UNIVERSIDADE PAULISTA

**JOÃO VICTOR MENDES DE MORAES, ROBERTA TEIXEIRA SILVA COSTA,**

**VICTOR HUGO DE OLIVEIRA PENGA**

**Desenvolvimento de um Sistema de Identificação e Autenticação Biométrica**

BRASÍLIA

2024

**JOÃO VICTOR MENDES DE MORAES, ROBERTA TEIXEIRA SILVA COSTA,**

**VICTOR HUGO DE OLIVEIRA PENGA**

**Desenvolvimento de um Sistema de Identificação e Autenticação Biométrica**

Trabalho de Arquitetura de Redes de Computadores do curso de Ciência da Computação 5° semestre, apresentado a Universidade Paulista – UNIP, como parte do título de bacharel em Ciência da Computação.

Orientador: Prof. Fabrício Freire

BRASÍLIA

2024

**JOÃO VICTOR MENDES DE MORAES, ROBERTA TEIXEIRA SILVA COSTA,**

**VICTOR HUGO DE OLIVEIRA PENGA**

**Desenvolvimento de um Sistema de Identificação e Autenticação Biométrica**

Trabalho de Arquitetura de Redes de Computadores do curso de Ciência da Computação 5° semestre, apresentado a Universidade Paulista – UNIP, como parte do título de bacharel em Ciência da Computação.

Orientador: Prof. Fabrício Freire

Aprovado em:

Prof. Fabrício Freire

Universidade Paulista- UNIP

/ /

RESUMO

**Palavras-chaves:**

ABSTRACT

.  
  
**Keywords:**

Sumário

[1 INTRODUÇÃO 6](#_Toc191128783)

[2 REFERENCIAL TEÓRICO 7](#_Toc191128784)

[3 DESENVOLVIMENTO 8](#_Toc191128785)

[4 RESULTADOS E DISCUSSÃO 9](#_Toc191128786)

[5 CONSIDERAÇÕES FINAIS 10](#_Toc191128787)

[REFERÊNCIAS 11](#_Toc191128788)

OBJETIVO E MOTIVAÇÃO DO TRABALHO

O presente trabalho tem como objetivo o desenvolvimento de um sistema de identificação e autenticação biométrica, implementado em Python, aplicando os conceitos e tecnologias estudados ao longo do curso de Ciência da Computação. A ferramenta proposta tem como foco restringir e gerenciar o acesso a uma rede e ao banco de dados do Ministério do Meio Ambiente, onde estão armazenadas informações estratégicas sobre propriedades rurais que utilizam agrotóxicos proibidos, que podem gerar impactos em rios, mares e lençóis freáticos. O sistema deverá contemplar diferentes níveis de acesso, assegurando que informações sensíveis sejam disponibilizadas apenas a perfis autorizados, variando desde acesso público a dados gerais até consultas restritas a diretores de divisão e ao ministro do meio ambiente.

A proposta envolve o estudo de diferentes métodos biométricos e suas características, tais como reconhecimento facial, impressão digital, leitura de íris, geometria da mão, voz e assinatura, avaliando seus aspectos gerais e principais características individuais. A utilização de técnicas biométricas contribui para aumentar a segurança na identificação dos usuários, utilizando os conceitos de integridade e confidencialidade durante o processo de autenticação.

O desenvolvimento e a implementação de um sistema de identificação biométrica possibilitam a aplicação prática dos estudos abordados ao longo do trabalho sobre o método biométrico de reconhecimento facial. O trabalho de estudo feito permite desenvolver um sistema explorando diferentes ferramentas e permite também enfrentar os desafios de sua implementação.

1 INTRODUÇÃO

Autenticação é o processo de verificação da identidade de um usuário, é presente em situações cotidianas como para assinaturas em contratos, uso em caixas eletrônicos e visando a segurança em ambientes computacionais, onde surgiu o aumento de ataques às vulnerabilidades dos sistemas. Tradicionalmente, utiliza-se a autenticação usando aquilo que o indivíduo sabe ou possui, como por exemplo métodos vulneráveis a perda como chaves, e métodos vulneráveis ao esquecimento ou compartilhamento como senhas. Já a biometria oferece maior segurança por ter como base o que o indivíduo é ou faz, podendo ser complementada por recursos como a verificação ao tempo, ao espaço ou pela validação por terceiros. (KAZIENKO, 2003).

A biometria é o campo que estuda as características únicas de indivíduos, utilizadas para autenticação de identidade, podendo ser físicas, como impressões digitais, íris e geometria da mão, ou comportamentais, como assinatura e reconhecimento de voz. Diferentemente dos métodos tradicionais baseados em senhas ou cartões, as características biométricas apresentam maior segurança por não poderem ser esquecidas, emprestadas ou facilmente falsificadas (KAZIENKO, 2003).

