UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE PALMAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO

UM ESTUDO SOBRE BIOMETRIA DE PESSOAS BASEADA NO PADRÃO DE VEIAS DO DEDO

ÉLENN DYPAULLA SILVA MILHOMEM

PALMAS (TO)
2021

ÉLENN DYPAULLA SILVA MILHOMEM

UM ESTUDO SOBRE BIOMETRIA DE PESSOAS BASEADA NO PADRÃO DE VEIAS DO DEDO

Trabalho de Conclusão de Curso II apresentado à Universidade Federal do Tocantins para obtenção do título de Bacharel em Ciência da Computação, sob a orietação do(a) Prof.(a) Dr. Eduardo Ferreira Ribeiro.

Orientador: Dr. Eduardo Ferreira Ribeiro

PALMAS (TO)

2021

ÉLENN DYPAULLA SILVA MILHOMEM

UM ESTUDO SOBRE BIOMETRIA DE PESSOAS BASEADA NO PADRÃO DE VEIAS DO DEDO

Trabalho de Conclusão de Curso II apresentado à UFT – Universidade Federal do Tocantins – Campus Universitário de Palmas, Curso de Ciência da Computação foi avaliado para a obtenção do título de Bacharel e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Data de aprovação: 18 / 8 / 2021

Banca Examinadora:

Prof. Dr. Eduardo Ferreira Ribeiro

Profa. Me. Juliana Leitão Dutra

Prof. Dr. Marcelo Lisboa Rocha

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

M644e Milhomem, Élenn Dypaulla Silva .

Um Estudo Sobre Biometria de Pessoas Baseada no Padrão de Veias do Dedo. / Élenn Dypaulla Silva Milhomem. – Palmas, TO, 2021.

60 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Ciências da Computação, 2021.

Orientador: Eduardo Ferreira Ribeiro

1. Identificação pessoal. 2. Reconhecimento de veias do dedo. 3. Análise de desempenho. 4. Segurança Digital. I. Título

CDD 004

Elaborado pelo sistema de geração automatica de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

Maybe this is the secret. It's not what we do, but why we do it.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela saúde e força para vencer os obstáculos que aparecem e possam aparecer.

Ao meu orientador, Eduardo Ribeiro pela oportunidade de desenvolver este trabalho, por acreditar em mim e por toda a ajuda, dedicação e incentivo durante esses anos.

Aos meus amados pais Elismar Divina e Rogério Milhomem, aos meus amados avós Bertolina Moura e Pedro Batista e aos demais membros amados da minha família Maria Sirlei, Flávia Moura, Luiz Cândido e Keith Santana, por serem minha base de força e perseverança, pelo amor, carinho, preocupação e por terem me apoiado nas minhas escolhas.

Ao meu namorado, Arthur Gabriel, pela motivação, amor, preocupação, paciência e toda a ajuda durante esse tempo.

Aos meus queridos amigos Natã Bandeira, Matheus Aguiar, Iago Tíbor, João Vitor Jacundá, Paulo Atavila, pela inestimável amizade oferecida desde o início, por toda a ajuda durante o desenvolvimento desse trabalho, pela força, companheirismo e pelos bons momentos.

A todos aqueles que de alguma forma estiveram presentes tornando esse trabalho possível.

RESUMO

Identificação biométrica é o estudo de atributos fisiológicos e comportamentais de um indivíduo para superar problemas de segurança. O reconhecimento das veias do dedo é uma técnica biométrica usada para analisar os padrões de veias das pessoas para uma autenticação adequada. Este trabalho apresenta uma revisão detalhada sobre algoritmos de reconhecimento de veias do dedo. Essas ferramentas incluem aquisição de imagens, pré-processamento, extração de recursos e métodos de correspondência para extrair e analisar padrões de resultados.

Palavra-chave: Identificação pessoal. Reconhecimento de veias do dedo. Análise de desempenho. Segurança Digital.

ABSTRACT

Biometric identification is the study of physiological and behavioral attributes of an individual to overcome security problems. Finger vein recognition is a biometric technique used to analyze finger vein patterns of persons for proper authentication. This work presents a detailed review on finger vein recognition algorithms. Such tools include image acquisition, preprocessing, feature extraction and matching methods to extract and analyze result patterns.

Keywords: Personal Identification. Finger vein recognition. Performance analysis . Digital Security.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

Abreviações

DNA Ácido Desoxirribonucleico

PIN Número de Identificação Pessoal

TSE Tribunal Superior Eleitoral

BTG British Technology Group

LED Diodo Emissor de Luz

RFID Identificação por Rádio Frequência

PIN Número de Identificação Pessoal

FAR Falsas Taxas de Aceitação

FRR Falsas Taxas de Rejeição

EER Taxa de Erro Equilibrado

FNMR Taxa de Não Correspondência Falsa

FMR Taxa de Correspondência Falsa

HFE Filtragem de Ênfase em Alta Frequência

CGF Filtro Circular de Gabor

FVR Reconhecimento de Padrões de Veias do Dedo

NIR Espectrômetro de Infravermelho Próximo

CCD Dispositivo Acoplado a Carga

ROI Região de Interesse

HSNR Relação Sinal / Ruído com Base no Sistema Visual Humano

SVM Máquina de Vetor de Suporte

SVR Máquina de Regressão de Suporte

DNN Rede Neural Profunda

USM Máscara de Nitidez

MC Algoritmo Curvatura Máxima

PC Algoritmo Curvatura Principal

1 INTRODUÇÃO

A biometria é a ciência da medição das propriedades físicas dos seres vivos, e deste modo, a identificação biométrica vem sendo a forma mais utilizada de identificar os indivíduos por suas características físicas ou comportamentais (JAIN et al., 2004).

Os sistemas biométricos podem ser usados para a autenticação de pessoas, e nessa categoria de sistema existem duas maneiras para realizar tal autenticação: a verificação e a identificação (BOLLE et al., 2013). A base da verificação está fundamentada na resposta à questão: "O usuário é quem alega ser?", deste modo, a característica biométrica é apresentada pelo usuário com uma identidade alegada, habitualmente através da digitação de um código de identificação, sendo realizada uma busca fechada em um banco de dados de perfis biométricos. Ao que corresponde a identificação, a questão a ser respondida é: "Quem é o usuário?", em vista disso, o usuário fornece apenas sua característica biométrica, cabendo ao sistema a tarefa de identificar o usuário, realizando neste caso, uma busca aberta no banco de dados (BOLLE; CONNELL; RATHA, 2002).

Apesar de a biometria se fazer cada vez mais presente no dia-a-dia das pessoas e ser adotada por bancos e empresas em todo o mundo, ela acaba recebendo diversas críticas quanto à sua eficácia, por ser uma tecnologia sujeita a falhas como, por exemplo, com usuários que obtiveram modificações na impressão causadas por cortes ou cicatrizes, ou até mesmo a falta da impressão, quando se trata de pessoas com diabetes ou que manipulem químicos em seu trabalho (HONG; WAN; JAIN, 1998). Sendo assim, dentre as diversas tecnologias existentes, há algumas pouco conhecidas pelo público geral que se encarregam de fazer a mesma função como, por exemplo, a de reconhecimento de veia de dedo, ou biometria vascular.

Por ser um método que trabalha com características biométricas intrínsecas, ele exige esforços mais desafiadores para adquirir sem o conhecimento do indivíduo, portanto mais difícil de forjar. Por utilizar recursos que estão escondidos no corpo humano, pode ser dito como uma tecnologia biométrica líder atualmente em segurança e conveniência, implementada em sistemas de segurança de bancos (KONO, 2000).

Este trabalho visa um estudo dos métodos de identificação pessoal modernos baseados em biometria, tendo como foco dessa monografia o reconhecimento biométrico através do padrão de veias do dedo, por ser uma tecnologia em ascensão, assim como uma descrição dos algoritmos aplicados para realizar tal reconhecimento.

1.1 Objetivo Geral

O presente trabalho visa realizar uma revisão bibliográfica sobre os principais métodos de biometria existentes, com ênfase no método de identificação biométrica baseada no padrão de veias do dedo, abordando a criação e os processos de aplicações atuais de cada um dos mesmos.

Em seguida realizar um estudo de dois algoritmos selecionados de processamento de imagens, realizar uma simulação testando-os em um banco de dados de imagens e comparar os resultados, analisando qual apresentou um melhor desempenho.

1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Realizar uma revisão bibliográfica sobre os principais conceitos relacionados à biometria de veias;
- Estudar e selecionar dois algoritmos de reconhecimento de veias;
- Apresentar e descrever os dois algoritmos selecionados;
- Simular e testar os dois algoritmos aplicados a base de dados selecionada;
- Comparar e analisar os resultados dos dois algoritmos escolhidos;

1.3 Justificativa

A biometria é um ótimo recurso para identificação pessoal, apresentando características que facilitam o processo como, por exemplo, a universalidade, unicidade, facilidade de coleta e grande aceitação pública. No entanto, devido ao alto índice de fraudes a que estamos suscetíveis, é imprescindível que haja um sistema que realize a identificação biométrica de pessoas com um maior nível de excelência. Para realizar este controle existem inúmeras tecnologias, contudo, a tecnologia de reconhecimento de indivíduos através do padrão de veias do dedo é a mais recente dentre as mesmas, por conseguinte sendo também a que oferece a melhor prevenção contra fraudes. Isso ocorre devido ao fato desta tecnologia utilizar-se de padrões de veias para realizar o reconhecimento biométrico, o que oferece segurança, eficácia e comodidade, podendo substituir os métodos convencionais de autenticação ou identificação que são mais utilizados atualmente.

Deste modo, a realização desta monografia tem como finalidade desenvolver um estudo e realizar testes com algoritmos de processamento de imagem, a partir do levantamento bibliográfico, sobre o tema de biometria, com ênfase no tópico de biometria vascular, que ainda é pouco abordado, mas que agrega valor acadêmico e profissional ao graduando de Ciência da Computação.

1.4 Estrutura do Trabalho

O trabalho está organizado em 5 capítulos conforme serão descritos a seguir.

O capítulo 1 apresenta a introdução e descreve os objetivos e a justificativa para o desenvolvimento do trabalho.

O capítulo 2 aborda assuntos como as etapas e técnicas básicas de processamento de imagem e realiza a revisão da literatura básica necessária para compreender conceitos específicos do trabalho, como os fundamentos de biometria e as várias categorias de biometria existentes. Também é abordado neste capítulo uma seção que apresenta uma introdução e conceitualização referente ao reconhecimento de padrões das veias do dedo. Nesta seção são descritas também as técnicas utilizadas para o processo de reconhecimento de padrões de veias e uma breve visão do toolkit que possui ferramentas referentes à esse tipo de biometria que será utilizado. Também é explanado acerca dos algoritmos que serão testados.

O capítulo 3 é referente à metodologia empregada no trabalho, a qual encontra-se dividida e descrita em cinco etapas como se dará o desenvolvimento do mesmo, para fins de melhor compreensão.

O capítulo 4 é referente aos resultados dos testes, onde há comparações entre as taxas de erro e aceite de cada um dos dois algoritmos.

O capítulo 5 é referente à conclusão do trabalho, considerações finais e sugestões para trabalhos futuros.

2 REVISÃO DE LITERATURA

Neste capítulo são apresentados os subsídios para se poder compreender e relacionar este a outros trabalhos. Assim, são apresentados também conceitos acerca de imagem digital e fundamentos de Processamento de Imagens, tal como o funcionamento das principais etapas do processo. Por fim, é explanado acerca da Biometria na totalidade, bem como os métodos de identificação pessoal, as técnicas e algoritmos atualmente utilizados. Será apresentado detalhadamente a Biometria Vascular, sua origem, principais características e como pode ser aplicada.

2.1 Fundamentos de Processamento Digital de Imagens

2.1.1 Conceito e Evolução de Processamento de Imagem

No início dos anos 20 surgiram as primeiras utilizações de imagens digitais a partir do sistema Bartlane, que fazia transmissão intercontinental de imagens por cabo submarino (RENSEN, 2010).

Porém, somente em meados de 1964, técnicas voltadas para a análise de dados multidimensional adquiridos por diversos categorias de sensores receberam o nome de processamento digital de imagens. As mesmas faziam manipulação de uma imagem por computador, de modo onde a entrada e a saída do processo são imagens, tais como fotografias ou quadros de vídeo. Desde então, são utilizadas para melhorar o aspecto visual de certas feições estruturais para o analista humano e para fornecer outros subsídios para a sua interpretação, inclusive gerando produtos que possam ser posteriormente submetidos a outros processamentos (BHABATOSH et al., 2011).

De maneira oposta ao tratamento de imagens, onde a maior preocupação está somente na manipulação de figuras para sua representação final, o processamento de imagens é um estágio para novos processamentos de dados, tais como aprendizagem de máquina ou reconhecimento de padrões (BAXES, 1994).

2.1.2 Aplicações de Processamento de Imagem

A principal relevância da utilização dos métodos de processamento de imagem digital origina-se das suas duas principais áreas de aplicação, que são: o aperfeiçoamento da informação pictórica para interpretação humana e o processamento de informações de cena para assimilação da máquina. Na segunda área, o interesse é centralizado em métodos que extraem informações de uma imagem em um formato que melhor se ajuste à um computador em processamento (ACHARYA; RAY; GALLAGHER, 2006).

Dentre os principais exemplos de aplicação, estão inclusos o reconhecimento automático de carácter, reconhecimento militar, visão de máquina para montagem e inspeção, processamento de impressões digitais, etc (BAXES, 1994).

Para que o processamento da imagem ocorra, existem etapas fundamentais. Algumas delas que são pertinentes à este trabalho são descritas a seguir:

2.1.3 Aquisição de Imagem

Para que cada categoria de imagem seja adquirida existem variadas categorias de sensores e técnicas e em todas essas técnicas imagiológicas, com algumas ressalvas, está envolvido um mapeamento de uma cena 3D em um espaço 2D. Da maioria dos sensores usados para produção de imagem, é possível obter como resultado uma voltagem contínua em forma de onda cuja amplitude e comportamento espacial estão relacionadas com o fenômeno físico sendo estudado (GONZALEZ; WOODS, 2002).

2.1.3.1 Equalização de Histogramas

A técnica de equalização de histograma consiste no ajustamento da escala de cinza de uma imagem para que o histograma de níveis de cinza da imagem de entrada seja mapeado em um histograma uniforme (ACHARYA; RAY, 2005). Consequentemente, a obtenção do mesmo a partir de uma imagem inicial é o objetivo da equalização.

2.1.4 Representação Matricial

Uma imagem matricial é a representação de uma imagem bidimensional usando números binários codificados, de modo a permitir seu armazenamento, transferência, impressão ou reprodução, e seu processamento por meios eletrônicos (MANSSOUR; COHEN, 2006).

Na representação matricial, a imagem é descrita por um conjunto de células em um arranjo espacial bidimensional, ou seja, uma matriz (MANSSOUR; COHEN, 2006). Cada célula representa os píxeis da imagem e os objetos são formados a partir da utilização adequada desses píxeis.

As imagens matriciais são chamadas também de ”bitmaps”(mapa de bits) e a representação matricial é usada para formar a imagem na memória e nas telas de computador, como é exemplificado na figura 2.1. (BAXES, 1994).

Figura 2.1 – Representação da Imagem Matricial ou Mapa de Bits
Fonte: BYD (2016)

Existem ainda as vantagens e desvantagens das imagens matriciais, que serão listadas a seguir:

Vantagens das imagens matriciais

- Possui fácil tradução para dispositivos baseados em pontos (monitores, impressoras, etc);
- Possui fácil armazenamento e leitura;
- Os valores dos píxeis podem ser alterados individualmente ou em grupo;

(EKSTROM, 2012)

Desvantagens das imagens matriciais

- As imagens podem ser muito grandes;
- Pode haver dificuldade em realizar operações de escalas;

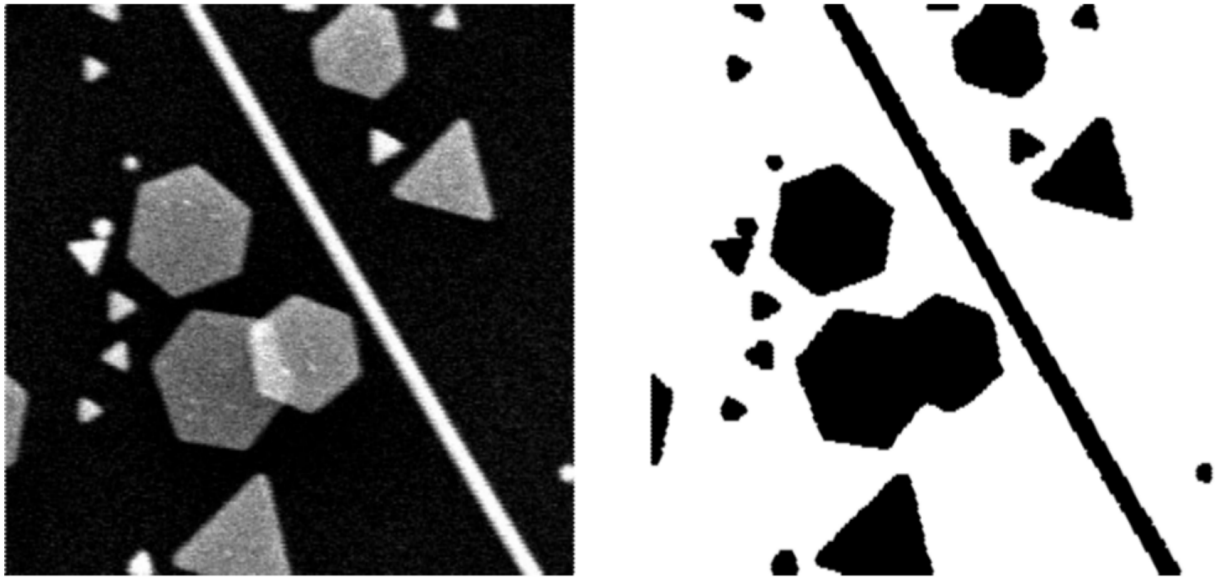
(EKSTROM, 2012)

2.1.5 Thresholding (Limiarização)

Thresholding, também conhecido como limiarização é uma técnica utilizada para segmentar imagens em tons de cinza. O limiar nada mais é do que uma constante que representa o limite entre duas regiões de cores.

