M., Khelifa, I., Gaudric, J., Fullana, J. M., and Lagrée, P.-Y. (2016). The dicrotic notch analyzed by a numerical model. *Computers in biology and medicine*, 72:54–64.

[Pruzansky 1963] Pruzansky, S. (1963). Pattern-matching procedure for automatic talker recognition. *J. Acoust. Soc. Am. 35*, 73.

[Rezgui and Lachiri 2016] Rezgui, D. and Lachiri, Z. (2016). Ecg biometric recognition using svm-based approach. *IEEJ Transactions on Electrical and Electronic Engineering*, 11:S94–S100.

[Ross et al. 1999] Ross, A., Jain, A., and Pankati, S. (1999). A prototype hand geometry-based verification system. In *Proceedings of 2nd conference on audio and video based biometric person authentication*, pages 166–171.

[Russel 2019] Russel, J. (2019). Chinese police are using smart glasses to identify potential suspects. `https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/`. Acessado em: Maio de 2019.

[Sajjad et al. 2018] Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A. K., Castiglione, A., Esposito, C., and Baik, S. W. (2018). Cnn-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters*.

[Salanke et al. 2013] Salanke, N. G. R., Maheswari, N., Samraj, A., and Sadhasivam, S. (2013). Enhancement in the design of biometric identification system based on photoplethysmography data. In *Green High Performance Computing (ICGHPC), 2013 IEEE International Conference on*, pages 1–6. IEEE.

[Sancho et al. 2018] Sancho, J., Alesanco, Á., and García, J. (2018). Biometric authentication using the ppg: A long-term feasibility study. *Sensors*, 18(5):1525.

[Sarkar et al. 2016] Sarkar, A., Abbott, A. L., and Doerzaph, Z. (2016). Biometric authentication using photoplethysmography signals. In *Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on*, pages 1–7. IEEE.

[Shafer et al. 1996] Shafer, J. C., Agrawal, R., and Mehta, M. (1996). Sprint: A scalable parallel classifier for data mining. In *In Proceedings of the 22th International Conference on Very Large Data Bases*, VLDB '96, pages 544–555. Morgan Kaufmann Publishers Inc.

[Shanir et al. 2017] Shanir, P. P. M., Khan, K. A., Khan, Y. U., Farooq, O., and Adeli, H. (2017). Automatic seizure detection based on morphological features using one-dimensional local binary pattern on long-term eeg. *Clinical EEG and Neuroscience*.

[Shashikumar et al. 2017] Shashikumar, S. P., Shah, A. J., Li, Q., Clifford, G. D., and Nemati, S. (2017). A deep learning approach to monitoring and detecting atrial fibrillation using wearable technology. In *2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*, pages 141–144. IEEE.

[Su et al. 2017] Su, H.-R., Chen, K.-Y., Wong, W. J., and Lai, S.-H. (2017). A deep learning approach towards pore extraction for high-resolution fingerprint recognition. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2057–2061. IEEE.

[Sun et al. 2018] Sun, X., Wu, P., and Hoi, S. C. (2018). Face detection using deep learning: An improved faster rcnn approach. *Neurocomputing*, 299:42–50.

[Szegedy et al. 2015] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., and Rabinovich, A. (2015). Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1–9.

[Tayal et al. 2015] Tayal, D. K., Jain, A., Arora, S., Agarwal, S., Gupta, T., and Tyagi, N. (2015). Crime detection and criminal identification in India using data mining techniques. *AI and Society*, 30:117–127.

[Times 2019] Times (2019). Delhi: Facial recognition system helps trace 3,000 missing children in 4 days. `https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-`

3000-missing-children-in-4-days/articleshow/63870129.cms. Acessado em: Maio de 2019.

[Tomlinson et al. 2019] Tomlinson, W. J., Banou, S., Yu, C., Chowdhury, K. R., and Nogueira, M. (2019). Secure on-skin biometric signal transmission using galvanic coupling. In *IEEE INFOCOM*.

[Trauring 1963] Trauring, M. (1963). Automatic comparison of finger-ridge patterns. *Nature*, 79.

[Tsinganos 2017] Tsinganos, Panagiotis; Skodras, A. (2017). A smartphone-based fall detection system for the elderly. In *In Proceedings of the 10th International Symposium on Image and Signal Processing and Analysis*. IEEE.

[Turner et al. 2014] Turner, J., Page, A., Mohsenin, T., and Oates, T. (2014). Deep belief networks used on high resolution multichannel electroencephalography data for seizure detection. In *2014 AAAI Spring Symposium Series*.

[Unar et al. 2014] Unar, J., Seng, W. C., and Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8):2673 – 2688.

[Venkatesh and Jayaraman 2010] Venkatesh, N. and Jayaraman, S. (2010). Human electrocardiogram for biometrics using dtw and flda. In *Pattern recognition (icpr), 2010 20th international conference on*, pages 3838–3841. IEEE.

[Wang et al. 2016] Wang, Y., Wu, Z., and Zhang, J. (2016). Damaged fingerprint classification by deep learning with fuzzy feature points. In *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pages 280–285. IEEE.

[Wayman 2007] Wayman, J. (2007). The scientific development of biometrics over the last 40 years. *The History of Information Security: A Comprehensive Handbook, Elsevier, Amsterdam.*, 79.

[Wieclaw et al. 2017] Wieclaw, L., Khoma, Y., Fałat, P., Sabodashko, D., and Herasymenko, V. (2017). Biometric identification from raw ecg signal using deep learning techniques. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 129–133. IEEE.

[Wright 2019] Wright, M. (2019). Metropolitan Police trial facial recognition technology in central London for first time. https://www.telegraph.co.uk/news/2018/12/17/metropolitan-police-trial-facial-recognition-technology-central/. Acessado em: Maio de 2019.

[Yadav et al. 2018] Yadav, U., Abbas, S. N., and Hatzinakos, D. (2018). Evaluation of ppg biometrics for authentication in different states. In *2018 International Conference on Biometrics (ICB)*, pages 277–282. IEEE.

[Yesilbudak et al. 2017] Yesilbudak, M., Sagiroglu, S., and Colak, I. (2017). A novel implementation of knn classifier based on multi-tupled meteorological input data for wind power prediction. *Energy Conversion and Management*, 13:434–444.

[Zhang et al. 2018] Zhang, Y., Gravina, R., Lu, H., Villari, M., and Fortino, G. (2018). Pea: Parallel electrocardiogram-based authentication for smart healthcare systems. *Journal of Network and Computer Applications*, 117:10 – 16.

[Zhang and Wu 2016] Zhang, Y. and Wu, J. (2016). Practical human authentication method based on piecewise corrected electrocardiogram. In *Software Engineering and Service Science (ICSESS), 2016 7th IEEE International Conference on*, pages 300–303. IEEE.

[Zhang et al. 2016] Zhang, Y., Zhou, B., Wu, H., and Wen, C. (2016). 2d fake fingerprint detection based on improved cnn and local descriptors for smart phone. In *Chinese Conference on Biometric Recognition*, pages 655–662. Springer.

[Zhao et al. 2018] Zhao, T., Wang, Y., Liu, J., and Chen, Y. (2018). Your heart won't lie: Ppg-based continuous authentication on wrist-worn wearable devices. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pages 783–785. ACM.

[Zuo 2019] Zuo, M. (2019). China's high-tech snack shops face a sizzling problem. `https://www.businessinsider.com/china-bingo-box-convenience-store-shanghai-melting-heat-2017-7`. Acessado em: Maio de 2019.