# 2 FUNDAMENTOS DAS PRINCIPAIS TÉCNICAS BIOMÉTRICAS (CONCEITOS GERAIS)

# 2.1 Reconhecimento facial

É possível identificar seu uso em diversos dispositivos que andam lado a lado com o ser humano, como nos celulares, onde há desbloqueio quando seu usuário olha para a tela, ou em situações onde é preciso fazer a prova de vida de usuário através de biometria facial, sendo exigido comportamentos espontâneos de alguma parte da face do usuário para garantir que a ação está sendo reproduzida por um ser vivo e não uma imagem (KATO, 2024).

"As abordagens mais populares usadas no problema de reconhecimento de face se baseiam na localização e análise de atributos faciais como olhos, nariz e boca, ou na análise global da mesma, representada como combinação ponderada de uma série de faces canônicas." (MORAES, 2010)

Em sistemas de reconhecimento facial são utilizados quatro passos básicos: o primeiro passo é a detecção de uma face em uma imagem ou vídeo, em seguida definimos a localização dessa face e extraímos características e comparamos com nossa base de dados, por fim retornamos o padrão que mais se assemelha a face detectada (MORAES, 2010).

No reconhecimento facial pode haver diversas falhas, como falsos negativos ocasionados pela posição da cabeça no momento da captura, pessoas com características similares, sendo possível melhorar a confiabilidade combinando o reconhecimento facial junto a outro tipo de identificação biométrica (KATO, 2024).

# 2.2 Assinatura

A assinatura é frequentemente utilizada no nosso dia a dia, seja em transações comerciais diárias (como cartão de crédito) (JAIN; KUMAR, 2010) ou para formalizar indivíduos e organizações em contratos (MAGALHÃES; SANTOS, 2003).

O reconhecimento automático de assinaturas enfrenta limitações, principalmente pelas variações intraclasse ao longo do tempo. Para superar isso, estudos exploram assinaturas dinâmicas coletadas com dispositivos sensíveis à pressão, que registram forma, velocidade, aceleração, pressão e ordem dos traços. Esses dados adicionais melhoram a verificação e dificultam falsificações, mas ainda existem poucos sistemas implantados efetivamente. (JAIN; KUMAR, 2010).

# 2.3 Geometria da mão e impressão digital

A pele recobre externamente o corpo humano, é composta por duas camadas, sendo elas a derme e a epiderme. A derme, localizada na parte mais profunda, contém papilas com vasos sanguíneos e corpúsculos do tato, enquanto a epiderme é uma fina membrana transparente que a reveste. Na pele encontram-se elementos como cristas papilares (estrias), sulcos intercristais (vales), glândulas sebáceas (excreção de gordura) e sudoríparas (excreção de suor), além dos poros, responsáveis pela excreção do suor e situados sobre as estrias. As papilas estão presentes nas superfícies palmares e plantares, e os poros apresentam propriedades que reforçam sua utilidade na identificação biométrica, semelhantes às dos desenhos digitais. (NASCIMENTO, 2015)

A papiloscopia estuda a identificação por meio das impressões papilares, sendo dividida em: quiroscopia, podoscopia e dactiloscopia. Quiroscopia estuda impressões palmares, podoscopia estuda a planta dos pés e a dactiloscopia estuda as extremidades digitais e suas impressões. (NASCIMENTO, 2015)

A dactiloscopia identifica um humano pela sua impressão digital, podendo ser usada na área civil, para identificação de documentos, na área criminal como na identificação de digitais em cenas de crime, e na área clínica, estudando como os desenhos digitais podem ser afetados por doenças ou trabalhos específicos. (NASCIMENTO, 2015)

O desenho digital combina os cristais papilares com os sulcos interpapilares na polpa digital, a impressão digital é a reprodução desse desenho. Os elementos da impressão digital são linhas pretas impressas, que representam cristas papilares, as linhas brancas representam os sulcos interpapilares, poros são orifícios sobre as linhas impressas, as minúcias diferenciam as impressões digitais, linhas albodactiloscópicas são interrupções formadas pelas cristas papilares e delta determina o tipo e impressão digital. (NASCIMENTO, 2015)

A geometria da mão foi um meio usado ao longo da história para autenticação, as mãos em pinturas rupestres podem ter sido assinaturas dos artistas. Em 1970 foi produzido o primeiro scanner para geometria da mão, ele fazia a comparação de medidas obtidas com a medida analisada. (NASCIMENTO, 2015)

Os pinos começaram a ser utilizados visando manter a posição correta das mãos, outros métodos também envolvem o uso da iluminação infravermelha, e a utilização de métodos que usem a mão junto com a geometria da mão. (NASCIMENTO, 2015)