A técnica consiste na decomposição de uma imagem digital em dois grupos de píxéis, os que possuem um nível de cinza abaixo do limiar e os que possuem um nível de cinza acima do limiar (AZEVEDO; CONCI, 2003), atribuindo valores diferentes de cor para ambas as regiões. A Figura 2.2, apresenta uma imagem binarizada por Thresholding.

Figura 2.2 – Exemplo de aplicação de Limiarização sobre uma imagem.
Fonte: BYD (2016)



Um dos desafios da área de processamento de imagens, é a determinação de valores adequados do limiar. Para a realização de tal tarefa, existem diversos tipos de abordagens, que podem ser divididas em três categorias:

- Threshold global: um único valor aplicado à toda a imagem;
- Threshold local: um valor de limiar é definido para cada pixel;
- Threshold adaptativo: utiliza uma ideia de separação da imagem em sub-regiões e, para cada uma é determinado um valor de limiar.

2.2 Fundamentos de Biometria

2.2.1 Definição

Biometria é uma palavra originária do grego que significa “Medida da vida” e baseia-se sobretudo em medições de características humanas, que podem ser tanto físicas quanto comportamentais e são utilizadas para identificação de pessoas. Através de sistemas biométricos pode ser realizada a devida identificação de uma pessoa, utilizando para isto métodos como: a impressão digital, geometria da mão, geometria da face, estrutura da íris, estrutura da retina, padrão de assinatura, padrão de voz, padrão de veias das mãos, dedos e dos pulsos, código genético (”DNA”), entre outros (BRÖMME, 2003).

Conforme o site dos Consultores Biométricos Associados (IBIOMETRICA, 2010), a princípio, as aplicações biométricas restringiam-se apenas à sistemas de alta segurança, porém atualmente, visto que os sistemas biométricos se aproximam cada vez mais do uso em massa, este fato está sendo ultrapassado. Esse avanço se deve a ruptura de fatores limitante, vencidos pelo avanço da tecnologia, pesquisas incessantes no assunto pelo mundo todo e redução do custo dos sistemas.

Existem diversos equipamentos biométricos e os mesmos alcançam sempre níveis de segurança elevados, que podem ser distinguidos em três níveis: o nível mais baixo

sendo algo que se possui como, por exemplo, um cartão de identificação com uma foto; o segundo nível sendo algo que se sabe como, por exemplo, uma senha para acessar um celular ou até mesmo um PIN, utilizado num caixa de banco; o nível de segurança mais alto sendo uma tecnologia biométrica, ou seja, algo que se faz e algo que faz parte do próprio ser (PINHEIRO, 2008).

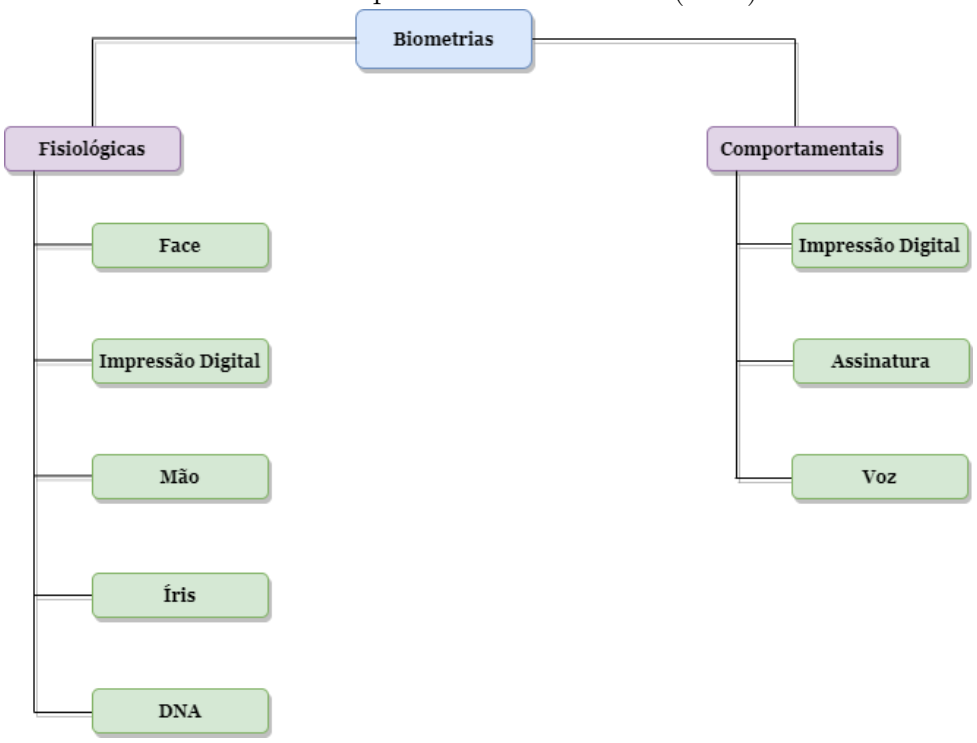
Ainda segundo o site dos Consultores Biométricos Associados (IBIOMETRICA, 2010), para ocorrer o reconhecimento durante o desenvolvimento de sistemas de identificação biométricos, são necessárias características físicas e comportamentais, tais como as listadas a seguir:

- Devem ser singulares, ou seja, serem únicas tão quanto possível como, por exemplo, um traço idêntico, mas que é único de pessoa para pessoa.
- Devem ser universais, ou seja, existirem na maior quantidade de pessoas possíveis.
- Devem poder serem medidas com instrumentos técnicos simples.
- Devem ser fáceis e confortáveis de serem medidas.

2.2.2 Tipos de Biometria

De acordo com o site Ibiometrica (IBIOMETRICA, 2010), os tipos biométricos são comumente classificados em duas categorias: fisiológicas e comportamentais. Essa separação pode ser vista na Figura 2.3.

Figura 2.3 – Tipos de Biometria
Fonte: Adaptado de IBiometrica (2010)



Tendo em vista na figura 2.2 acima, a impressão digital se faz presente em ambas as categorias, sendo o motivo justificado pelo fato de que as linhas da impressão, as características extraídas, encontram-se nas mãos, uma parte do corpo humano que é essencialmente utilizada diariamente. Sendo assim, estão diretamente ligadas ao comportamento e sujeitas a alterações físicas tais como, o uso excessivo de produtos que contenham substâncias fortes, que acarretam o clareamento dessas linhas, cortes ou até mesmo a perda do membro.

Fisiológicas

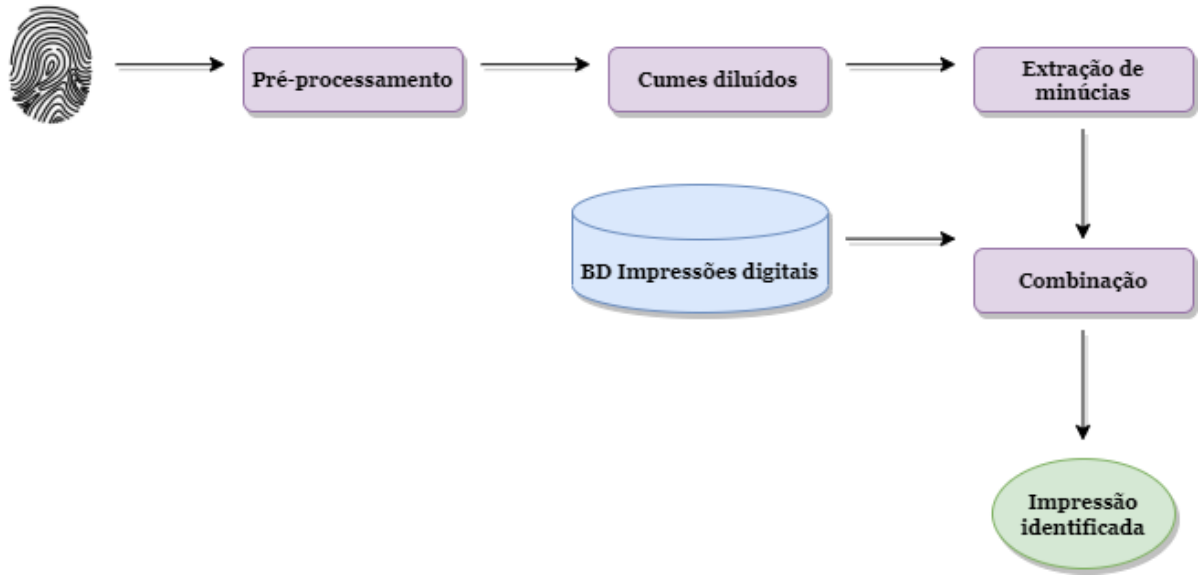
Como o próprio nome já indica, na categoria fisiológica, estão relacionadas características do corpo, como, por exemplo o formato, espessura, tamanho e outros parâmetros. Segundo as pesquisas, as categorias de biometria que fazem parte desse grupo serão descritos em sequência.

2.2.3 Reconhecimento da Impressão Digital

O primeiro sistema de identificação por impressões digitais foi criado por Francis Galton, através de observações feitas por outros autores e se tornou uma das técnicas de identificação biométrica mais utilizadas no mundo desde o fim do século XIX, sobretudo em análises forenses. Este sistema utiliza equipamentos que capturam imagens dos dedos, mais frequentemente do indicador ou polegar. A partir desta imagem, é realizado o pré-processamento para fornecer uma imagem robusta da região de interesse, em seguida ocorre a diluição dos cumes ao redor da região que forma as dimensões do polegar; As características chamadas de ”minúcias”são analisadas e combinadas com as imagens de impressões digitais armazenadas no banco de dados. Após as minúcias serem reconhecidas, os algoritmos são aplicados para transformar as posições coletadas em informações digitais e a impressão digital é identificada.

Na figura 2.4 é possível visualizar as etapas do processo de detecção da impressão digital.

Figura 2.4 – Processo de Detecção da Impressão Digital
Fonte: Adaptado de Bayometric (2013)



As imagens adquiridas são de baixa dimensão, assim os equipamentos costumam ser pequenos e de baixo custo, podendo ser instalados em aparelhos menores, como celulares, notebooks, dentre outros que necessitam da identificação do usuário para o controle de acesso lógico. Existem algumas fechaduras eletrônicas que também possuem um leitor de impressões digitais para abertura das portas, e estes sistemas são usados tanto para controle residencial quanto para uso comercial como, por exemplo, a abertura de salas de servidor de informática (JANES, 2009).

Os principais algoritmos fundamentam-se na esqueletização da imagem, ou seja, os processos e etapas que ocorrem após a captura da imagem, sendo esses:

- A normalização, onde é feita uma aplicação de filtros para melhoramento de contraste;
- Posteriormente é feita uma transformação de imagem colorida em imagem com tons de cinza apenas;
- É realizada a extração da região de interesse com correção indevida de rotação;
- Em seguida é feita a aplicação das técnicas de threshold;
- Por fim, é feita a extração das linhas que formam a impressão digital.

Quando essas linhas são extraídas, o algoritmo as digitaliza, levando em consideração a sua dimensão única, e faz uma verificação da existência das terminações, núcleo, bifurcações e deltas, e cria então dados que serão utilizados para identificação da pessoa (Balti; Sayadi; Fnaiech, 2012).

Além da vantagem do sistema possuir um baixo custo citada anteriormente, também há uma facilidade na utilização por parte dos usuários, o que acaba gerando uma alta divulgação e faz com que as pessoas tenham uma maior aceitabilidade. Porém, alguns fatores como cortes, fissuras nos dedos ou até mesmo sujeira, podem interferir no desempenho da tecnologia, o que causa falsas rejeições. Ainda há outro grande fator que causa rejeição quanto a utilização deste sistema em países asiáticos, por exemplo, onde existem grandes surtos de gripes e altas chances de contaminação, devido a necessidade do toque do usuário para que seja coletada a imagem (COSTA; OBELHEIRO; FRAGA, 2006).

O Brasil implementou recentemente pelo TSE (Tribunal Superior Eleitoral), sistemas de coleta de impressão digital para identificar as pessoas e controlar as votações em épocas eleitorais. Contudo, o sistema não abrange ainda todas as regiões do Brasil, pois está em fase de teste, e conforme informações do TSE, o sistema tem se mostrado bastante eficiente na identificação correta das pessoas (BARBOSA, 2014).

Também no Brasil, sistemas semelhantes aos implantados no TSE estão sendo utilizados em Departamentos de Trânsito para controle de treinamento prático por pessoas que pretendem obter uma carteira de habilitação, entretanto diversas fraudes foram relatadas pela imprensa, onde estavam sendo elaboradas próteses de silicone em formato de dedo que passavam ilesas na hora da identificação (JANES; JÚNIOR, 2014).

2.2.4 Reconhecimento da Face

A partir dos anos 60 os detalhes faciais foram utilizados quando o governo dos Estados Unidos contratou uma empresa para desenvolver um sistema semiautomático que

analisasse fotos para encontrar características como olhos, orelhas, nariz e boca (PAYNE, 2000).

A tecnologia de reconhecimento da face também utiliza câmeras convencionais de baixo custo que faz com que a aceitação pelas pessoas seja mais alta, devido o método não ser intrusivo. As imagens são captadas através de câmeras fotográficas ou filmadoras e são sistemas interessantes por parte dos órgãos de defesa e justiça, pois é possível analisar a identidade de uma pessoa sem que ela saiba e evitar, por exemplo, um ataque terrorista em aeroportos ou para controlar a travessia de pessoas em fronteiras (JAIN et al., 1999).

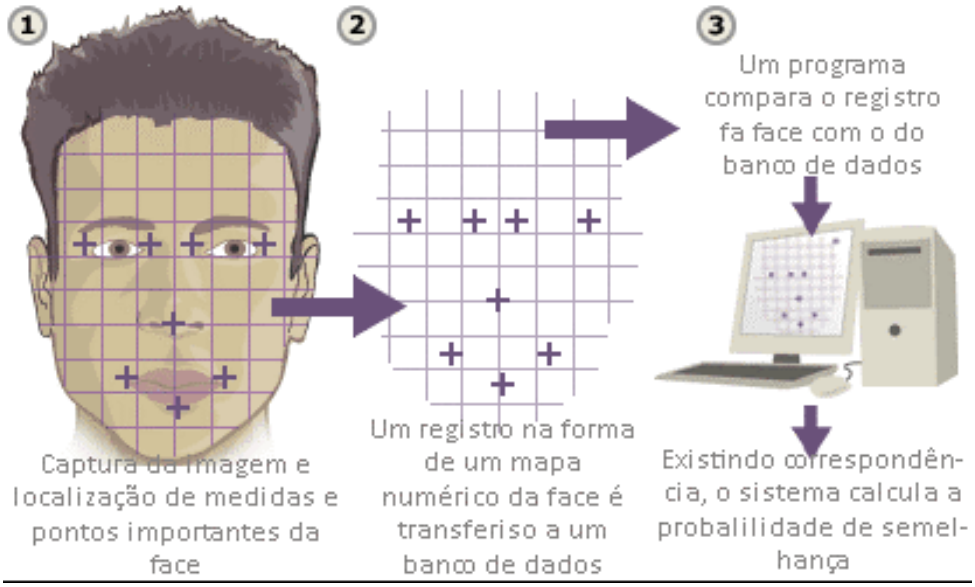
Como em todas as outras tecnologias, há alguns fatores que levam ao sistema a geração de falsas rejeições que podem afetar o nível de segurança como, por exemplo, a variação da fisionomia da pessoa devido à idade, presença de óculos ou barba, entre outros.

A técnica utiliza um software de análise que identifica pontos importantes da face, como as bordas da boca, bordas dos olhos, nariz e seus cantos, medidas da largura e altura do rosto e todas as relações entre estas áreas. Após a imagem ser capturada, os fatores necessários à identificação de uma pessoa são extraídos e os dados armazenados em um banco de dados, como um registro na forma de um mapa numérico da face, para uma futura comparação. Após a comparação, existindo correspondência, o sistema calcula a probabilidade de semelhança (SAVVIDES; KUMAR; KHOSLA, 2004).

As análises biométricas podem ser feitas através de um algoritmo singular ou pela aplicação de vários algoritmos, em duas dimensões da imagem ou em três, levando em consideração que o primeiro método é menos eficiente e mais sujeito a falsificações, pois pode ser utilizada uma fotografia da pessoa para gerar uma falsa aceitação pelo dispositivo, ao passo que na análise tridimensional, o sistema é bastante criterioso e necessita um equipamento específico e com maior custo, ampliando também o nível de intrusão, onde o usuário necessita de um conhecimento prévio para geração correta da imagem (ACHERMANN; BUNKE, 1996).

Pode-se visualizar na figura 2.5 as etapas do processo de identificação de uma pessoa através da face:

Figura 2.5 – Processo de Detecção da Face
Fonte: Adaptado de Biometrics (2015)



O fato ruim de ter um dispositivo eletrônico construído com uma câmera que pode efetuar capturas de imagens é a chance de alguém ter sua imagem capturada sem o seu consentimento e utilizá-la para atos criminosos. Seguindo este mesmo assunto, na atualidade existem diversos tipos de relatos sobre a criação de um banco de dados de faces (rostos) capturados pela empresa Facebook (projeto Deep Face) por meio das imagens colocadas no perfil do usuário do sistema.

Na atualidade, segundo especialistas, cerca de 300 milhões de faces são analisadas por dia sem o conhecimento do dono da imagem. Isso pode ocorrer através da captura de imagens de softwares gratuitos de reconhecimento facial para celulares, para plataforma híbrida (tanto IOS quanto Android), ou até mesmo pelo uso de imagens colocadas em perfis de rede social como, por exemplo, da empresa Facebook, a qual já possui diversos relatos sobre a criação de um banco de dados de faces capturadas pela mesma (projeto Deep Face) (LYNCH, 2012).

2.2.5 Geometria das Mãos

Esta categoria de sistema também está entre as mais antigas ferramentas biométricas utilizadas para reconhecimento de pessoas. Desde o final dos anos 70, diversas patentes deste tipo de sistema foram emitidas e dispositivos de controle de acesso têm sido fabricados e comercializados. Estes dispositivos são usados principalmente em aeroportos, hotéis, oficinas nucleares, dentre outros, no decorrer dos últimos 40 anos (SANCHEZ-REILLO; SANCHEZ-AVILA; GONZALEZ-MARCOS, 2000).

Contudo, a biometria baseada em características extraídas da mão desperta um grandioso interesse na área acadêmica, tendo em vista o progresso na análise em visão artificial e processamento e análise de imagem.

Os sistemas de reconhecimento baseados na mão apresentam elevada confiança baseando-se na hipótese de que ao menos em pequenas populações não existem mãos idênticas e que estas características não sofrem grandes mudanças ao passar dos anos. Também possuem baixo custo e são dispositivos fáceis de interagir para o usuário (SANCHEZ-REILLO, 2000).

Apesar de ser um argumento válido, há vários fatores que tornam o sistema vulnerável a fraudes, gerando falsas rejeições como, por exemplo, cortes na mão, sujeira, aumento do peso corporal da pessoa, anéis e pulseiras. Deste modo, como estes fatores afetam o nível de segurança do sistema, habitualmente o mesmo é utilizado somente para a autenticação, e a identificação é realizada através do uso de crachás ou outro documento que ateste a identificação pessoal (SANCHES; ANTUNES; CORREIA, 2007).

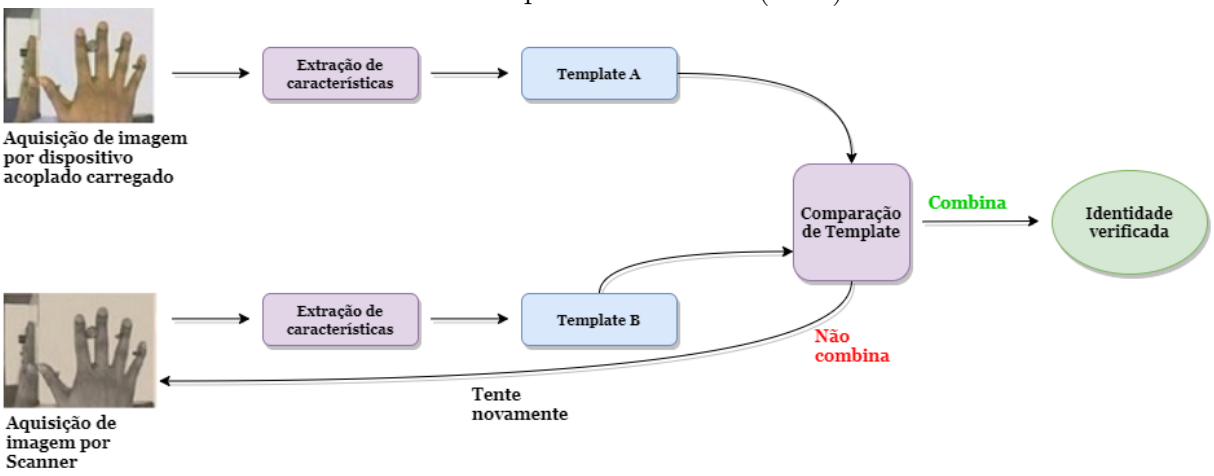
Um dispositivo composto por câmera e um conjunto de lentes e espelhos é um dos responsáveis pela aquisição da imagem das mãos tridimensionalmente. Posteriormente, é feita uma análise da largura das mãos, bem como posições das juntas dos dedos, comprimento dos dedos, área total e vários outros pontos de análise e, dessa forma, as características são extraídas e armazenadas em um modelo A. Este mesmo processo também é realizado em um dispositivo de scanner e as características são armazenadas em um modelo B. Um algoritmo específico extrai estes conjuntos de características, calcula e as armazena para que seja feita a comparação de template e verificação da identidade. Com base no resultado da comparação, a identidade reivindicada é aceita (combina) ou negada(não combina), ou uma nova identidade é atribuída (DELAC; GRGIC, 2004).

A grande desvantagem deste método é a forma como a mão é posicionada no dispositivo e para solucionar isso, grande parte dos equipamentos possuem pinos de alinhamento, que impedem que a pessoa rotacione as mãos no momento da aquisição da

imagem (JAIN; FLYNN; ROSS, 2007).

Pode-se visualizar na figura 2.6 as etapas do processo de identificação de uma pessoa através da geometria das mãos:

Figura 2.6 – Processo de Detecção da Geometria das Mãos
Fonte: Adaptado de Infosec (2018)



Devido ao equipamento ocupar um espaço pequeno de armazenamento, se torna perfeito em locais de grande acesso, como Universidades ou estádios. Além do mais, a primeira vez que o sistema foi testado em grande escala foi durante os jogos olímpicos de 1996 para controlar o acesso à vila olímpica (MARAN, 2009).

2.2.6 Reconhecimento da Íris

Em 1936, Frank Burch introduziu a ideia do uso da textura da íris como característica biométrica importante na identificação de pessoas. Em seguida, Jammes Daggarts documentou a teoria em 1949. Finalmente, em 1987, o uso da textura da íris como padrão biométrico foi de fato patenteado pelos oftalmologistas Aran Sar e Leonard Flom (COSTA, 2009).

O pesquisador John Daugman da Universidade de Cambridge implementou pela primeira vez esta técnica como ferramenta para identificação em 1993, e criou um algoritmo chamado de íris code, baseado na transformada de Wavelet e com o uso do filtro de Gabor, para a extração das características da íris, que se tratava de uma sequência de 256 bytes para a representação da íris. Daugman deixava as imagens capturadas da íris expostas à luz infravermelha de espectro próximo, pois ele acreditava que este tipo de iluminação apontava mais características de textura do que quando vista a olho nu (DAUGMAN, 2001).

A partir desta data, o uso da íris como característica biométrica foi elaborado em diversos trabalhos por outros autores, entretanto, todos tiveram como base a proposta de Daugman (LI; SAVVIDES, 2013).

A íris é um músculo no olho, a parte visível do olho humano responsável pela coloração e com pigmentação específica para cada pessoa (com exceção de albinos). É composta por uma rede de ligamentos cruzados formados por volta do oitavo mês de gestação, formando-se a cor cerca de um ano após o nascimento (MATHEW, 1989).

A região onde a íris se encontra é protegida de agentes externos pela córnea, pois se localiza entre a mesma e o cristalino. Dentro da íris, precisamente no centro, encontra-se

a pupila que controla a quantidade de luz no olho através da dilatação, fazendo com que as dimensões visíveis da íris variem. Em volta dela está a esclera, a parte branca do olho (GAZZANIGA; HEATHERTON, 2007).

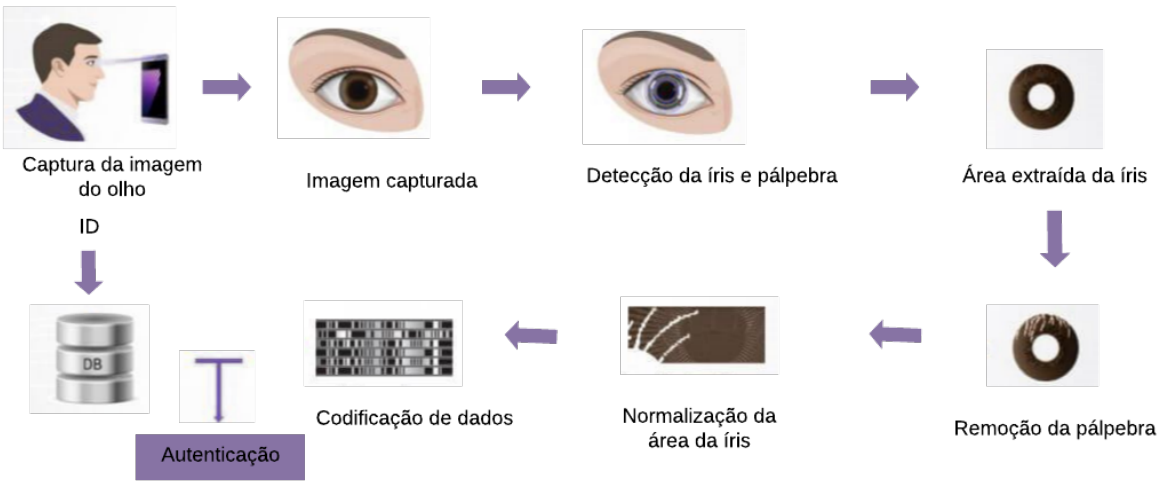
A retina é encontrada atrás do olho e é responsável pela formação das imagens. Uma característica fundamental da íris, que a torna um ótimo meio para se reconhecer indivíduos através da biometria, é a sua unicidade, ela possui cores e texturas diferentes mesmo entre olhos direito e esquerdo da mesma pessoa, e em sua composição é possível verificar diferenças entre as características que compõem a íris, fazendo com que a mesma seja praticamente única quando comparadas as íris de várias pessoas (CHIRCHI; WAGHMARE; CHIRCHI, 2011).

Portanto, a íris tem bastante eficácia aplicada em sistemas biométricos, pois a probabilidade de uma íris ser idêntica a outra é cerca de 1 em 1072. Essa probabilidade praticamente garante que não haverá nenhuma íris idêntica a outra no mundo (DAUGMAN, 2002).

A tecnologia de leitura da íris é 12 vezes mais precisa que a análise da impressão digital. O algoritmo criado por (DAUGMAN, 2007) analisa cerca de 600 pontos de características da íris, ao tempo em que se comparado com outros sistemas biométricos, como, por exemplo, a impressão digital, a quantidade de minúcias fica na ordem de 50 pontos. Grande parte da eficácia dessa tecnologia ocorre devido aos equipamentos utilizados para realizar a leitura da íris, que são capazes de identificar até mesmo uma pessoa com o uso de lentes de contato, apesar de ser orientada a retirada de óculos escuros, principalmente se o mesmo possuem lentes polarizadas no momento da aquisição da imagem, o que pode alterar a imagem a ser analisada, bem como os resultados (HENTATI; HENTATI; ABID, 2012).

O processo de identificação de uma pessoa através do uso da íris consiste nos seguintes passos mostrados na figura 2.7 e descritos a seguir.

Figura 2.7 – Processo de Detecção da Íris Utilizado pelo Aparelho Celular Samsung Note 7
Fonte: Adaptado de NewsRoom (2016)



- Detectar a presença do olho na imagem, usando como referência as pálpebras superior e inferior;
- Definir os limites da íris, usando sua borda externa e a pupila como referência;
- Excluir pálpebras, cílios e outros componentes que não fazem parte da íris;
- Extrair as características da íris e armazenar estas informações em um banco de dados.

A partir do armazenamento das características no banco de dados, é feita a comparação do padrão armazenado com o padrão da pessoa a ser identificada, e o algoritmo usado por Daugman é a distância de Hamming (DAUGMAN, 2007).

Comportamentais

Essa categoria de biometria é inteiramente ligado ao comportamento da pessoa, tendo como referência, por exemplo, pausas, tons, velocidades e outros. As categorias de biometria que fazem parte desse grupo também serão descritos em sequência (HANNA; HOYOS, 2014).

2.2.7 Reconhecimento da Voz

A voz humana é gerada através da ressonância das cordas vocais, que sofre influência das cavidades nasais e do formato da boca, portanto gera uma característica singular para cada indivíduo. Deste modo, o reconhecimento de voz pode ser utilizado como característica biométrica (GONZÁLEZ-RODRÍGUEZ; TOLEDANO; ORTEGA-GARCÍA, 2008).

Sistemas comerciais para reconhecimento da fala têm estado acessíveis desde os anos 90, entretanto apesar do sucesso aparente da tecnologia, poucas pessoas os usam para evitar uma sobrecarga vocal. A maioria dos usuários de computador podem realizar tarefas como editar ou criar um documento de maneira mais rápida se usando um teclado comum ao invés da voz, mesmo considerando que muitas pessoas conseguem falar significativamente mais depressa do que podem digitar (JAISWAL, 2013).

É muito importante que no momento da aquisição da amostra a pessoa não apresente nenhum problema de saúde que possa afetar a voz como, por exemplo, amigdalites, obstrução nasal, ou tenha feito algum tipo de tratamento odontológico, uma vez que estes fatores irão influenciar no som concebido pelas cordas vocais no momento de gravação e armazenamento do padrão, bem como no futuro, gerando falsas rejeições quando o usuário for efetuar a tentativa de identificação. Condições como nervosismo ou cansaço também podem alterar o padrão de voz (RASHID et al., 2008).

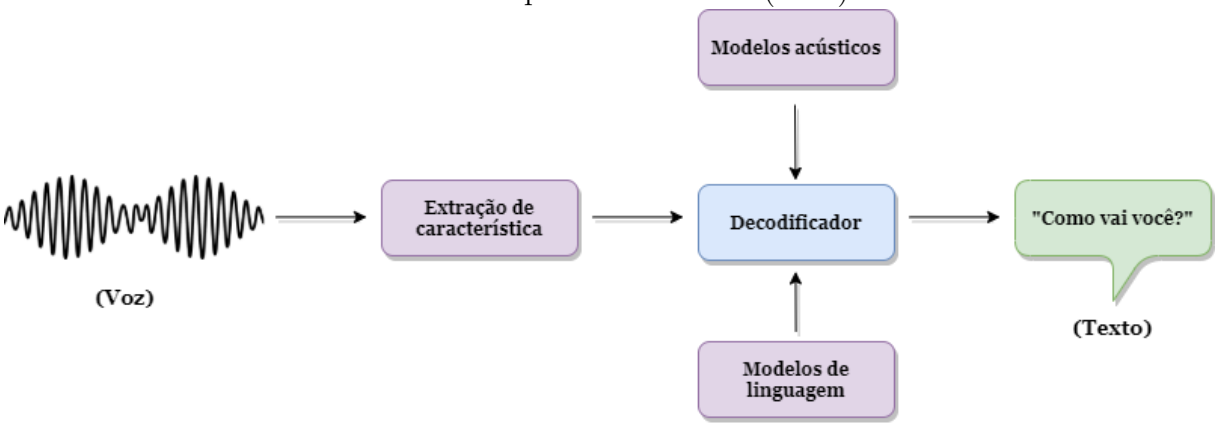
Dentre as técnicas utilizadas, existem as que testam aleatoriamente o padrão da voz humana e as que dependem de pronúncia de textos específicos. Os sistemas independentes fornecem ao usuário a possibilidade de escolher falar uma frase específica pré-cadastrada, usados para controle de acesso físicos. Já os sistemas dependentes de texto são usados normalmente em equipamentos comerciais para aquisição de acesso lógico a softwares e os mesmos geram textos que devem ser lidos pelo usuário para ser feita a análise da voz. O método de reconhecimento através da voz é utilizado não só para identificação de pessoas, mas também em algumas residências que empregam automação e utilizam os mesmos algoritmos de reconhecimento de voz para acionamento de iluminação,controle

de ar condicionado, dentre outras funções (ALSHU'EILI; GUPTA; MUKHOPADHYAY, 2011).

O processo de detecção da voz começa com a gravação de entrada da voz humana, em seguida, ocorre a extração de características em relação à voz da pessoa em questão. O próximo passo é a passagem pelo decodificador, onde há dados referentes à modelos acústicos e modelos de linguagem em formato de frases simples ditas por pessoas, que estão armazenadas em um banco de dados. Por fim, a série de Fourier realiza o reconhecimento da fala a partir de uma análise que extrai frequências específicas de cada pessoa, e logo em seguida estas informações são armazenadas com as que estão no banco de dados e comparadas (ALEY-RAZ et al., 2013).

Pode-se visualizar na figura 2.8, as etapas do processo de detecção de uma pessoa através da voz.

Figura 2.8 – Processo de Detecção da Voz
Fonte: Adaptado de Athena (2017)



O cadastro de cada usuário é feito de forma simples e necessita basicamente de um equipamento gravador com um microfone, o que faz com que estes sistemas sejam relativamente baratos, no entanto, a credibilidade se torna muito baixa e o número de falsas rejeições aumenta, pois, qualquer som ambiente pode modificar os resultados (YU; DENG, 2016).

Outro fator que torna o uso desta técnica limitado está no fato de que a voz muda ao longo dos anos, devido ao desgaste e enfraquecimento natural das cordas vocais, tornando-a mais grave, alterando assim o resultado da identificação. Pode ainda haver a situação em que a voz de uma pessoa seja gravada antecipadamente em um equipamento portátil e usada para identificação e fraude no sistema (CUI; XUE, 2009).

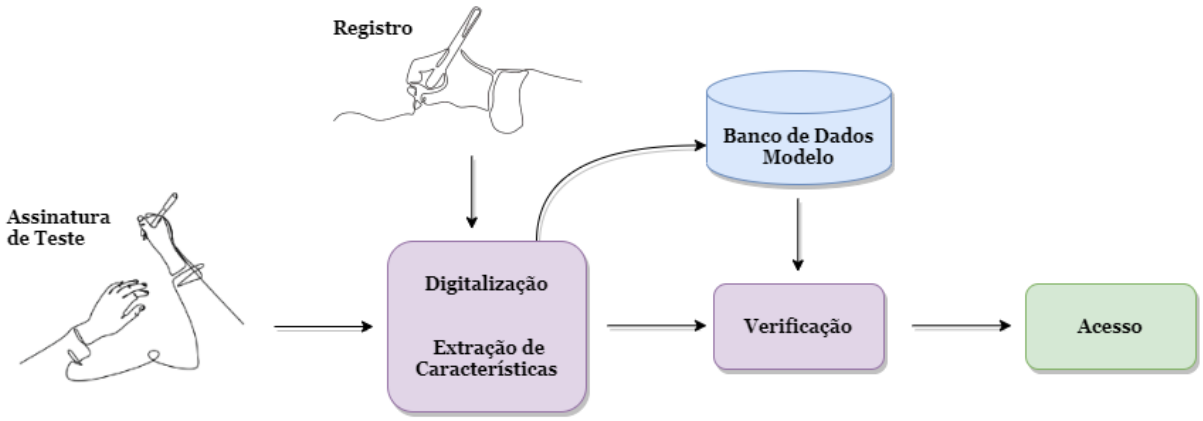
2.2.8 Reconhecimento da Assinatura

A assinatura está entre uma das mais antigas formas de biometria, empregada essencialmente na identificação de pessoas e na verificação de documentos formais. Inicialmente, o método mais utilizado no aprimoramento da veracidade de uma assinatura digital era somente o visual. Com o passar dos anos e evolução da tecnologia, houve o surgimento de métodos de validação mais avançados que levam em consideração diversos outros fatores (FABREGAS; FAÚNDEZ-ZANUY, 2009).

No contexto de biometria de assinatura, existem dois modos distintos de reconhecimento: o estático ou off-line, e o dinâmico ou online. O primeiro modo utiliza o método

menos eficiente, onde é feita uma análise da imagem estática após a assinatura ter sido realizada. No segundo, é realizada uma medição no ato de escrever, através de equipamentos baseados em scanners de mesa compostos de variados sensores que são capazes de reconhecer o ângulo, direção e pressão da escrita (assemelham-se a mousepads) (MAIORANA et al., 2010).
Pode-se visualizar na figura 2.9 as etapas do processo de reconhecimento de uma pessoa através da Assinatura:

Figura 2.9 – Processo de Reconhecimento da Assinatura
Fonte: Adaptado de Ostap (2017)



Dentre as características consideradas, estão: a pressão sobre o equipamento pela caneta, velocidade da escrita , ritmo, momentos em que a caneta não pressiona o leitor, o modo como o usuário acrescenta pontos e traços, momentos de pausa entre duas palavras, dentre outros padrões específicos para cada pessoa. Após estes dados serem registrados em um banco de dados, os mesmos são utilizados para comparação com o objetivo de identificar o indivíduo. Poucas pessoas mantêm o mesmo padrão ao longo dos anos, assim a assinatura varia, e essa é a maior desvantagem desta técnica, fazendo com que o sistema necessite periodicamente de armazenamento do padrão. Esta técnica tem maior utilização por instituições financeiras na verificação de assinatura de cheques. (PLAMONDON; PARIZEAU, 1988).

2.2.9 Reconhecimento de Padrão de Digitação

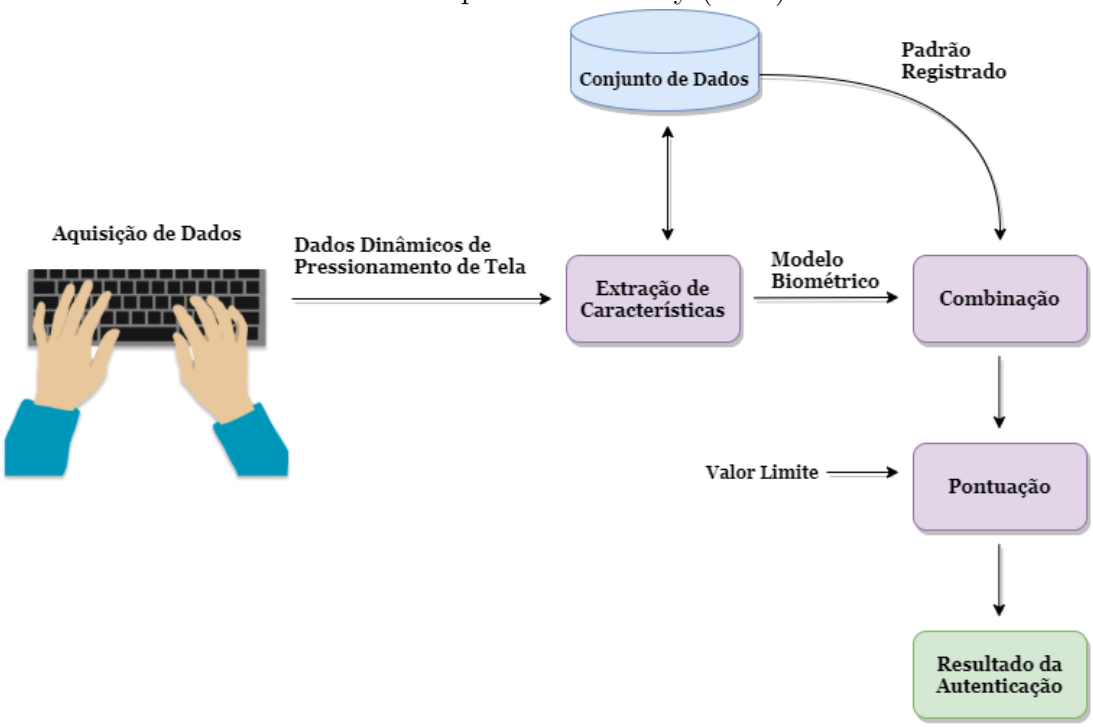
A biometria por padrão de digitação, também chamada de ”ritmo de digitação”, é um método biométrico que está fundamentalmente ligado a área de segurança de computadores. De acordo com o próprio nome, percebe-se que esse método avalia a forma como os usuários digitam no teclado seus dados de entrada, como login e senha. Sendo assim, aspectos como a sequência de valores alfanuméricos que está sendo digitada e o intervalo de tempo entre apertar uma tecla e outra em uma palavra, são extraídos como características biométricas (WONG et al., 2001).

De uma maneira geral, para aquisição de dados o sistema necessita que o usuário, na primeira interação, digite a mesma frase um determinado número de vezes e deste modo, dados dinâmicos sobre pressionamento de tecla são armazenados. Entretanto, teoricamente um sistema pode, na primeira interação, reunir a informação necessária

para encontrar um padrão, sem o conhecimento do usuário. A partir dessa etapa é feita a extração de características, estas que geram um modelo biométrico e com o conjunto de dados passam pela etapa de combinação, pontuação e por fim retorna o resultado da autenticação. O sistema também é capaz de adequar o modelo do padrão ao longo do tempo, ajustando-se a novos padrões recolhidos (ORD; FURNELL, 2000).

Pode-se visualizar na figura 2.10 as etapas do processo de reconhecimento de uma pessoa através do Padrão de Digitação:

Figura 2.10 – Processo de Detecção do Padrão de Digitação
Fonte: Adaptado de Weebly (2017)



O mais relevante nos sistemas que se utilizam dessa abordagem biométrica é que o usuário não percebe que está sendo identificado através de uma, a menos que lhe seja dito. Em contrapartida, para que o sucesso através desse método seja obtido, o usuário deve possuir uma habilidade maior de digitação, pois somente dessa maneira será mais fácil e confiável de ser reconhecido, visto que a variação intrapessoal será menor (MONROSE; REITER; WETZEL, 2002).

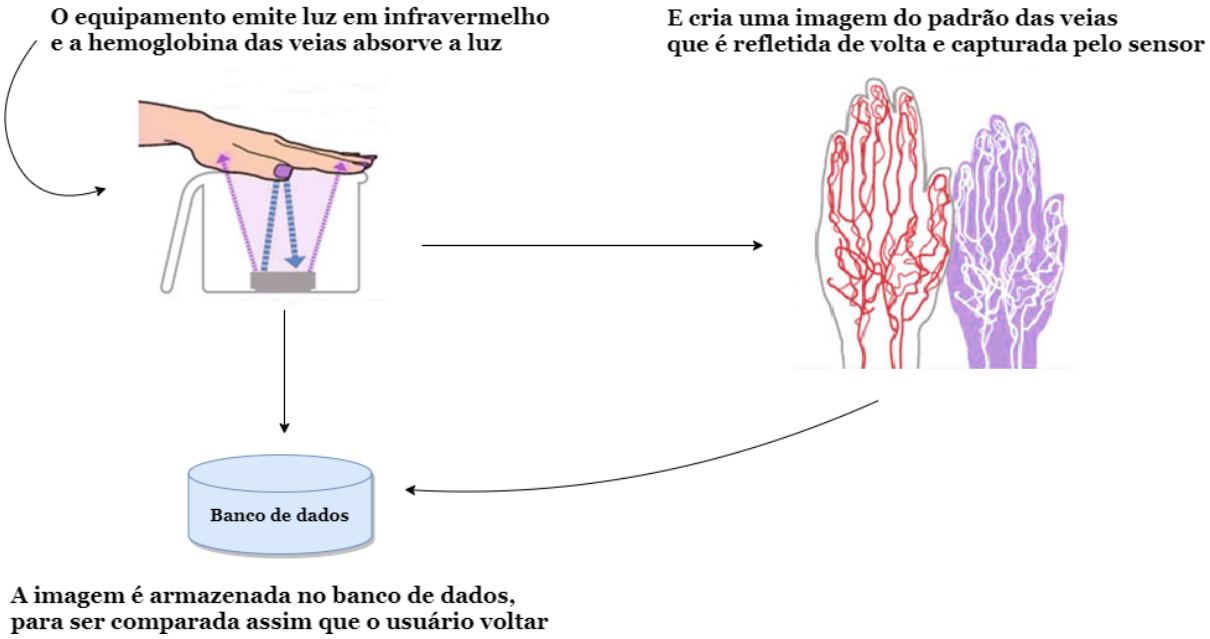
2.2.10 Reconhecimento de Padrão de Veias

A primeira pesquisa realizada sobre identificação biométrica utilizando os padrões de veias das mãos, ocorreu em Londres (UK) no ano de 1994, com o trabalho de Rice (RICE, 1994), onde o autor apresenta uma explanação breve sobre o que é biometria, e em seguida detalha sobre seu equipamento criado em 1990, o qual registrou em nome da empresa British Technology Group (BTG).

Segundo a proposta do autor, o processo consistia em iluminar a parte dorsal da mão, ou do dedo, com LEDs infravermelhos, capturando dessa maneira imagens da mão utilizando diodos fotossensíveis. Sua meta era a de que o equipamento conseguisse reconhecer e identificar adequadamente uma pessoa em até um segundo.

O processo de reconhecimento e registro é executado adquirindo duas imagens da mesma mão ou dedo, e após isto, passam-se as duas imagens por uma lógica booleana ou-exclusivo, no intuito de gerar uma terceira imagem somente com as diferenças entre as duas primeiras. Em seguida, é realizada a binarização da imagem por um algoritmo matemático (não citado pelo autor) e os dados são armazenados em um banco de dados, onde cada figura incorpora um cabeçalho com informações do indivíduo. Pode-se visualizar na figura 2.11 as etapas do processo de reconhecimento de uma pessoa através do padrão de veias:

Figura 2.11 – Processo de reconhecimento de Padrão de veias
Fonte: Adaptada de Tulyakov (2006)



Durante o processo de autenticação há padrões vasculares subjetivos que são analisados rigorosamente, dentre eles a singularidade, a estabilidade, a independência de contaminações e cicatrizes ou outros fatores externos.

Por se tratar de uma técnica baseada em uma característica interna do corpo, o sistema biométrico por meio do reconhecimento das veias do dedo fornece a autenticação segura da identidade do indivíduo. (VIGLIAZZI, 2006). O fato de não necessitar contato direto com o dispositivo de captura é um facilitador para poder ser utilizado em locais públicos, tornando-se assim mais abrangente.

Portanto, esta é a razão deste sistema biométrico ser considerado seguro, rápido e preciso, além de se mostrar superior a outras soluções biométricas como a leitura de impressões digitais ou da retina. (NUIDA et al., 2009).

2.2.11 Comparação Entre os Tipos de Biometria

Segundo o Fórum de Biometria(IBIOMETRICA, 2010), há alguns critérios que precisam ser obedecidos para que um aspecto comportamental ou físico seja considerado uma técnica biométrica válida para utilização em sistemas de reconhecimento:

- **Universalidade:** As características em análise devem ser possuídas por todos os seres humanos;
- **Distinção:** A característica em questão deve diferir de pessoa para pessoa;
- **Permanência:** As mudanças e aspectos característicos do indivíduo não devem sofrer mudanças durante a sua vida, ou se existirem devem ser praticamente nulas;
- **Coletibilidade:** O armazenamento e a leitura dessa característica deve ser realizado através de alguma categoria de processo ou equipamento.

A figura 2.12 abaixo mostra uma comparação entre os sistemas biométricos existentes de acordo com esses critérios, utilizando-se da classificação entre "Alta", "Média"ou "Baixa"para cada tipo de tecnologia biométrica em comparação.

Figura 2.12 – Comparação de Tecnologias Biométricas
Fonte: Adaptada de Tulyakov (2006)

Comparação das várias tecnologias biométricas, modificado de Jain et al., 2004							
(A = Alta, M = Média, B = Baixa)							
Biometria:	**Universalidade**	**Distinção**	**Permanência**	**Colectabilidade**	**Desempenho**	**Aceitabilidade**	**Segurança**
Face	A	B	M	A	B	A	M
Impressão Digital	M	A	A	M	A	M	A
Geometria das Mãos	M	M	M	A	M	M	M
Padrão de Digitação	M	B	B	A	B	A	B
Veias da Mão	M	M	M	M	M	M	A
Íris	A	A	A	A	A	B	A
Assinatura	B	B	B	A	B	A	B
Voz	M	B	B	M	B	A	B

Existem também alguns outros critérios que devem ser considerados em relação à eficiência do sistema adotado, como por exemplo:

- **Desempenho:** Os tempos para adquirir a característica e seu respectivo processamento devem ser razoáveis para o uso comercial (HEINEN; OSÓRIO, 2004).
- **Aceitabilidade:** O método de aquisição deve ser o menos invasivo possível, ou seja, ele deve ser aceito pelo usuário do sistema;
- **Segurança:** É necessário que o sistema seja forte o suficiente para impedir possíveis falhas;

Se tratando de sistemas biométricos, há dois termos fortemente utilizados, que são Autenticação e Identificação, que se distinguem em diversas formas e são abordados a seguir:

2.2.12 Autenticação Biométrica - Modo 1:1

Nesta categoria de sistema o usuário será identificado inicialmente pelo uso de um crachá que possui um código de barras por um cartão magnético, tendo o crachá uma tag do tipo RFID ou qualquer outro dispositivo que pertença ao usuário (dentro deste dispositivo há um dado comumente conhecido como PIN, e logo após essa identificação, é realizada a obtenção da característica biométrica do indivíduo para ser feita a constatação de que se trata da mesma pessoa. Neste sistema, a biometria não é direcionada para identificação, sendo o foco a validação de que o processo de identificação é seguro e funciona. É uma categoria de sistema extremamente rápido porque ocorre somente uma validação cruzada entre dois dados, sendo estes, um dado armazenado anteriormente e o dado momentâneo usado na autenticação, e não em um banco de dados completo, o que levaria mais tempo (BHATTACHARYYA et al., 2009).

2.2.13 Identificação Biométrica - Modo 1:N

Neste sistema biométrico é extraída a característica da pessoa sem uma identificação inicial, após isso é realizada uma busca em um banco de dados por uma similitude que seja mais próxima possível desta característica, na tentativa de validar a identificação. Por se tratar de um sistema onde os algoritmos trabalham com taxas de coincidência, o programador do sistema decide qual será a porcentagem de acerto para ser feita a aceitação daquele indivíduo, sendo definida uma probabilidade estatística de validação. Entretanto, deve haver um equilíbrio em relação à essa porcentagem, pois se o valor for muito alto, o sistema rejeita a identificação mesmo de pessoas já cadastradas, e se for muito baixo, o sistema valida identificações de pessoas que nem mesmo estão cadastradas (BHATTACHARYYA et al., 2009).

Na biometria este equilíbrio é comumente chamado de índice e os mesmos representam as falsas taxas de aceitação (FAR) e as falsas taxas de rejeição (FRR), e em todos os sistemas biométricos, o maior objetivo e idealização de um sistema conciso é atingir o threshold, ou seja, o ponto limiar entre estes dois índices. O ponto de threshold ideal é dito como a taxa de erro igual EER, onde a FAR é exatamente igual a FRR, e determina a qualidade do sistema biométrico em estudo. Quanto menor for a taxa de ERR, melhor é o sistema (SAINT; WEN; HAMID, 2011).

Há alguns critérios quanto à escolha de qual sistema biométrico utilizar em determinado local como, por exemplo, o nível de segurança, o tempo de resposta do sistema, aceitabilidade por parte dos usuários (se tratando de métodos invasivos ou não), o custo, a facilidade de instalação e manutenção e a confiabilidade (WEAVER, 2006).

2.2.14 FAR e FRR

Um dos primeiros elementos significativos no entendimento da precisão de sistemas biométricos é o desempenho como contra-ponto da segurança. Para chegar no equilíbrio, dois acrônimos são determinantes: FAR e FRR.

FAR, que em inglês significa False Acceptance Rate, está relacionado com o erro do sistema ao permitir o acesso de indivíduos que não estão autorizados. Já FRR, que em inglês significa False Rejection Rate, tem a ver com o erro do sistema de não autorizar o acesso de um indivíduo que possui autorização legítima para este acesso.

Quanto maior for a necessidade de segurança, menor deverá ser o FAR. Desse modo, quanto maior for a necessidade de desempenho, menor deverá ser o FRR. O acesso

a um sistema restrito, que normalmente é feito por poucas pessoas, pode ter um FRR mais alto para se ter um FAR muito baixo.

2.3 Técnicas de Reconhecimento de Padrões de Veias

2.3.1 Introdução

A biometria baseada no padrão vascular, como um traço biométrico novo e emergente, lida com os padrões formados pelos vasos sanguíneos localizados no corpo humano, ou seja, é um traço biométrico interno. Esses padrões vasculares não são visíveis a olho nu, portanto, um dispositivo de captura especificamente projetado, geralmente denominado scanner biométrico ou sensor biométrico, é necessário para amostrar esta biometria (ZHOU; KUMAR, 2011).

A hemoglobina contida no sangue que flui através dos vasos tem um coeficiente de absorção de luz mais alto no espectro do infravermelho próximo (NIR) do que o tecido circundante. Portanto, os padrões vasculares podem ser tornados visíveis como linhas escuras nas imagens capturadas com a ajuda de iluminação NIR e câmeras sensíveis a NIR, mas não usando câmeras digitais convencionais, pois geralmente possuem um filtro de bloqueio NIR integrado. As partes mais comuns do corpo consideradas incluem dedos (FADHIL; GEORGE, 2017), mãos (ENG; KHALIL-HANI, 2009) e também pulsos (PASCUAL et al., 2010).

Os dispositivos digitalizadores de veias de dedo já estão equipados em produtos comerciais, como caixas eletrônicos (ATMs) no Japão (KAUBA; PROMMEGGER; UHL, 2019), para autenticação de clientes de bancos na Polônia (LANE, 2012), para proteção de transações bancárias online em casa no Reino Unido (TASSABEHJI; KAMALA, 2012) e também como uma alternativa aos sistemas de autenticação baseados em impressão digital, em geral.

2.3.2 Scanners de veia de dedo

O reconhecimento da veia do dedo pertence à biometria baseada no padrão vascular. Como o nome sugere, essa biometria é baseada no padrão vascular, formado pela estrutura dos vasos sanguíneos no corpo humano. O reconhecimento da veia do dedo lida com o padrão vascular nos dedos humanos. Este padrão deve ser tornado visível e capturado por um dispositivo de scanner biométrico adequado, de modo a permitir o reconhecimento biométrico. A hemoglobina desoxinada no sangue que flui através dos vasos sanguíneos absorve a luz no espectro NIR, enquanto o tecido circundante tem um coeficiente de absorção de luz muito mais baixo dentro desse espectro. Deste modo, o padrão vascular pode ser tornado visível com a ajuda de uma fonte de luz NIR em combinação com um sensor de imagem sensível a NIR.

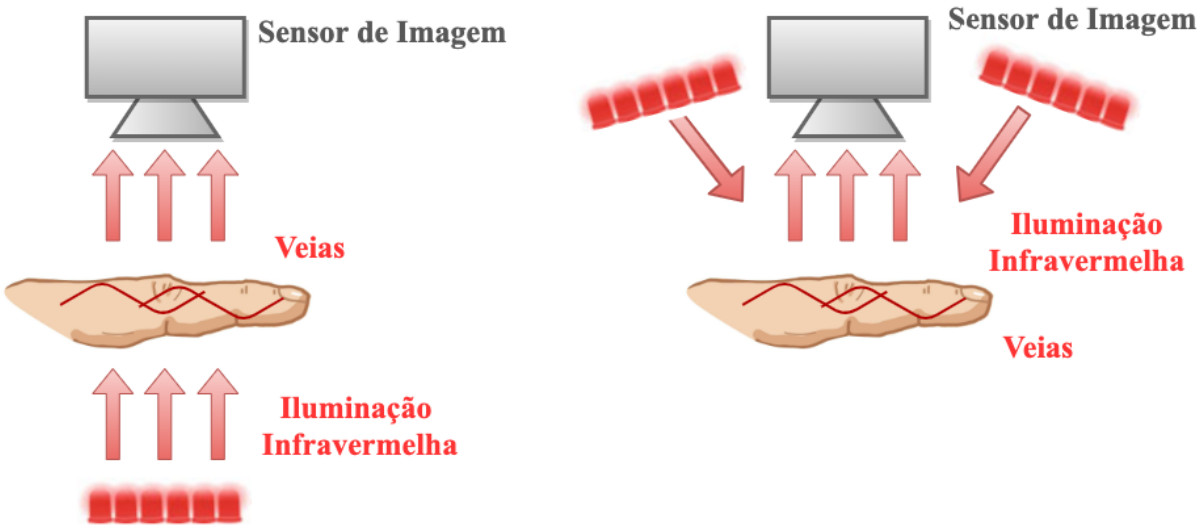
Consequentemente, as partes mais importantes de um scanner de veias de dedo são uma fonte de luz NIR e um sensor de imagem ou câmera sensível ao NIR. A fonte de luz NIR geralmente consiste em LEDs NIR (diodos emissores de luz) com um comprimento de onda de pico de emissão de luz entre 750 e 950 nm. Além da câmera NIR e da fonte de luz NIR, um filtro de passagem NIR ou uma caixa opticamente opaca para reduzir a influência da luz ambiente também é benéfico. Para auxiliar o posicionamento do dedo do indivíduo no momento da captura, a maioria dos scanners de veia de dedo possuem alguma categoria de suporte de posicionamento de dedo ou guia de dedo, a menos que sejam feitos para operação totalmente sem toque.

2.3.3 Posicionamento da fonte de luz

Existem duas categorias de iluminação distintos, com base no posicionamento relativo do dedo, do sensor de imagem e do iluminador: que pode ser luz refletida ou transmissão de luz, também chamada de transiluminação.

A figura 2.13 exemplifica os dois modos de luzes que um scanner de veias pode ter.

Figura 2.13 – Posicionamento da fonte de luz e do sensor de imagem
Produção Própria



Na figura 2.13, o lado esquerdo representa o modo de transmissão de luz e o direito o modo de luz refletida. A luz refletida permite dispositivos de scanner menores, enquanto a transmissão de luz torna mais detalhes do padrão vascular visíveis devido à maior profundidade de entrada no tecido do dedo.

2.3.3.1 Transmissão de luz

Nesse modo o sensor de imagem e o iluminador são colocados no lado oposto ao do dedo. A luz penetra na pele do lado do dedo próximo ao iluminador, percorre o tecido do dedo, onde é refletida, refratada, dispersa, espalhada e absorvida. Uma fração de luz emitida imerge no lado oposto do dedo e é capturada pelo sensor de imagem. Como a luz deve percorrer todo o dedo, intensidades de luz mais altas são necessárias em comparação com a luz refletida, levando a um maior consumo de energia. Devido ao posicionamento do iluminador e do sensor de imagem opostos um ao outro, os dispositivos do scanner são maiores em comparação com os de luz refletida.

2.3.3.2 Luz refletida

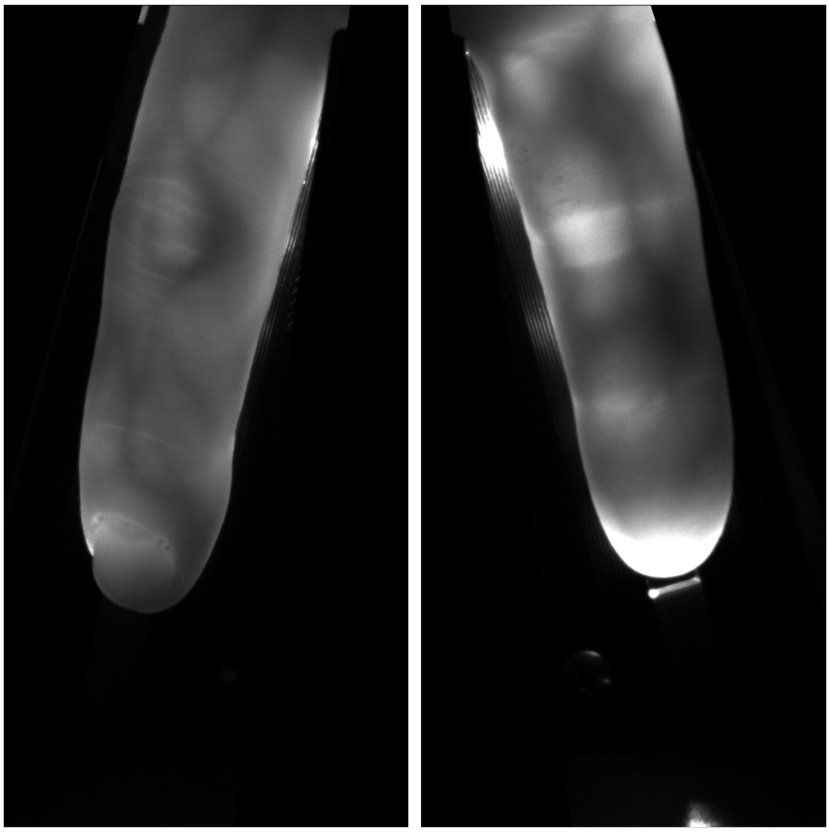
O sensor de imagem e o iluminador são colocados no mesmo lado do dedo, dorsal ou palmar. A luz se origina do iluminador, uma pequena parte é refletida diretamente na superfície do dedo, a parte restante penetra na pele e no tecido e é refletida, refratada e espalhada ali. A fração da luz que emerge do mesmo lado do dedo é captada pelo sensor de imagem. Scanners baseados em luz refletida precisam de menos intensidade de luz. Dessa forma, possuem baixo consumo de energia e podem ser construídos de forma menor, pois a fonte de luz e o sensor de imagem estão posicionados um ao lado do outro. No entanto, a

profundidade de penetração da luz é menor do que a transmissão de luz, portanto, menos detalhes dos padrões vasculares se tornam visíveis. No entanto, no reconhecimento, da veia do dedo, a transmissão de luz é usada quase exclusivamente.

2.3.4 Duas perspectivas principais do dedo - Dorsal e Palmar

As principais perspectivas ou vistas a partir das quais o dedo é capturado são dorsal e palmar (também chamadas ventrais). As imagens dorsais são tiradas do dorso ou lado dorsal da mão, enquanto as imagens palmares são tiradas da palma ou da parte inferior da mão. A figura 2.14 retirada do banco de dados PLUSVein-FV3 mostra ambas as perspectivas de captura. Contudo, existem diversas outras vistas ao redor do dedo que podem ser capturadas como as vistas laterais, mas o reconhecimento da veia do dedo lida principalmente com imagens palmares, com algumas exceções onde a vista dorsal é usada.

Figura 2.14 – Duas perspectivas principais do dedo



2.3.5 Scanners comercias de veias de dedo

Como no reconhecimento da veia do dedo, a transmissão de luz em combinação com imagens palmares é usada quase exclusivamente, então todos os scanners são baseados nesta configuração também (alguns scanners têm a fonte de luz e a câmera dispostas perpendicularmente entre si, que os fabricantes chamam de dispersão de luz). A figura 2.14 mostra alguns scanners de veia digitais amplamente usados. As duas principais empresas que fornecem soluções de autenticação de veias de dedo são Hitachi Ltd. e Morfiria Ltd. Suas tecnologias são patenteadas e não divulgadas.

Figura 2.15 – Scanners comerciais de veias de dedo

2.3.6 Algoritmos de extração de características baseados em curvatura

Uma imagem digital capturada usando luz infravermelha contém veias que possuem várias larguras e brilhos, que podem mudar com o tempo devido às flutuações na quantidade de sangue na veia, causado por mudanças na temperatura, condições físicas, etc.

Para identificar uma pessoa com alta precisão, o padrão das veias finas/ grossas e claras/ pouco claras em uma imagem deve ser extraída igualmente. Além disso, o padrão deve ser extraído com pouca ou nenhuma dependência da largura da veia e das flutuações de brilho.

Os métodos convencionais existentes podem extrair padrões se as larguras das veias forem constantes. No entanto, esses métodos não podem extrair veias que são mais estreitas ou largas do que as larguras assumidas, o que degrada a precisão da identificação pessoal. Deste modo, para suprir esses problemas existentes, alguns métodos de extração de características da veia do dedo buscam analisar a curvatura máxima, média ou principal dos perfis das imagens obtidas das veias do dedo, ou das mãos.

2.3.6.1 Curvatura Máxima (Maximum Curvature)

Em 2007, Miura e outros autores, propuseram no artigo intitulado ”Extração de padrões de veias dos dedos usando pontos de curvatura máxima em perfis de imagem”(MIURA; NAGASAKA; MIYATAKE, 2007), um método que verifica a curvatura dos perfis das imagens das veias enfatizando o dimensionamento apenas das linhas centrais, portanto, é insensível a diferentes larguras de veias.

Segundo o autor, a primeira etapa da técnica consiste na extração das posições centrais das veias através da determinação da curvatura máxima local em perfis transversais obtidos nas quatro direções: horizontal, vertical e as duas direções oblíquas. O perfil da seção transversal é determinado com base na primeira e na segunda derivada. Deste modo, cada perfil é classificado como côncavo ou convexo, onde apenas os máximos locais pertencentes a um perfil côncavo indicam uma linha de veia. Em seguida, uma pontuação conforme a largura e curvatura da região da veia é atribuída a cada posição central e registrada em uma matriz. Devido ao ruído ou outras distorções, alguns píxeis podem não ser classificados corretamente na primeira etapa. Assim, as posições centrais das veias são conectadas usando uma operação de filtragem em todas as quatro direções, tomando a vizinhança de 8 píxeis em consideração. A imagem de saída final é obtida por limiar do espaço da matriz usando a mediana como thresholding.

2.3.6.2 Curvatura Principal (Principal Curvature)

Em 2009, Choi e outros autores propuseram no artigo intitulado "Extração da veia do dedo usando normalização de gradiente e curvatura principal"(CHOI et al., 2009), um método de extração de características baseado em curvatura. Até então, os métodos mais populares de extração de veias de dedo existentes eram o de Miura (MIURA; NAGASAKA; MIYATAKE, 2007) e o de Song (SONG, 2008), os quais foram utilizados por Choi para comparação de desempenho quanto ao seu método.

Segundo o autor, o novo método de extração da veia do dedo é compreendido em três etapas, sendo elas: normalização do gradiente, cálculo da curvatura principal e binarização, nesta ordem. Desta forma, primeiramente o campo gradiente da imagem é calculado. Para evitar a amplificação indesejada de pequenos componentes de ruídos, é efetuado um limite rígido que filtra pequenos gradientes, definindo seus valores para zero. Desta forma, o gradiente em cada píxel é normalizado a uma magnitude de 1 para obter um campo de gradiente normalizado. Este campo de gradiente normalizado é suavizado pela aplicação de filtro Gaussiano. A próxima etapa é o cálculo da curva principal real. As curvaturas são obtidas a partir dos valores próprios da matriz Hessiana em cada píxel. Os dois autovetores da matriz representam as direções da curvatura máxima e mínima e os autovalores correspondentes são as curvaturas principais. Apenas o maior valor próprio que corresponde à curvatura máxima entre todas as direções é usado. A última etapa é uma binarização baseada em limiar dos valores da curvatura principal para chegar à imagem de saída da veia binária.

2.3.7 PLUS OpenVein Toolkit

Para ocorrerem pesquisas sobre qualquer característica biométrica, existem dois pré-requisitos importantes: a disponibilidade de conjuntos de dados para treinamento e testes, e a disponibilidade de uma cadeia de ferramentas (Toolkit) de reconhecimento biométrico completa e adaptada a característica biométrica específica para conseguir conduzir avaliações de desempenho de reconhecimento.

Atualmente pode-se encontrar um pacote de software abrangente e de código aberto que contém todas as ferramentas necessárias para a realização do processo de reconhecimento das veias chamado PLUS OpenVein, criado pelo grupo de pesquisadores que fazem parte do Departamento de Ciências da Computação da Universidade de Salzburg, liderado por Christof Kauba e Andreas Uhl no laboratório WaveLab (The Multimedia Signal Processing and Security Lab)(WAVELAB, acessado em Janeiro, 2021).

O pacote de software PLUS OpenVein é composto por diversos algoritmos de aprimoramentos de veias bem estabelecidos e modernos, bem como extração de recursos e esquemas de comparação. Ele dispõe de ferramentas que possuem foco na avaliação e desempenho de reconhecimento, assim como funções que realizam fusão de recursos e níveis de pontuação. A imagem 2.16 mostra uma cadeia genérica existente de reconhecimento biométrico, enquanto a imagem 2.17 mostra em comparação toda a parte da cadeia de ferramentas de reconhecimento que fazem parte do software PLUS OpenVein.

Figura 2.16 – Sistema de reconhecimento biométrico
Produção Própria

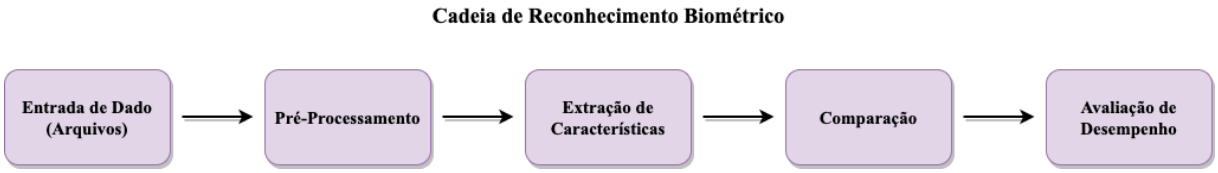
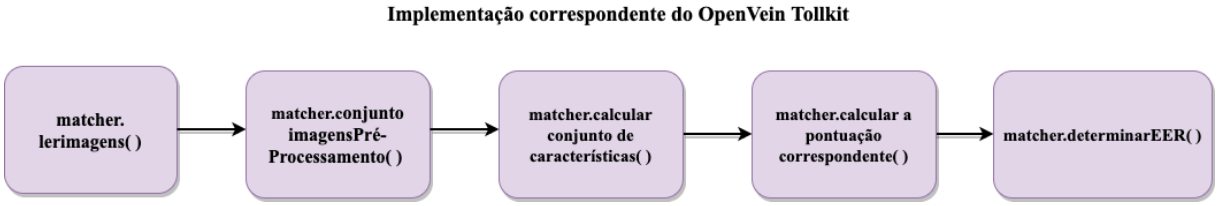


Figura 2.17 – Implementação das diferentes etapas de processamento pelo PLUS OpenVein Toolkit
Produção Própria



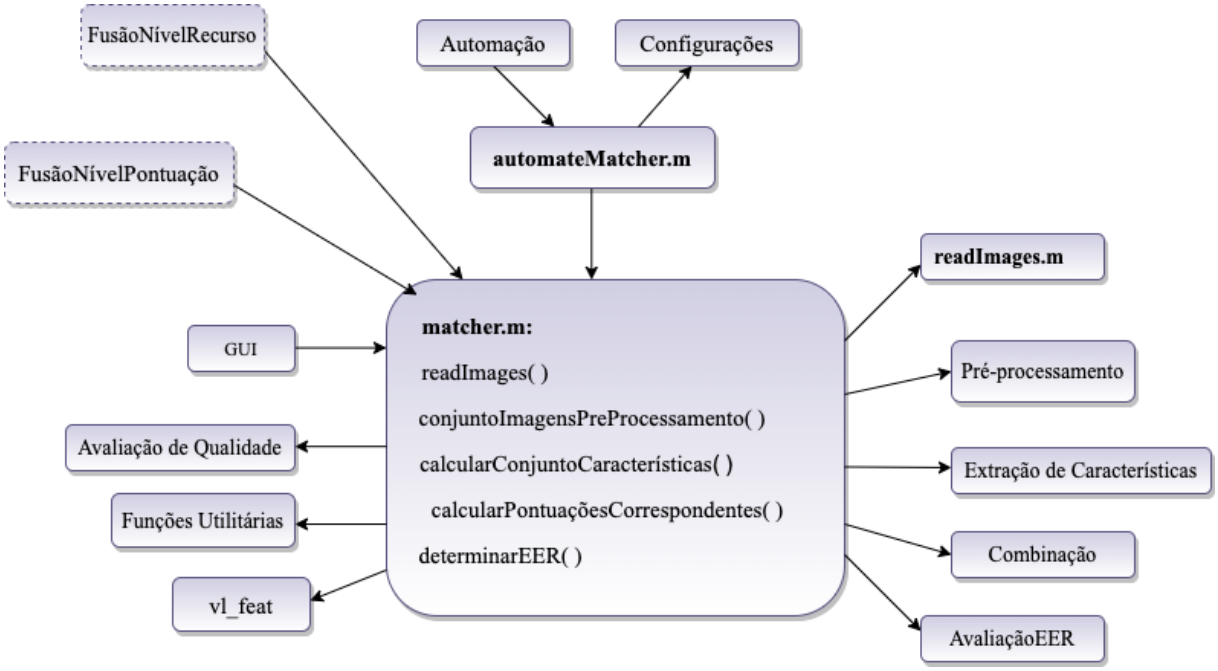
2.3.7.1 Estrutura de Diretório

A imagem 2.17 mostra uma visão geral esquemática da estrutura de reconhecimento de veia. O arquivo principal é o Matcher.m, que contém a maior parte da lógica do programa, incluindo o pré-processamento, extração de características e funções de execução de comparação. O ”matcher”é um objeto MATLAB que armazena as imagens de entrada, os recursos extraídos, as pontuações de comparação e os resultados. Algumas partes dos esquemas de reconhecimento são implementados diretamente no Matcher.m, mas a maioria dos esquemas são funções externas, implementadas em arquivos .m distintos. Esses arquivos .m estão organizados nos seguintes subdiretórios:

- Automação: diversos scripts para automação e teste automatizado de configuração.
- Avaliação EER: funções para determinar os números e gráficos de desempenho.
- Extração de características: a maioria das funções de recursos independentes.
- Fusão em nível de característica: ferramentas para realizar a fusão em nível de recurso e avaliar os resultados da fusão.
- GUI: relacionado à interface gráfica do usuário.

- Combinação: diferentes funções de comparação.
- Pré-processamento: diversas funções de pré-processamento para imagem de veias.
- Avaliação de qualidade: métricas gerais de contraste de imagem, bem como métricas de qualidade específicas da veia.
- Fusão de nível de pontuação.
- Configurações: contém os arquivos de configurações para vários conjuntos de dados.
- Funções de utilidade: diversas funções auxiliares, como por exemplo, para ler arquivos ini e plotagem.
- Vlfeat: diretório onde é colocada a fonte vlfeat.

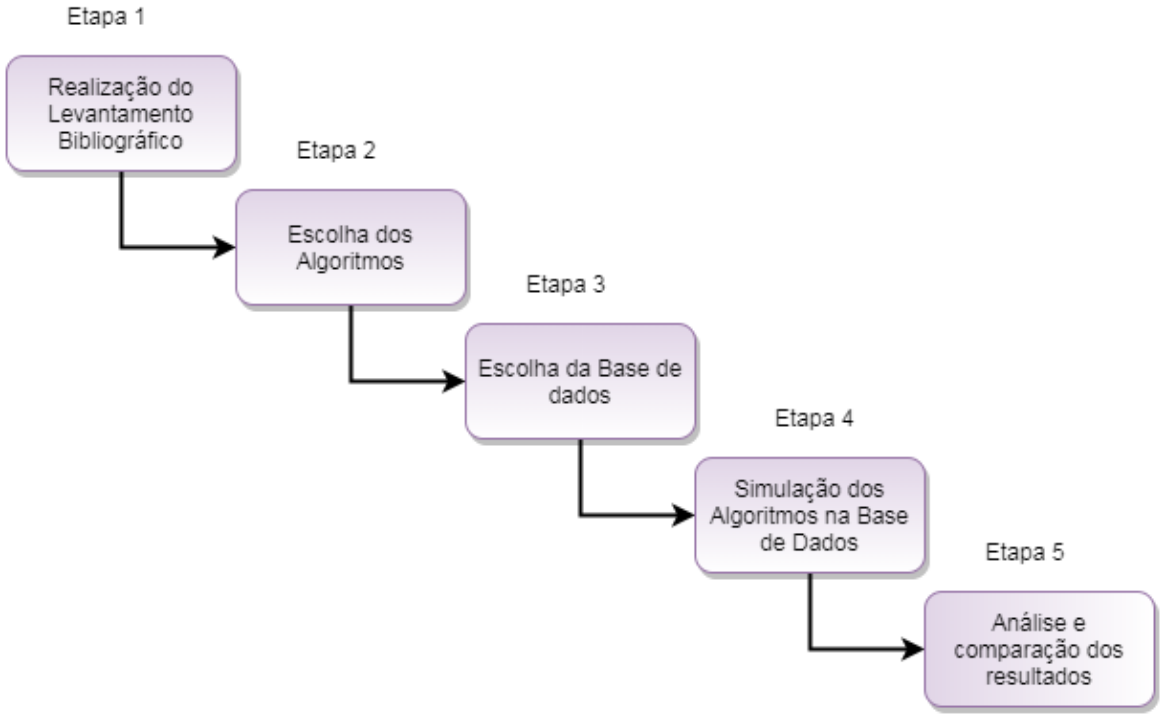
Figura 2.18 – Visão geral esquemática do PLUS OpenVein Toolkit, os arquivos do MATLAB e os diretórios



3 METODOLOGIA

Neste capítulo é descrita a metodologia utilizada, que está dividida em cinco etapas e exemplificada na figura 3.1.

Figura 3.1 – Etapas da Metodologia
Produção Própria



3.1 Realização do Levantamento Bibliográfico

Esta etapa visa a revisão da literatura acerca das biometrias existentes, bem como o surgimento de cada uma delas e como são aplicados atualmente, com foco principal na biometria de reconhecimento de padrões de veias do dedo e suas técnicas de captura. Também é conduzida uma breve introdução sobre o toolkit PLUSOpen Vein, sua estrutura de diretórios e funcionamento.

3.2 Escolha dos Algoritmos

Como citado na seção anterior, para haver o reconhecimento do padrão de veias do dedo é necessário passar por algumas fases de processamento de imagem, onde cada fase possui uma sequência de algoritmos e métodos diferentes que o pacote de software PLUSOpen Vein dispõe.

Os esquemas de pré-processamento existentes no toolkit PLUSOpen Vein podem ser combinados em diferentes ordens e mais de uma vez. A lista de métodos e parâmetros fornecidos no arquivo de configurações para realização dos testes possui diversos algoritmos. Para realização de testes e comparações os algoritmos escolhidos foram: curvatura máxima e curvatura principal, os quais foram explanados na subseção 2.5.6 do capítulo anterior.

3.3 Escolha da Base de Dados

3.3.1 Descrição do Banco de Dados

O banco de dados utilizado é o PLUSVein-FV3 pulicado pelo laboratório WaveLab (Laboratório de Processamento e Segurança de Sinais Multimídia) disponível em (WAVELAB, acessado em Janeiro, 2021), adquirido com dois leitores de veias do dedo de design personalizado, um NIR LED e uma versão baseada em módulo de laser NIR.

Atualmente o banco de dados contém imagens das veias dorsais e palmares dos dedos das mãos de 60 indivíduos. São no total 3600 imagens de 360 dedos individuais, sendo 6 dedos por indivíduo e 5 imagens por dedo a cada sessão de captura de imagem.

3.4 Simulação dos Algoritmos na Base de Dados

O objetivo desta etapa é simular os dois algoritmos escolhidos e aplica-los à base de dados escolhida na fase anterior, para a obtenção de resultados.

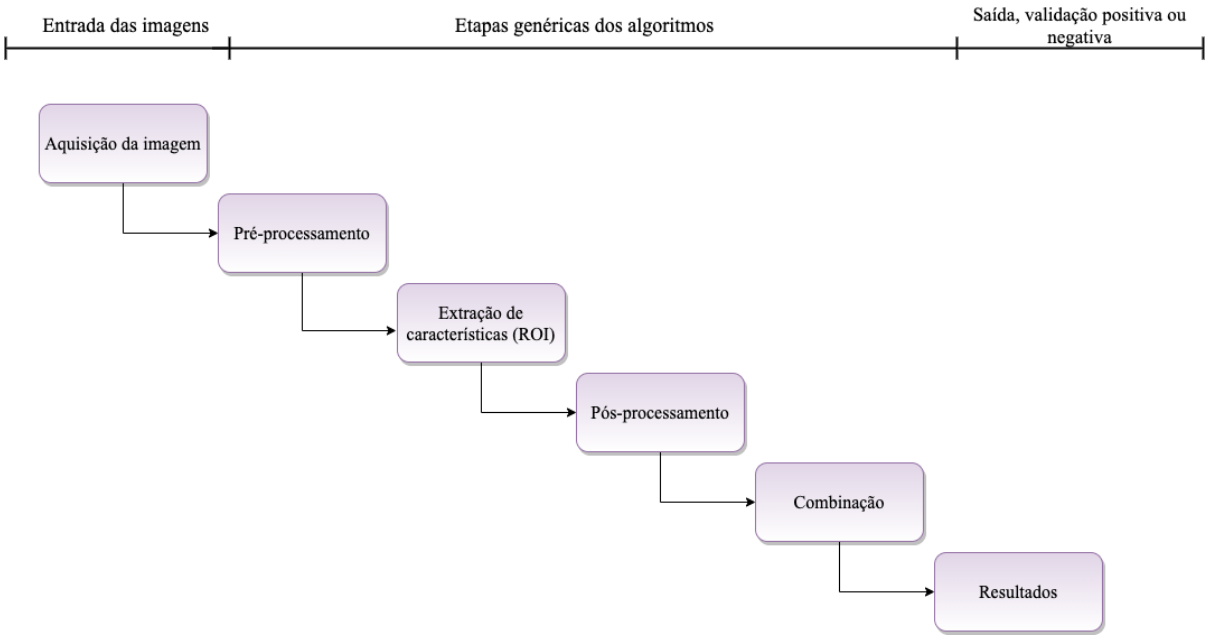
A fase de aquisição da imagem é suprida pela etapa 3 (onde a base de dados foi escolhida). Por conseguinte, a base de dados será aplicada ao software toolkit PLUSOpen

Vein, onde os dois algoritmos, já especificados anteriormente, serão simulados separadamente.

Os mesmos passarão por suas fases de aquisição da imagem, pré-processamento, extração de características (ROI), pós-processamento, combinação e resultados. Cada qual a sua maneira devolverá os resultados das validações e das taxas de comparação entre si.

A figura 3.2 exemplifica as etapas citadas anteriormente pelas quais os algoritmos passarão.

Figura 3.2 – Etapa de simulação dos algoritmos na base de dados
Produção Própria



3.5 Análise e Comparação dos Resultados

O objetivo desta etapa é por fim, analisar e comparar os resultados dos dois algoritmos selecionados. Para que isso ocorra, serão analisadas todas as taxas de combinação e templates de comparação.

3.5.1 Ferramentas de Avaliação de Desempenho

Para haver uma avaliação do desempenho e reconhecimento de um esquema de comparação em um conjunto de dados específico, vários números e gráficos de desempenho

são gerados automaticamente pela estrutura de reconhecimento de veia. Esses números e gráficos são baseados nas pontuações de comparação genuínas e impostores que foram calculadas.

3.5.1.1 EER / FMR100 / FMR1000 / ZeroFMR

Os números obtidos com os testes são utilizados para quantificar o desempenho de esquemas de reconhecimento biométrico. Teoricamente, o ponto ideal estará próximo do EER, que em inglês quer dizer Equal Error Rate, ou Proporção de Erro Equilibrada. Se um sistema biométrico tem EER de 0,1%, isso significa que a sua eficácia será de 99,9%. Em resumo, é a partir do EER que serão dosadas as necessidades de segurança e desempenho de uma solução.(VIGLIAZZI, 2006).

O FMR, do inglês False Match Rate, ou Taxa de Correspondência Falsa, é a porcentagem da probabilidade de vezes em que o sistema declara incorretamente que a amostra biométrica pertence à identidade reivindicadora quando a amostra realmente pertence a um sujeito diferente (impostor).

O FNMR, do inglês False Non-Match Rate, ou Taxa de Falsa Não Correspondência, é a porcentagem da probabilidade de o sistema rejeitar incorretamente uma identidade reivindicada quando a amostra realmente pertence ao sujeito (usuário genuíno).

Sendo assim, o EER é o ponto onde o FMR e o FNMR são iguais. O FMR100 é o menor FNMR para FMR = 1%; O FMR1000 é o menor FNMR para FMR = 0,1% e o ZeroFMR é o menor FNMR para FMR = 0%. Além desses, o FNMR1000 é o menor FMR para FNMR = 0,1 e o ZeroFNMR é o menor FMR para FNMR = 0%, que também estão inclusos.

3.5.2 Configurações de Testes

Para a realização dos testes, são usadas 300 imagens das veias dorsais de dedo único, adquiridas com a categoria de leitor de veia do dedo versão, módulo de laser NIR da base de dados PLUSVein-FV3 citada anteriormente. As imagens possuem uma resolução de 420x1024 píxeis e estão armazenadas no formato png da escala de cinza de 8 bits.

As etapas empregadas consistem nos seguintes componentes:

- Pré-processamento: Primeiramente ocorre a segmentação da imagem de entrada do dedo e a região do fundo da imagem é mascarada usando o método LeeRegion com uma largura de filtro de 40 píxeis e altura de 4 píxeis. Após isso ocorre a normalização da imagem do dedo através da abordagem HuangNormalise. Depois, é aplicado o método CLAHE com limite de clipe de 0,01 e para o realce da imagem é usado o proposto por Zhang, com largura de banda do filtro Gabor de 1,12 e Sigma Gabor de 3. Por fim, a imagem é redimensionada para a metade do seu tamanho original.

- Extração de Característica: Para essa etapa foram aplicados dois algoritmos com métodos de extração de características diferentes. O primeiro é o método de Curvatura Máxima de Miura (Maximum Curvature) com Sigma de 2,5. O segundo é o método de Curvatura Principal de Choi (Principal Curvature) com Sigma de 2,5 e threshold de 1,5.

- Pós-processamento: É realizado um pós processamento morfológico adicional através da utilização dos métodos AreaOpen e InverseAreaOpen com 30 iterações cada.

- Comparação: Para as comparações das características da veia extraída é utilizado o esquema de comparação Miura Matcher, com um deslocamento horizontal de 80 píxeis, um deslocamento vertical de 30 píxeis e um deslocamento rotacional de 2 em combinação com o protocolo de avaliação FVC.

- Avaliação de Desempenho: O desempenho do reconhecimento é avaliado utilizando o EER, o FMR100, o FMR1000 e o ZeroFMR, assim como os gráficos DET e ROC correspondentes, mostrados no capítulo a seguir.

4 RESULTADOS

Os resultados seguintes dizem respeito às classificações dos dados realizados pelos algoritmos propostos no capítulo anterior. A primeira imagem da sequência apresentada na figura 4.1 mostra um exemplo do banco de dados PLUSVein-FV3 como dado de entrada, após o mascaramento da região da veia ter sido aplicado. Em seguida, a segunda imagem apresentada na figura 4.2 representa a mesma imagem após a aplicação do pré-processamento. A terceira imagem apresentada na figura 4.3 e a quarta imagem apresentada na figura 4.4 mostram a extração de características pelos algoritmos, Curvatura Máxima e Curvatura Principal, nesta sequência.

Figura 4.1 – Imagem de entrada | Máscara ROI aplicada
Produção Própria

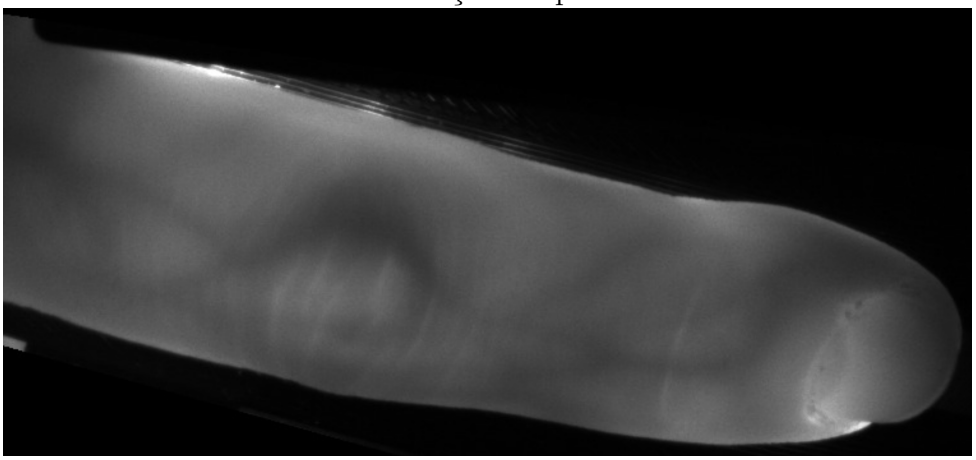


Figura 4.2 – Imagem Pré-processada
Produção Própria

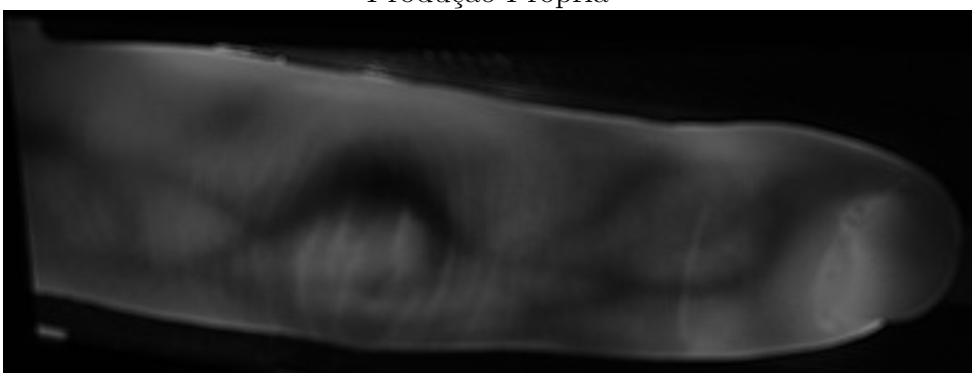


Figura 4.3 – Extração de características pelo algoritmo Curvatura Máxima
Produção Própria

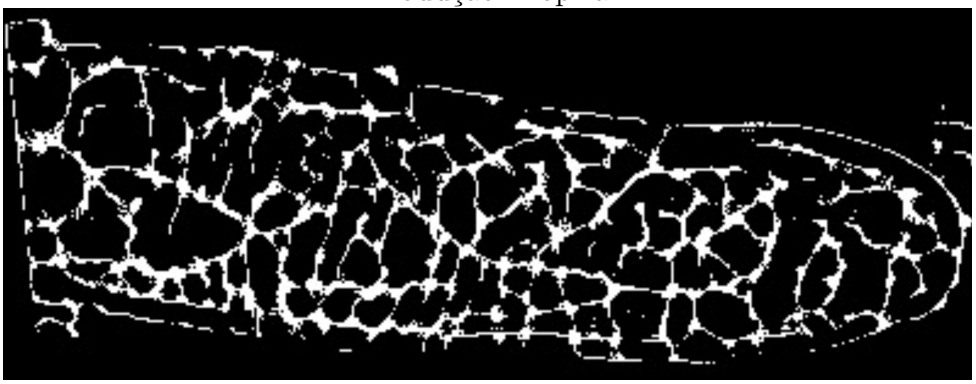


Figura 4.4 – Extração de características pelo algoritmo Curvatura Principal
Produção Própria

4.1 Análise dos Resultados

Após observar os resultados visuais da etapa de extração de características dos dois algoritmos, é possível concluir que para o objeto de interesse, dedo único, o algoritmo Curvatura Máxima apresentou um resultado superior ao algoritmo Curvatura Principal, pois a região de interesse demonstra melhor definição nas demarcações fazendo com que as linhas das veias possam ser reconhecidos mais facilmente, o que causa uma diminuição alta em relação à falsos positivos. Isso se deve ao fato de que o algoritmo Curvatura Máxima, como citado anteriormente no capítulo 2.4, tem como foco destacar apenas as linhas das veias, não sendo sensível a diferentes larguras de veias.

A tabela 4.1 lista os resultados da avaliação dos algoritmos em questões de desempenho para as extrações de características do algoritmo Curvatura Máxima e o algoritmo Curvatura Principal. Conforme os resultados, o algoritmo Curvatura Máxima apresentou um melhor desempenho geral, possuindo um EER de 0,35%, enquanto o algoritmo

Curvatura Principal apresentou um EER de 0,70%.

Tabela 4.1 – Resultados para a avaliação de desempenho entre os algoritmos Curvatura Máxima e Curvatura Principal no conjunto de dados UTFVP

Produção Própria

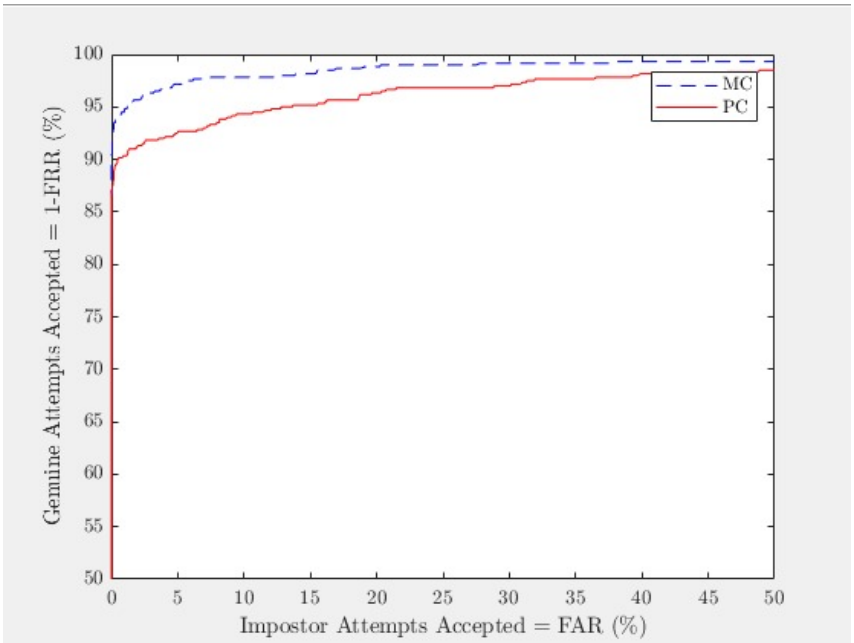
Algoritmo	EER (%)	FMR100 (%)	FMR1000(%)	ZeroFMR (%)
Curvatura Máxima	0,35	0,51	0,75	0,95
Curvatura Principal	0,70	0,96	1,25	1,33

Em relação aos valores de FMR, o algoritmo Curvatura Máxima também apresentou um melhor desempenho. O ZeroFMR é uma métrica de desempenho usada em algoritmos de altíssimo risco onde não são aceites nenhum impostor e mesmo assim, ambos apresentam um bom resultado.

Outro ponto importante a ser ressaltado são as porcentagens de EER. A maioria dos algoritmos possui EER menores que 1%, desse modo, os resultados apresentados demonstram que o reconhecimento de veias pode ser uma boa alternativa também.

Além dos números de desempenho, pode-se observar também a seguir a plotagem dos gráficos ROC na figura 4.5 e DET na figura 4.6.

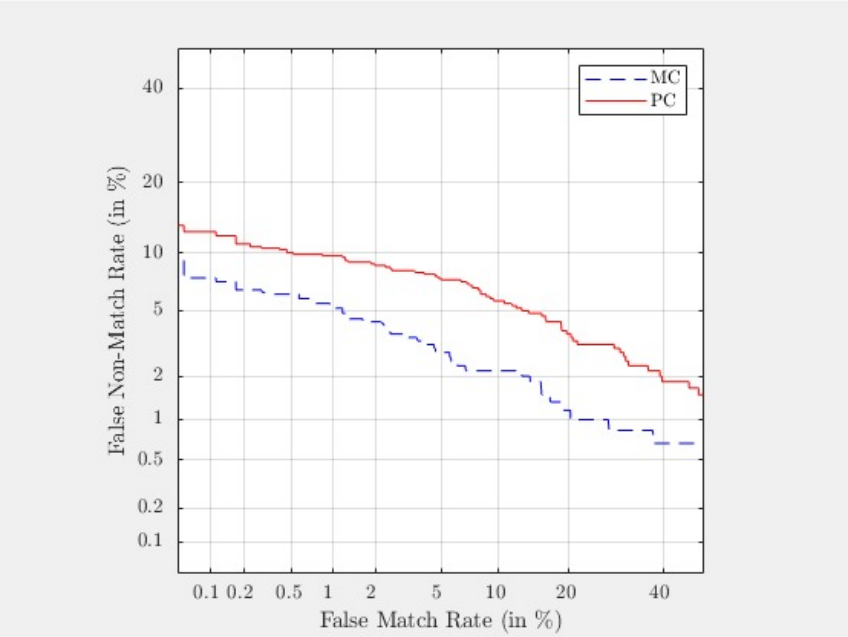
Figura 4.5 – Gráfico ROC



O ROC é o gráfico que mostra a taxa de falsos positivos (tentativas de impostor aceitas) no eixo x contra a taxa correspondente de verdadeiros positivos (tentativas

genuínas aceitas) no eixo y. Deste modo, é possível observar então que a linha do gráfico referente ao algoritmo Curvatura Máxima (MC) está próxima de 95% em relação à taxa FRR de tentativas genuínas aceitas, enquanto o algoritmo Curvatura Principal (PC) alcança somente 90%.

Figura 4.6 – Gráfico DET



Já o gráfico DET é uma curva ROC modificada que traça as taxas de erro em ambos os eixos (falsos positivos no eixo x e falsos negativos no eixo y). Sendo assim, é possível observar através do gráfico que a taxa de não correspondência falsa FNMR é menor para o algoritmo Curvatura Máxima (MC) em relação à taxa FNMR do algoritmo Curvatura Principal (PC). Mesmo assim, é possível constatar que a extração de característica da veia pelo método Curvatura Principal apresenta uma boa extração, com o interior homogêneo de suas regiões. Entretanto, os caminhos de veias são bruscos e de espessura larga, o que foge dos requisitos de uma extração perfeita.

Contudo, um ponto a ser considerado são as imagens de entrada. Em seu artigo, Choi ressalta o ponto de que sensor de veia do dedo utilizado para obter o seu banco de dados de imagens é da categoria totalmente sem contato, enquanto Miura (MIURA; NAGASAKA; MIYATAKE, 2007) aborda em seu artigo o fato de ter realizado os testes do seu método utilizando imagens extraídas de um scanner físico, o caso do banco de

dados utilizado para a realização dos testes. Como já visto anteriormente, essas são condições que mudam fortemente os resultados, porém ambos algoritmos são cabíveis de configurações mais adequadas para a aplicação onde será implementado.

Ambos os algoritmos se provam ser extremamente capazes de serem implementados na criação de um software de identificação biométrica através da veia do dedo, pois certamente conseguirão identificar o usuário e realizar o maior foco, a segurança digital.

5 CONCLUSÃO

O presente estudo através de sua metodologia possui o objetivo de enfatizar a importância da segurança biométrica atualmente, destacando a ascensão eminente de um novo método de identificação de pessoas baseado no padrão de veia do dedo e principalmente a comparação de desempenho entre dois algoritmos de extração de características de padrão de veia.

Os resultados obtidos através da utilização dos métodos propostos por Choi (CHOI et al., 2009) e Miura (MIURA; NAGASAKA; MIYATAKE, 2007) para realizar a etapa de extração de característica da veia foram satisfatórios com a base de dados utilizada PLUSVein-FV3. Não só se mostraram confiáveis e robustos, como apresentaram um bom desempenho computacional, mesmo que haja um destaque para o método Curvatura Máxima sobre o Curvatura Principal nas comparações de desempenho utilizadas.

Todos os resultados apresentados foram baseados nas métricas utilizadas por outros autores e já propostas pelo software PLUS OpenVein, como a taxa de falsos positivos FAR e a taxa de falsos negativos FRR para poderem ser realizadas comparações minuciosas entre os dois algoritmos selecionados.

Portanto, com o trabalho concluiu-se que para aplicações com fins de reconhecimento biométrico através de padrão de veia, os métodos testados são precisos e confiáveis observando a base de dados que foi utilizada, para serem inseridos em situações que demandem baixas taxas de erro e alta confiabilidade.

Como recomendação para trabalhos futuros, fica a proposta de combinar diferentes métodos no desenvolvimento de sistemas de autenticação biométrica, pois, desta maneira é possível usufruir ainda mais das vastas funcionalidades que nos proporcionam estas técnicas na hora de identificar ou reconhecer unicamente uma pessoa.

REFERÊNCIAS

ACHARYA, T.; RAY, A. Image formation and representation. **Image Processing-Principles and Applicatons**, p. 17–36, 2005.

ACHARYA, T.; RAY, A. K.; GALLAGHER, A. C. *Image Processing: Principles and Applications*. **J. Electronic Imaging**, v. 15, n. 3, p. 039901, 2006. Disponível em: <https://doi.org/10.1117/1.2348895>.

ACHERMANN, B.; BUNKE, H. Combination of face classifiers for person identification. In: **13th International Conference on Pattern Recognition, ICPR 1996, Vienna, Austria, 25-19 August, 1996**. [s.n.], 1996. p. 416–420. Disponível em: <https://doi.org/10.1109/ICPR.1996.546981>.

ALEY-RAZ, A. et al. **Device, system, and method of liveness detection utilizing voice biometrics**. [S.l.]: Google Patents, 2013. US Patent 8,442,824.

ALSHU'EILI, H.; GUPTA, G. S.; MUKHOPADHYAY, S. Voice recognition based wireless home automation system. In: IEEE. **2011 4th International Conference on Mechatronics (ICOM)**. [S.l.], 2011. p. 1–6.

ATHENA. **"Recognition Process Voice"**. 2017. <"https://athena.ecs.csus.edu/~changw/Sounds/SpeechRecog/recognition.html">. Último acesso em: 09/08/2019.

AZEVEDO, E.; CONCI, A. **Computação gráfica: teoria e prática**. [S.l.]: Elsevier, 2003.

Balti, A.; Sayadi, M.; Fnaiech, F. Improved features for fingerprint identification. In: **2012 16th IEEE Mediterranean Electrotechnical Conference**. [S.l.: s.n.], 2012. p. 878–883. ISSN 2158-8481.

BARBOSA, P. B. Avanços na tecnologia desenvolvida pela justiça eleitoral no brasil e seus efeitos na contemporaneidade. **Estudos Eleitorais: vol. 9, n. 3 (set./dez. 2014)**, Tribunal Superior Eleitoral, 2014.

BAXES, G. A. **Digital image processing: principles and applications**. [S.l.]: Wiley New York, 1994.

BAYOMETRIC. **Minutiae Based Extraction in Fingerprint Recognition**. 2013. <"https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/">. Último acesso em: 07/08/2019.

BHABATOSH, C. et al. **Digital image processing and analysis**. [S.l.]: PHI Learning Pvt. Ltd., 2011.

BHATTACHARYYA, D. et al. Biometric authentication: A review. **International Journal of u-and e-Service, Science and Technology**, v. 2, n. 3, p. 13–28, 2009.

BIOMETRICS. **Biometrics in Facial Recognition**. 2015. <"https://www.doc.ic.ac.uk/~jam414/AffectiveComputing/anmol.html">. Último acesso em: 08/08/2019.

BOLLE, R. M. et al. **Guide to biometrics**. [S.l.]: Springer Science & Business Media, 2013.

BOLLE, R. M.; CONNELL, J. H.; RATHA, N. K. Biometric perils and patches. **Pattern Recognition**, Elsevier, v. 35, n. 12, p. 2727–2738, 2002.

BRÖMME, A. A classification of biometric signatures. In: **Proceedings of the 2003 IEEE International Conference on Multimedia and Expo, ICME 2003, 6-9 July 2003, Baltimore, MD, USA**. [s.n.], 2003. p. 17–20. Disponível em: <https://doi.org/10.1109/ICME.2003.1221237>.

BYD. **"Qual a diferença entre bitmap e vetores?"**. 2016. <"https://byd.pt/qual-a-diferenca-entre-bitmap-e-vetores/">. Último acesso em: 11/10/2019.

CHIRCHI, V. R. E.; WAGHMARE, L.; CHIRCHI, E. Iris biometric recognition for person identification in security systems. **International Journal of Computer Applications**, International Journal of Computer Applications, 244 5 th Avenue,# 1526, New . . . , v. 24, n. 9, p. 1–6, 2011.

CHOI, J. H. et al. Finger vein extraction using gradient normalization and principal curvature. In: INTERNATIONAL SOCIETY FOR OPTICS AND PHOTONICS. **Image Processing: Machine Vision Applications II**. [S.l.], 2009. v. 7251, p. 725111.

COSTA, L. R.; OBELHEIRO, R. R.; FRAGA, J. S. Introdução á biometria. **Livro texto dos Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg2006). SBC: Porto Alegre**, v. 1, p. 103–151, 2006.

COSTA, R. M. d. **Uma nova abordagem para reconhecimento biométrico baseado em características dinâmicas da íris humana**. Tese (Doutorado) — Universidade de São Paulo, 2009.

CUI, B.; XUE, T. Design and realization of an intelligent access control system based on voice recognition. In: IEEE. **2009 ISECS International Colloquium on Computing, Communication, Control, and Management**. [S.l.], 2009. v. 1, p. 229–232.

DAUGMAN, J. Statistical richness of visual phase information: Update on recognizing persons by iris patterns. **International Journal of Computer Vision**, v. 45, n. 1, p. 25–38, 2001. Disponível em: <https://doi.org/10.1023/A:1012365806338>.

DAUGMAN, J. How iris recognition works. In: **Proceedings of the 2002 International Conference on Image Processing, ICIP 2002, Rochester, New York, USA, September 22-25, 2002**. [s.n.], 2002. p. 33–36. Disponível em: <https://doi.org/10.1109/ICIP.2002.1037952>.

DAUGMAN, J. New methods in iris recognition. **IEEE Trans. Systems, Man, and Cybernetics, Part B**, v. 37, n. 5, p. 1167–1175, 2007. Disponível em: <https://doi.org/10.1109/TSMCB.2007.903540>.

DELAC, K.; GRGIC, M. A survey of biometric recognition methods. In: IEEE. **Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine**. [S.l.], 2004. p. 184–193.

EKSTROM, M. P. **Digital image processing techniques**. [S.l.]: Academic Press, 2012. v. 2.

ENG, P.; KHALIL-HANI, M. Fpga-based embedded hand vein biometric authentication system. In: IEEE. **TENCON 2009-2009 IEEE Region 10 Conference**. [S.l.], 2009. p. 1–5.

FABREGAS, J.; FAÚNDEZ-ZANUY, M. On-line signature verification system with failure to enrol management. **Pattern Recognition**, v. 42, n. 9, p. 2117–2126, 2009. Disponível em: <https://doi.org/10.1016/j.patcog.2009.01.019>.

FADHIL, R. I.; GEORGE, L. E. **Finger vein identification and authentication system**. [S.l.]: LAP Lambert Academic Publishing, 2017.

GAZZANIGA, M.; HEATHERTON, T. Ciência psicológica: Mente, cérebro e comportamento (mav veronese, trans.). **Porto Alegre: Artmed.(Trabalho original publicado em 2005)**, 2007.

GONZALEZ, R.; WOODS, R. Image enhancement in the spatial domain. **Digital image processing**, Prentice Hall, v. 2, p. 75–147, 2002.

GONZÁLEZ-RODRÍGUEZ, J.; TOLEDANO, D. T.; ORTEGA-GARCÍA, J. Voice biometrics. In: **Handbook of biometrics**. [S.l.]: Springer, 2008. p. 151–170.

HANNA, K. J.; HOYOS, H. T. **Methods for performing biometric recognition of a human eye and corroboration of same**. [S.l.]: Google Patents, 2014. US Patent 8,818,053.

HEINEN, M. R.; OSÓRIO, F. S. Biometria comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas. **INFOCOMP**, v. 3, n. 2, p. 32–37, 2004.

HENTATI, R.; HENTATI, M.; ABID, M. Development a new algorithm for iris biometric recognition. **International Journal of Computer and Communication Engineering**, IACSIT Press, v. 1, n. 3, p. 283, 2012.

HONG, L.; WAN, Y.; JAIN, A. Fingerprint image enhancement: algorithm and performance evaluation. **IEEE transactions on pattern analysis and machine intelligence**, IEEE, v. 20, n. 8, p. 777–789, 1998.

IBIOMETRICA. **IBiometrica**. 2010. <"https://duodigit.com.br/ibiometrica/">. Último acesso em: 01/08/2019.

INFOSEC. **"Biometrics in the Cloud"**. 2018. <"https://resources.infosecinstitute.com/biometrics-in-the-cloud/#gref'>. Último acesso em: 08/08/2019.

JAIN, A. K.; FLYNN, P.; ROSS, A. A. **Handbook of biometrics**. [S.l.]: Springer Science & Business Media, 2007.

JAIN, A. K. et al. An introduction to biometric recognition. **IEEE Transactions on circuits and systems for video technology**, v. 14, n. 1, 2004.

JAIN, L. C. et al. **Intelligent biometric techniques in fingerprint and face recognition**. [S.l.]: CRC press, 1999. v. 10.

JAISWAL, P. **Detecting and communicating biometrics of recorded voice during transcription process**. [S.l.]: Google Patents, 2013. US Patent 8,457,964.

JANES, R. **Estudo sobre sistemas de segurança em instalações elétricas automatizadas.** Tese (Doutorado) — Universidade de São Paulo, 2009.

JANES, R.; JÚNIOR, A. F. B. A low cost system for dorsal hand vein patterns recognition using curvelets. In: . [S.l.: s.n.], 2014.

KAUBA, C.; PROMMEGGER, B.; UHL, A. Combined fully contactless finger and hand vein capturing device with a corresponding dataset. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 19, n. 22, p. 5014, 2019.

KONO, M. A new method for the identification of individuals by using of vein pattern matching of a finger. In: **Proc. Fifth Symposium on Pattern Measurement, Yamaguchi, Japan, 2000**. [S.l.: s.n.], 2000. p. 9–12.

LANE, L. Intel throws its weight behind palm vein id. **Biometric Technology Today**, Elsevier, 2012.

LI, Y.; SAVVIDES, M. An automatic iris occlusion estimation method based on high-dimensional density estimation. **IEEE Trans. Pattern Anal. Mach. Intell.**, v. 35, n. 4, p. 784–796, 2013. Disponível em: <https://doi.org/10.1109/TPAMI.2012.169>.

LYNCH, J. What facial recognition technology means for privacy and civil liberties; written testimony of jennifer lynch, staff attorney with the electronic frontier foundation (eff) before the senate committee on the judiciary subcommittee on privacy, technology, and the law; jul. 18, 2012; 24 pages. 2012.

MAIORANA, E. et al. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. **IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans**, IEEE, v. 40, n. 3, p. 525–538, 2010.

MANSSOUR, I. H.; COHEN, M. Introdução à computação gráfica. **RITA**, v. 13, n. 2, p. 43–68, 2006.

MARAN, A. V. Ppas: uma proposta para reconhecimento biométrico da palma da mão, utilizando local binary pattern. 2009.

MATHEW, B. **Iris**. [S.l.]: JSTOR, 1989.

MIURA, N.; NAGASAKA, A.; MIYATAKE, T. Extraction of finger-vein patterns using maximum curvature points in image profiles. **IEICE TRANSACTIONS on Information and Systems**, The Institute of Electronics, Information and Communication Engineers, v. 90, n. 8, p. 1185–1194, 2007.

MONROSE, F.; REITER, M. K.; WETZEL, S. Password hardening based on keystroke dynamics. **International Journal of Information Security**, Springer, v. 1, n. 2, p. 69–83, 2002.

NEWSROOM, S. **"[In-Depth Look] Keeping an Eye on Security: The Iris Scanner of the Galaxy Note7"**. 2016. <"https://news.samsung.com/global/in-depth-look-keeping-an-eye-on-security-the-iris-scanner-of-the-galaxy-note7">. Último acesso em: 09/08/2019.

NUIDA, K. et al. An improvement of discrete tardos fingerprinting codes. **Designs, Codes and Cryptography**, Springer, v. 52, n. 3, p. 339–362, 2009.

ORD, T.; FURNELL, S. M. User authentication for keypad-based devices using keystroke analysis. In: **Proceedings of the second international network conference (INC-2000)**. [S.l.: s.n.], 2000. p. 263–272.

OSTAP. **"What is the difference: email signature, electronic signature and digital signature?"**. 2017. <"https://newoldstamp.com/blog/what-is-the-difference-email-signature-electronic-signature-and-digital-signature/">. Último acesso em: 09/08/2019.

PASCUAL, J. E. S. et al. Capturing hand or wrist vein images for biometric authentication using low-cost devices. In: IEEE. **2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing**. [S.l.], 2010. p. 318–322.

PAYNE, J. H. **Biometric face recognition for applicant screening**. [S.l.]: Google Patents, 2000. US Patent 6,072,894.

PINHEIRO, J. M. d. S. **Biometria nos sistemas computacionais: você é a senha**. [S.l.]: Ciência Moderna, 2008.

PLAMONDON, R.; PARIZEAU, M. Signature verification from position, velocity and acceleration signals: a comparative study. In: **9th International Conference on Pattern Recognition, ICPR 1988, 14-17 November 1988, Ergife Palace Hotel, Rome, Italy**. [s.n.], 1988. p. 260–265. Disponível em: <https://doi.org/10.1109/ICPR.1988.28218>.

RASHID, R. A. et al. Security system using biometric technology: Design and implementation of voice recognition system (vrs). In: IEEE. **2008 International Conference on Computer and Communication Engineering**. [S.l.], 2008. p. 898–902.

RENSEN, M. Rensen, marius: "the bartlane system". hffax.de. retrieved 7 january 2010. 2010.

RICE, A. A quality approach to biometric imaging. In: IET. **IEE Colloquium on Image Processing for Biometric Measurement**. [S.l.], 1994. p. 4–1.

SAINT, E. F. L.; WEN, W.; HAMID, L. **Method for improving false acceptance rate discriminating for biometric authentication systems**. [S.l.]: Google Patents, 2011. US Patent 8,014,570.

SANCHES, T.; ANTUNES, J.; CORREIA, P. L. A single sensor hand biometric multimodal system. In: **15th European Signal Processing Conference, EUSIPCO 2007, Poznan, Poland, September 3-7, 2007**. [s.n.], 2007. p. 30–34. Disponível em: <http://ieeexplore.ieee.org/document/7098758/>.

SANCHEZ-REILLO, R. Hand geometry pattern recognition through gaussian mixture modelling. In: IEEE. **Proceedings 15th International Conference on Pattern Recognition. ICPR-2000**. [S.l.], 2000. v. 2, p. 937–940.

SANCHEZ-REILLO, R.; SANCHEZ-AVILA, C.; GONZALEZ-MARCOS, A. Biometric identification through hand geometry measurements. **IEEE Transactions on pattern analysis and machine intelligence**, IEEE, v. 22, n. 10, p. 1168–1171, 2000.

SAVVIDES, M.; KUMAR, B. V.; KHOSLA, P. K. Cancelable biometric filters for face recognition. In: IEEE. **Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.** [S.l.], 2004. v. 3, p. 922–925.

SONG, W. **Finger-vein identification system using level set curvature**. Tese (Doutorado) — MS Thesis, Seoul National University, 2008.

TASSABEHJI, R.; KAMALA, M. A. Evaluating biometrics for online banking: The case for usability. **International Journal of Information Management**, Elsevier, v. 32, n. 5, p. 489–494, 2012.

TULYAKOV. **"Classifier combination types for biometric applications"**. 2006. <"https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf">. Último acesso em: 10/10/2019.

VIGLIAZZI, D. **Biometria: Medidas de Segurança**. [S.l.: s.n.], 2006. v. 2.

WAVELAB. **Title of Citation**. acessado em Janeiro, 2021.

WEAVER, A. C. Biometric authentication. **Computer**, IEEE, v. 39, n. 2, p. 96–97, 2006.

WEEBLY. **"Report about Pattern classification"**. 2017. <"https://http://bxy.weebly.com/week-three.html">. Último acesso em: 10/10/2019.

WONG, F. W. M. H. et al. Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. In: IEEE. **Conference Record of Thirty-Fifth Asilomar Conference on Signals, Systems and Computers (Cat. No. 01CH37256)**. [S.l.], 2001. v. 2, p. 911–915.

YU, D.; DENG, L. **AUTOMATIC SPEECH RECOGNITION.** [S.l.]: Springer, 2016.

ZHOU, Y.; KUMAR, A. **Human identification using palm-vein images**. [S.l.]: IEEE, 2011. 1259–1274 p.