A biometria por geometria da mão utiliza as medidas da mão do usuário para fins de identificação ou verificação. Embora não seja tão precisa quanto métodos como a impressão digital, mostra-se adequada em contextos em que a privacidade deve ser preservada e não é necessária uma identificação absoluta, como em sistemas de controle de acesso de baixa e média segurança. Suas vantagens incluem boa aceitação entre usuários, facilidade de integração com outros sistemas biométricos e funcionamento em diferentes ambientes. Entretanto, apresenta limitações como o tamanho do dispositivo de captura, a influência de fatores externos e fisiológicos sobre a forma da mão, além da necessidade de extrair diversas características que podem ser alteradas por pressão ou mudanças naturais ao longo do tempo, resultando em menor eficácia em comparação a outros métodos biométricos. (BARROS, 2013)

# 2.4 Reconhecimento de íris

O reconhecimento de íris, conforme detalhado na obra "Introduction to Biometrics" de Jain, Ross e Nandakumar (2011), constitui um método biométrico de alta precisão e relevância. A íris, definida como a região anular do olho localizada entre a pupila e a esclera, possui uma textura visual complexa que se forma durante o desenvolvimento fetal e se estabiliza nos primeiros anos de vida. Essa característica intrínseca confere à íris um elevado grau de distintividade, tornando-a um identificador pessoal robusto (JAIN; ROSS; NANDAKUMAR, 2011).

Historicamente, os sistemas de reconhecimento de íris apresentavam desafios relacionados à necessidade de cooperação do usuário e aos custos elevados. Contudo, avanços tecnológicos têm resultado no desenvolvimento de sistemas mais acessíveis e amigáveis, ampliando sua aplicabilidade. A eficácia desses sistemas é evidenciada por seu desempenho em cenários de identificação em larga escala (JAIN; ROSS; NANDAKUMAR, 2011).

A implementação de um sistema de reconhecimento de íris envolve diversas etapas, incluindo a aquisição da imagem, a segmentação da íris do restante do olho, a normalização para compensar variações de tamanho e rotação, a codificação da textura da íris em um formato digital e, finalmente, a correspondência entre as amostras. A qualidade da imagem capturada é um fator crítico que influencia diretamente a precisão do reconhecimento, sendo objeto de técnicas específicas para sua avaliação e aprimoramento (JAIN; ROSS; NANDAKUMAR, 2011).

O desempenho de sistemas de reconhecimento de íris tem sido consistentemente avaliado em testes de tecnologia, demonstrando taxas de erro competitivas. Por exemplo, em avaliações sob condições controladas de iluminação, os sistemas de íris apresentaram baixas taxas de falsa rejeição e falsa aceitação, confirmando sua confiabilidade para aplicações de segurança (JAIN; ROSS; NANDAKUMAR, 2011).

# 2.5 Reconhecimento de voz

O reconhecimento de voz, ou reconhecimento de locutor, é uma área multifacetada da biometria que se distingue pela sua natureza inerentemente multidisciplinar, conforme abordado por Beigi (2011) em "Fundamentals of Speaker Recognition". Diferentemente do reconhecimento de fala, que se concentra no conteúdo da mensagem, o reconhecimento de locutor visa identificar ou verificar a identidade de uma pessoa com base nas características únicas de sua voz (BEIGI, 2011).

A complexidade do reconhecimento de locutor reside na sua dependência de diversas áreas do conhecimento, incluindo cinemática, dinâmica, controle, processamento de sinais, otimização, teoria de aprendizado de redes neurais e compressão de imagem. Essa interconexão de disciplinas é fundamental para a compreensão profunda do tema e para o desenvolvimento de sistemas eficazes (BEIGI, 2011).

Beigi (2011) categoriza o reconhecimento de locutor em ramos "simples" e "compostos". Os ramos simples incluem a verificação de locutor (autenticação), a identificação de locutor e a classificação de locutor. A verificação de locutor, por exemplo, é o ramo mais popular devido à sua importância em segurança e controle de acesso, e envolve a comparação da voz de um indivíduo com um modelo de referência para confirmar sua identidade declarada. A identificação de locutor, por sua vez, pode ser de conjunto fechado (onde o locutor está necessariamente no banco de dados) ou de conjunto aberto (onde o locutor pode não estar no banco de dados), sendo esta última mais complexa por exigir um mecanismo de rejeição (BEIGI, 2011).

Os ramos compostos, que utilizam uma ou mais manifestações simples, incluem a segmentação de locutor, a detecção de locutor e o rastreamento de locutor. A segmentação, por exemplo, é crucial para dividir um fluxo de áudio em partes que contêm a fala de diferentes locutores, música ou ruído, sendo fundamental para aplicações como a transcrição de conversas em teleconferências (BEIGI, 2011).

Uma das principais vantagens do reconhecimento de locutor é a sua capacidade de ser testado remotamente através da infraestrutura de rede telefônica existente, tornando-o inigualável em muitas aplicações do mundo real. No entanto, a modalidade de reconhecimento de locutor pode variar, incluindo sistemas dependentes de texto (onde uma frase específica é exigida), independentes de texto (mais versáteis, mas suscetíveis a gravações) e solicitados por texto (que combinam a flexibilidade do independente de texto com a segurança de uma frase específica para combater falsificações) (BEIGI, 2011).

Apesar de sua promessa, o reconhecimento de locutor enfrenta desafios como a variabilidade da voz (devido a doenças, emoções ou falta de cobertura fonética), efeitos do canal de comunicação (ruído, variabilidade do canal) e compressão de áudio, que podem degradar a qualidade do sinal e, consequentemente, o desempenho do sistema. No entanto, a pesquisa contínua busca mitigar esses problemas, tornando o reconhecimento de locutor uma ferramenta biométrica cada vez mais robusta e aplicável em diversas áreas, desde aplicações financeiras e forenses até controle de acesso e indexação de áudio e vídeo (BEIGI, 2011).

# 3 PLANO DE DESENVOLVIMENTO DA APLICAÇÃO (ELEMENTOS E FERRAMENTAS QUE SERÃO UTILIZADAS)

# 3.1 Python

# 3.2 MariaDB

Um sistema de gerenciamento de banco de dados (SGBD) é um software projetado para gerenciar a estrutura de um banco de dados e controlar o acesso aos dados armazenados. O SGBD age como o intermediário entre os usuários ou aplicações e o banco de dados. A complexidade interna é ocultada pelo SGBD, facilitando a interação com os dados. Um banco de dados, por sua vez, é uma estrutura computacional que armazena dados brutos de usuários e metadados, descrevendo suas características e relacionamentos. O uso de um SGBD promove vantagens cruciais para o gerenciamento de dados, proporcionando um acesso mais eficiente e organizado às informações (ROB; CORONEL, 2011).

O MariaDB Server é um dos bancos de dados relacionais de código aberto mais populares do mundo, criado pelos desenvolvedores originais do MySQL com a garantia de permanecer um software livre. Utilizado como um substituto aprimorado do MySQL, sua ampla adoção em serviços de nuvem e distribuições Linux, por usuários notáveis como Wikipédia e Google, é atribuída à sua construção focada em desempenho, estabilidade e escalabilidade.

# 3.3 Deepface

A biblioteca DeepFace constitui uma solução abrangente e acessível para reconhecimento facial e análise de atributos faciais em Python. Esta ferramenta de código aberto se distingue por sua simplicidade de implementação, permitindo que desenvolvedores executem tarefas complexas de reconhecimento facial com apenas algumas linhas de código, sem necessidade de conhecimento aprofundado dos processos subjacentes. A biblioteca oferece quatro funcionalidades principais: verificação facial para comparação entre faces, reconhecimento facial em bancos de dados de imagens, análise de atributos faciais como idade e emoções, e análise em tempo real através de feeds de vídeo (KLINGLER, 2023).

A DeepFace apresenta características técnicas que facilitam sua adoção pela comunidade de desenvolvedores. Sua arquitetura leve, baseada principalmente em TensorFlow e Keras, evita as complexidades de instalação associadas a dependências em C e C++. A biblioteca integra sete modelos de reconhecimento facial de última geração e cinco detectores faciais avançados, oferecendo flexibilidade na escolha de algoritmos. Sua licença MIT garante liberdade total de uso para propósitos individuais e comerciais, contribuindo para o desenvolvimento de uma comunidade ativa com milhares de usuários e contribuidores (KLINGLER, 2023).

O projeto mantém desenvolvimento contínuo com planos para incorporar novos recursos, incluindo modelos adicionais de atributos faciais e reconhecimento, além do desenvolvimento de uma API em nuvem. A arquitetura independente de linguagem permite implementação tanto local quanto através de APIs, facilitando integração com aplicações móveis e web. Em síntese, a DeepFace democratiza o acesso a tecnologias avançadas de reconhecimento facial, combinando facilidade de uso, robustez técnica e flexibilidade de implementação em uma única biblioteca de código aberto (KLINGLER, 2023).

# 4 PROJETO (ESTRUTURA E MÓDULOS QUE SERÃO DESENVOLVIDOS) DO PROGRAMA

# 5 RELATÓRIO COM AS LINHAS DE CÓDIGO DO PROGRAMA

# 5 APRESENTAÇÃO DO PROGRAMA EM FUNCIONAMENTO EM UM COMPUTADOR, APRESENTANDO TODAS AS FUNCIONALIDADES PEDIDAS E EXTRAS

**REFERÊNCIAS**

**FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS**