UNIVERSIDADE PAULISTA

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO

DIEGO FREIRE DE ALMEIDA, N8059D2

KAIKY DE LARA SALES, N9218H8

LEONARDO DE SOUZA RODRIGUES, F344HB2

NÍCOLAS PIMENTA DA SILVA, N863579

VITOR DOS SANTOS ROSA, G521CE3

AUTENTICAÇÃO BIOMÉTRICA - SEGURANÇA PARA INVESTIGAÇÕES GOVERNAMENTAIS

Jundiaí – SP

2024

DIEGO FREIRE DE ALMEIDA, N8059D2

KAIKY DE LARA SALES, N9218H8

LEONARDO DE SOUZA RODRIGUES, F344HB2

NÍCOLAS PIMENTA DA SILVA, N863579

VITOR DOS SANTOS ROSA, G521CE3

AUTENTICAÇÃO BIOMÉTRICA - SEGURANÇA PARA INVESTIGAÇÕES GOVERNAMENTAIS

Artigo das atividades práticas supervisionadas, apresentado ao Curso de Ciência da Computação para composição de nota.

Orientador: Prof. Marcos Paulo

Jundiaí – SP

2024

SUMÁRIO

1. RESUMO

A cibersegurança tornou-se um aspecto fundamental no cenário tecnológico atual, especialmente quando consideramos os sistemas atuais, que constantemente crescem e evoluem, assim tendo que lidar com uma grande quantidade de dados. Com esse crescimento acelerado, as ameaças cibernéticas também vêm crescendo e se tornando mais sofisticadas, aumentando o risco à integridade e confiabilidade dos dados. Por esse motivo, as empresas vêm realizando investimentos contínuos e significativos em novas soluções e sistemas de segurança, a fim de acompanhar a evolução das ameaças, sempre garantindo o resguardo e proteção dos dados.

Este trabalho tem como objetivo a implementação de um sistema de proteção baseado no reconhecimento biométrico facial, com o intuito de gerenciar o acesso de um banco de dados sensível. O uso da biometria facial foi essencial devido a ser uma tecnologia mais precisa e acessível, superando as formas de segurança tradicionais. A motivação central surgiu da necessidade de aprofundar nos conceitos teóricos sobre segurança digital e proteção de dados, além de aplicar esses conceitos na prática.

Em resumo, o trabalho busca explorar a área de cibersegurança e proteção de dados, com o propósito de aprofundar o entendimento das estratégias eficazes para esse problema que afeta não apenas no âmbito corporativo, mas também no contexto pessoal e governamental.

2. INTRODUÇÃO

A autenticação biométrica tem se tornado cada vez mais relevante no cenário atual de cibersegurança, oferecendo uma alternativa robusta e conveniente aos métodos tradicionais de autenticação. No contexto da ciência da computação, o desenvolvimento de sistemas que utilizam características biológicas únicas para verificar a identidade de um indivíduo representa um avanço significativo na proteção de dados sensíveis e no controle de acesso a sistemas críticos.

A importância da autenticação por biometria reside em diversos fatores. Primeiramente, ela oferece um nível de segurança superior aos métodos

tradicionais, como senhas ou tokens, pois se baseia em características físicas únicas e difíceis de serem replicadas ou roubadas. Além disso, a autenticação biométrica proporciona uma experiência de usuário mais fluida e conveniente, eliminando a necessidade de memorizar senhas mais complexas ou carregar dispositivos adicionais.

No contexto empresarial e institucional, a implementação de sistemas biométricos pode resultar em uma redução significativa de custos associados à manutenção de sistemas de autenticação tradicionais, além de oferecer um controle mais eficiente de acesso e presença. A versatilidade da autenticação biométrica também permite sua aplicação em diversos setores, desde a segurança bancária até o controle de fronteiras, demonstrando seu potencial para revolucionar a forma como gerenciamos a identidade digital.

À medida que as ameaças cibernéticas se tornam mais sofisticadas, a necessidade de métodos de autenticação mais seguros e confiáveis cresce proporcionalmente. Neste contexto, o desenvolvimento de soluções biométricas, como o software proposto neste trabalho, representa uma contribuição valiosa para o campo da segurança da informação e para a evolução das práticas de autenticação na era digital.

3. PROBLEMA ABORDADO NO TRABALHO E OBJETIVOS

O reconhecimento facial, em particular, oferece vantagens únicas em comparação com outras modalidades biométricas. Sua capacidade de realizar autenticação de forma não intrusiva e à distância o torna ideal para uma variedade de aplicações, desde o desbloqueio de dispositivos móveis até o controle de acesso em áreas de alta segurança. Além disso, os avanços recentes em inteligência artificial e aprendizado de máquina têm melhorado significativamente a precisão e a confiabilidade dos sistemas de reconhecimento facial, tornando-os cada vez mais robustos contra tentativas de fraude.

Este trabalho, desenvolvido no âmbito do 6º semestre do curso de Ciência da Computação, concentra-se na implementação de um software de autenticação biométrica baseado em reconhecimento facial para proteger um banco de dados. A escolha do reconhecimento facial como método de autenticação biométrica se deve à sua combinação de alta segurança e

facilidade de uso, características essenciais para sistemas modernos de proteção de dados.

Ao longo do desenvolvimento deste projeto, serão abordados os fundamentos teóricos do reconhecimento facial, as técnicas e algoritmos utilizados na implementação do software, os desafios enfrentados durante o processo e as soluções propostas. Além disso, serão discutidos os resultados obtidos em termos de precisão, eficiência e segurança do sistema, bem como suas convenientes aplicações.

4. APORTES TEÓRICOS

A biometria, consiste no estudo estatístico das características físicas e comportamentais dos organismos vivos. Nos últimos anos, esse conceito expandiu-se para incluir a análise de atributos físicos e comportamentais específicos de seres humanos, com a finalidade de identificá-los de maneira única e precisa. Esse campo é aplicado em uma variedade de contextos, incluindo a identificação criminal, controle de acesso a instalações e dispositivos, autenticação em sistemas digitais e até em transações financeiras e segurança nacional. Os sistemas biométricos baseiam-se em características corporais que variam conforme a parte do corpo analisada, como padrões das írises e da retina, contornos da palma da mão, digitais dos dedos e estruturas faciais. A premissa fundamental desses sistemas é que cada indivíduo possui traços físicos e comportamentais exclusivos — como a voz, a maneira de caminhar, o ritmo cardíaco ou o calor das mãos — que permitem sua distinção dos demais.

Na seção a seguir, serão apresentados os recursos técnicos e metodológicos utilizados para a construção da solução proposta neste trabalho. Serão descritos os equipamentos, ferramentas de software e algoritmos empregados, assim como os processos específicos de coleta, processamento e análise dos dados biométricos. Essa seção busca detalhar como cada recurso foi aplicado para garantir precisão, eficiência e segurança no desenvolvimento da solução, permitindo uma compreensão clara dos fundamentos técnicos que sustentam a implementação.

Todas as definições e descrições das técnicas de biometria abordadas neste trabalho baseiam-se nos estudos de diversos autores. As tecnologias de

leitura de impressões digitais eletrônicas e de contato com tinta são fundamentadas nas pesquisas de Duarte (2004) e Ferreira (1999), respectivamente. As características invariáveis das impressões digitais, conforme Pankati (2000), e o registro direto por glândulas sudoríparas discutido por Tavares Junior (1991), complementam a compreensão desse método. A biometria de íris é sustentada pelos estudos de Kalyani (2017) e Li e Jain (2015), enquanto Jacquet e Champod (2020) discutem a aplicação do reconhecimento facial em ciência forense. Por fim, a utilização da biometria em dispositivos móveis é abordada por Mitra e Gofman (2016), e Sumares (2018) explora o monitoramento facial em eventos de grande porte.

4.1. Linguagem de programação e biblioteca

Para que a aplicação fosse desenvolvida utilizamos a linguagem C# e uma série de recursos gratuitos, com o intuito de abordar diversas vertentes do projeto. Em seguida está uma breve descrição das tecnologias utilizadas para endereçar cada uma delas.

Área	**Tecnologia**
Reconhecimento Facial	Biblioteca FaceAiSharp
Armazenamento	SQLite
Comunicação com a Câmera	Biblioteca OpenCvSharp4

A escolha de C# como linguagem para desenvolvimento de um sistema de biometria facial é vantajosa por sua estrutura orientada a objetos, facilidade de manutenção, e forte suporte para integração com bibliotecas externas, que possibilitam uma implementação modular e escalável de funções biométricas. Segundo Maltoni et al. (2009), C# oferece uma base sólida para sistemas biométricos devido à sua capacidade de integrar tecnologias de processamento de imagem e dispositivos de captura em tempo real, características fundamentais para um sistema de reconhecimento facial.

Neste trabalho, o uso da biblioteca FaceAiSharp em C# possibilita a implementação de algoritmos complexos de reconhecimento facial, viabilizando a extração e o mapeamento de pontos faciais (como distâncias entre olhos, largura do nariz e contornos da mandíbula) em tempo real. O FaceAiSharp se destaca pelo suporte a operações rápidas e precisas de detecção e

reconhecimento, fatores essenciais para aplicações biométricas que exigem alta confiabilidade.

Além disso, a biblioteca OpenCvSharp4 permite que o sistema se comunique diretamente com a câmera, capturando imagens ao vivo com alta eficiência e qualidade. Essa integração é fundamental, pois o sistema precisa processar imagens faciais em tempo real e transformar essas imagens em dados biométricos imediatamente comparáveis com as referências existentes no banco de dados. O OpenCvSharp4 facilita a captura contínua de imagens e oferece uma interface de programação acessível para manipulação de vídeos e imagens diretamente em C#, alinhando-se perfeitamente aos requisitos de um sistema biométrico.

Portanto, a utilização de C# em conjunto com FaceAiSharp e OpenCvSharp4 não apenas facilita o desenvolvimento de uma aplicação biométrica funcional e eficaz, mas também garante que o sistema atenda a critérios de precisão e velocidade, fundamentais em sistemas de segurança biométrica.

4.2. Dispositivo para captura das imagens

Para a implementação do sistema de biometria facial proposto, utilizou-se um dispositivo computadorizado, que pode ser um notebook ou desktop, operando com o sistema operacional Windows 10 ou versão superior. A escolha por Windows garante compatibilidade com as bibliotecas necessárias (FaceAiSharp e OpenCvSharp4) e estabilidade na execução de tarefas exigentes em processamento.

O sistema requer uma câmera de boa qualidade, que pode ser integrada ao dispositivo ou conectada externamente, com uma resolução mínima recomendada de 720p. Essa resolução permite a captura de detalhes faciais essenciais para um reconhecimento preciso, evitando distorções e garantindo que os algoritmos possam mapear as características faciais com exatidão.

Para otimizar a captação de imagens, o sistema deve ser utilizado em um ambiente com iluminação adequada, de modo a reduzir sombras e melhorar o contraste das características faciais. Além disso, é recomendado que apenas o rosto do usuário esteja em foco diante da lente da câmera, minimizando interferências visuais e permitindo que o sistema foque exclusivamente nos pontos biométricos necessários para a análise e comparação facial.

5. DESENVOLVIMENTO

A biometria não é um conceito contemporâneo; suas raízes podem ser rastreadas em civilizações passadas, onde já se buscava registrar características pessoais. Na antiga China, por exemplo, artesãos usavam suas impressões digitais como uma marca de autoria ao imprimirem-nas em peças de cerâmica, associando suas identidades às obras que produziam. Este ato de registro pessoal ilustra uma forma primitiva de autenticação e preservação de identidade. Nos Estados Unidos, o uso sistemático das impressões digitais para identificação de criminosos foi iniciado no início do século XX, especificamente em Nova York. Esse processo evoluiu significativamente nas duas décadas seguintes, culminando na criação da Divisão de Identificação do FBI pelo Congresso Americano. Esse órgão consolidou a prática da biometria no sistema de justiça criminal, adotando-a como método confiável e eficiente para identificar prisioneiros e foragidos. Em 1946, o FBI já possuía um acervo com mais de 100 milhões de impressões digitais, registradas manualmente em cartões de identificação. Este arquivo monumental de dados biométricos representava um marco na institucionalização da biometria como ferramenta de segurança pública.

Com o avanço tecnológico, a biometria passou por um processo de modernização que a integrou aos sistemas digitais. No contexto atual, o uso de algoritmos sofisticados de inteligência artificial e aprendizado de máquina tem permitido uma precisão e confiabilidade cada vez maiores na autenticação biométrica. Sistemas biométricos modernos, por exemplo, fazem uso de reconhecimento facial, detecção de emoções, análise de padrões de batimento cardíaco e até mapeamento de veias. Essas tecnologias são aplicadas de forma expansiva em smartphones, sistemas de vigilância pública, controle de fronteiras e transações financeiras, assegurando uma proteção mais abrangente contra fraudes e acessos não autorizados.

Outro campo em crescimento é a biometria comportamental, que analisa padrões de comportamento, como a forma de digitar, a pressão ao tocar uma tela sensível ao toque e até mesmo o uso do mouse em um computador. Esse tipo de biometria é particularmente valioso em ambientes digitais, onde a

necessidade de segurança é contínua e pode ser aplicada sem a necessidade de interação física com o usuário.

Em perspectiva futura, os avanços na biometria prometem um impacto ainda maior. Inovações emergentes, como o reconhecimento de DNA e o uso de biochips implantáveis, apresentam-se como novas fronteiras que expandem o alcance da identificação biométrica. Estes desenvolvimentos oferecem o potencial para revolucionar áreas de segurança, personalização de serviços e até saúde, onde a biometria pode ser utilizada para monitoramento de condições médicas e resposta a emergências em tempo real.

A seguir, serão apresentadas as principais técnicas observadas em implementações comumente encontradas nos dias de hoje, a exemplo da biometria fácil, tecnologia utilizada neste trabalho bem as ferramentas e recursos usadas para a implementação da solução.

5.1. Biometria digital

Nesta técnica, temos o que chamamos de impressão digital (Imagem 1). Esta refere-se à marca deixada pela reprodução das papilas da pele, localizadas nas extremidades dos dedos das mãos e dos pés, sobre uma superfície lisa. Essa reprodução pode ser feita através de substâncias como tinta, que permitem que a marca seja visível (FERREIRA, 1999), ou capturada eletronicamente por meio de dispositivos de leitura de impressões digitais (ID) (DUARTE, 2004, p.3).

Imagem 1 - Impressão digital.

Fonte: Vexels, 2024.

Essas marcas são constituídas por padrões de cristas e sulcos gerados pelas dobras cutâneas na epiderme, camada externa da pele, e que têm origem na camada subjacente, a derme. Esses padrões começam a se formar ainda no

período fetal, aproximadamente ao sexto mês de gestação, e estabelecem-se de forma permanente, criando configurações únicas e imutáveis ao longo da vida. Embora as digitais possam aumentar em tamanho à medida que o indivíduo cresce, o desenho essencial permanece invariável, a menos que fatores externos, como lesões ou queimaduras, causem mudanças irreversíveis na pele (PANKATI, 2000, p.3). Mesmo gêmeos idênticos, que compartilham a mesma carga genética, apresentam padrões de impressões digitais diferentes. Além disso, cada dedo possui um padrão distinto de cristas, tornando impossível correlacionar diretamente as impressões digitais entre os diferentes dedos de uma mesma pessoa.

A marca digital também pode ser transferida para superfícies devido ao contato com substâncias corporais naturais. Quando um dedo entra em contato com uma superfície, as glândulas sudoríparas e sebáceas, presentes nas cristas da pele, secretam suor e pequenas quantidades de gordura, que são eliminados pelos poros da pele e permitem a transferência do desenho das cristas para essa superfície. Dessa maneira, uma impressão digital pode ser registrada sem necessidade de substâncias externas, bastando o contato direto do dedo, o que gera uma imagem detalhada dos padrões papilares (TAVARES JUNIOR, 1991, p.30).

Com o avanço tecnológico, a captura das impressões digitais através de leitores de ID tornou-se uma técnica amplamente adotada. Segundo Duarte (2004, p.3), o método de captura eletrônica é considerado mais eficaz do que os processos tradicionais, como a aplicação de tinta, uma vez que evita distorções de imagem causadas pelo excesso ou insuficiência de tinta e pela variação da pressão aplicada ao pressionar o dedo. O leitor eletrônico utiliza um sistema que converte as características físicas da impressão digital em um “template” digital, garantindo uma leitura precisa e reproduzível para uso em sistemas de identificação biométrica.

Essa confiabilidade dos leitores de ID é particularmente relevante para sistemas biométricos modernos, onde a precisão e a consistência dos dados são cruciais para a segurança e a identificação de indivíduos em contextos como controle de acesso e autenticação pessoal. O uso desses leitores reduziu substancialmente o erro humano na coleta de impressões, facilitando a criação de bases de dados robustas e permitindo que a biometria digital seja amplamente adotada em dispositivos móveis e plataformas de segurança digital.

5.2. Biometria da íris

A íris, o músculo responsável pela coloração dos olhos (Imagem 2), apresenta características únicas para cada indivíduo, mantendo-se inalterada ao longo da vida. Em 1936, o oftalmologista Burch propôs o uso da íris como método de identificação, mas somente em 1989 o matemático Daugman desenvolveu os algoritmos necessários, que hoje são amplamente usados em scanners de íris. Esses dispositivos utilizam câmeras infravermelhas (700-900 nm) para digitalizar e codificar a imagem da íris, que é então armazenada para fins de comparação em sistemas de identificação biométrica (LI; JAIN, 2015). A identificação é robusta, pois a córnea protege a íris de danos, permitindo que o reconhecimento funcione mesmo com óculos ou lentes de contato (KALYANI, 2017).

Imagem 2 - Íris ocular.

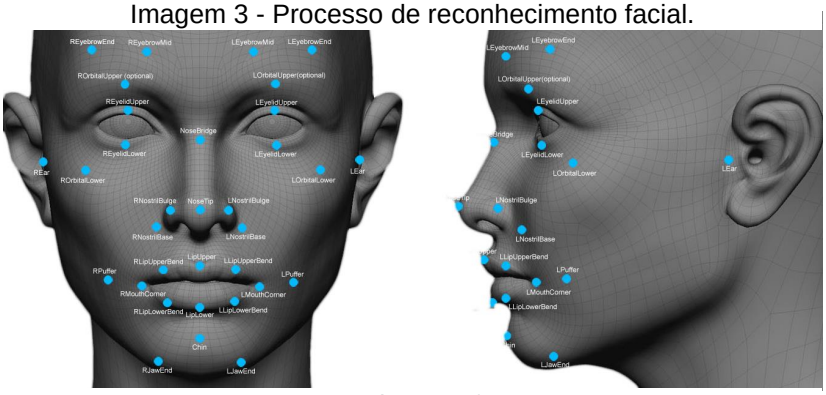
Fonte: Wikipédia, 2024

Por outro lado, a biometria de retina, uma tecnologia relacionada, utiliza a leitura do padrão de vasos sanguíneos localizados na retina, a camada mais interna do olho. Essa captação ocorre através de um feixe de luz de baixa intensidade direcionado ao olho, que ilumina os vasos sanguíneos únicos da retina. Essa imagem é então analisada e armazenada em um sistema de dados biométricos. Como esses vasos são exclusivos e complexos, a biometria da retina é altamente precisa e utilizada em sistemas de alta segurança.

5.3. Biometria facial

A técnico empregada nesta implementação. O método leitura facial (Imagem 3), fundamenta-se na coleta de imagens tridimensionais e na análise de métricas de uma face, extraindo pontos de referência do rosto para estabelecer uma ligação algorítmica entre características como traços e dimensões. A partir dessas informações, o sistema processa e compara a face capturada com imagens previamente registradas no banco de dados. Esse tipo de biometria pode operar de duas formas distintas: em uma, o próprio sistema realiza o reconhecimento e autoriza o acesso; na outra, um técnico verifica a correspondência entre a imagem registrada e o rosto do indivíduo presente.

Imagem 3 - Processo de reconhecimento facial.



Fonte: Projeto Draft, 2024.

Os algoritmos de reconhecimento facial podem ser aplicados em dois cenários principais: verificação e identificação. No contexto de verificação, o sistema faz uma comparação direta entre a imagem de uma pessoa desconhecida e uma imagem de referência já registrada. Esse procedimento é amplamente utilizado em dispositivos como celulares e computadores para liberar o acesso ao usuário. O sistema avalia o grau de semelhança entre as imagens, e, se a pontuação obtida ultrapassa um limite predefinido, o acesso é autorizado; caso contrário, o acesso é negado. Na identificação, por outro lado, o sistema compara a imagem de uma pessoa desconhecida com todas as imagens armazenadas no banco de dados. Esse processo busca os candidatos mais semelhantes e é amplamente empregado em investigações forenses (JACQUET; CHAMPOD, 2020).

Em 2017, durante a final da Champions League, foi implementado um sistema de monitoramento biométrico por reconhecimento facial. No entanto, ele apresentou uma taxa de 92% de falsos positivos; dos 2.470 indivíduos identificados como criminosos, apenas 173 foram confirmados pela polícia do

Sul de Gales (SUMARES, 2018). Apesar dessa limitação, o reconhecimento facial vem sendo integrado a dispositivos tecnológicos para garantir tanto a segurança de usuários de eletrônicos, como celulares, quanto de grandes populações em áreas urbanas. Atualmente, vários modelos de smartphones contam com sistemas de reconhecimento facial, permitindo que os usuários acessem aplicativos e recursos do aparelho de forma rápida e segura (MITRA; GOFMAN, 2016).

5.4. Biometria comportamental

A biometria comportamental é um dos diversos tipos de sistemas de proteção de dados e cibersegurança existentes atualmente, destacando-se pelo seu alto nível de eficácia. Ela utiliza padrões comportamentais únicos, como a forma de digitação de uma pessoa, para verificar sua identidade. Diferente das formas tradicionais de biometria, como impressões digitais e reconhecimento facial, que se baseiam em características físicas, a biometria comportamental foca nas interações e nos padrões de uso dos dispositivos, proporcionando uma camada adicional de segurança e personalização (Imagem 4).

A biometria comportamental pode ser dividida em três principais etapas:

1. Captura: É o momento de aquisição dos comportamentos. Na biometria comportamental, isso ocorre de forma passiva conforme o usuário interage com o sistema. Alguns comportamentos analisados incluem:

- Movimento do telefone: O telefone está sendo segurado em posição de paisagem ou retrato? Qual é a rotação ou o ângulo do telefone?
- Comportamento na tela sensível ao toque: Qual é o formato do dedo utilizado? Quanta pressão está sendo exercida?
- Comportamento no teclado: Como o teclado é usado? Qual é o ritmo de digitação? Alguma tecla especial foi pressionada? Algum atalho foi utilizado?

2. Extração: Consiste na análise dos dados coletados, gerando um modelo comportamental específico para aquele usuário.

3. Comparação: Quando há necessidade de autenticação, o sistema compara o modelo do usuário com os dados recentes coletados durante a tentativa de acesso.

Imagem 4 - Processo de biometria comportamental.

Fonte: *MELO JUNIOR, Wilson. Autenticação de Sistemas Baseados em Biometria Comportamental,* 2024.

Muitas empresas de tecnologia, bancos e até redes sociais já adotaram a biometria comportamental como forma de proteção adicional. Instituições financeiras, como o Bank of America e o HSBC, utilizam-na para detectar fraudes em transações bancárias, enquanto plataformas como o PayPal empregam essa tecnologia para autenticar usuários com mais precisão. Outras empresas especializadas em segurança cibernética, como a BioCatch e a BehavioSec, oferecem soluções baseadas em biometria comportamental para empresas ao redor do mundo.

A biometria comportamental pode gerar vários benefícios como Aumento da segurança: criando uma camada extra de segurança ao autenticar a identidade de uma pessoa com base em seu comportamento único, dificultando fraudes e roubos de identidade. Experiência do Usuário mais Fluida: Como a captura dos dados é passiva, a biometria comportamental permite que a autenticação ocorra de forma invisível ao usuário, sem necessidade de interrupções. Autenticação Contínua: Em vez de uma verificação única, como a senha digitada uma única vez, a biometria comportamental pode autenticar continuamente ao longo da sessão, melhorando a segurança em sistemas de acesso prolongado. Menor Dependência de Senhas: A biometria comportamental pode complementar ou até substituir as senhas tradicionais, reduzindo o risco associado ao uso de senhas fracas ou repetidas.

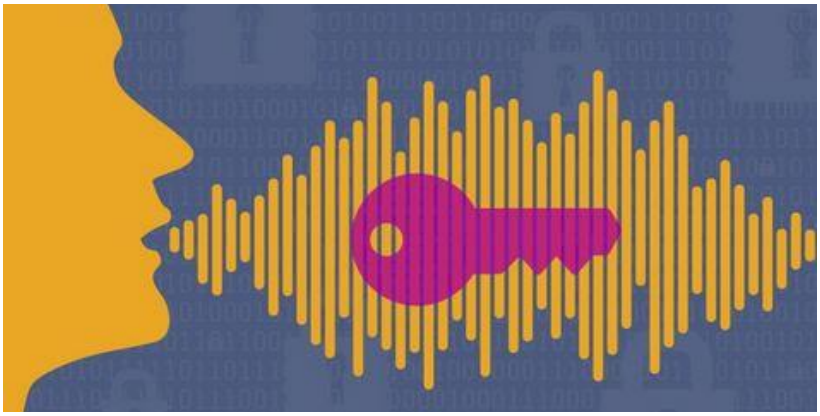
5.5. Biometria por voz

A biometria por voz é uma tecnologia que se baseia no treinamento de um modelo que utiliza fatores fisiológicos e comportamentais dos indivíduos para autenticação. Um aspecto central dessa tecnologia é a identidade sonora, que é uma característica composta por diversos elementos, como idioma, timbre de voz, sotaque, dicção e todos os aspectos notáveis que definem a maneira como um indivíduo fala. Esses fatores formam o componente biométrico.

O sistema de biometria por voz opera a partir de um modelo inicial, que é criado mediante a captura de amostras da voz do usuário. Esse processo envolve a gravação de uma série de frases ou palavras, permitindo que o sistema análise e armazene as características únicas da voz do indivíduo. Essas amostras são fundamentais para o treinamento do algoritmo, que aprende a identificar padrões e nuances específicas da fala. Assim, ao longo do tempo, o modelo se torna mais preciso na autenticação, sendo capaz de reconhecer a voz do usuário mesmo em diferentes condições ambientais ou variações naturais na fala.

Análise de Características da Voz O algoritmo examina gravações de áudio em busca de características que são difíceis de imitar, como a frequência natural da voz, o padrão de entonação e o ritmo da fala. Deep fakes geralmente apresentam pequenas discrepâncias nessas características, que podem ser identificadas por sistemas de biometria de voz treinados. Comparação com Espectrograma da Voz Quando um áudio é submetido para autenticação, o sistema compara as características da voz no áudio suspeito com o espectrograma da voz. O espectrograma é uma representação visual única gerada pelas ondas sonoras de uma pessoa (Imagem 5).

Imagem 5 – Espectrograma de reconhecimento vocal.



Fonte: Boson treinamentos, 2024.

Podemos citar alguns benefícios como, Segurança Aprimorada: A biometria de voz utiliza características únicas da voz humana, tornando-a difícil de falsificar. Isso proporciona um nível elevado de segurança contra fraudes e ataques cibernéticos, já que a voz é uma característica intrínseca que não pode ser facilmente replicada.

Detecção de Fraudes: Os sistemas de biometria de voz são eficazes na identificação de deep fakes e outras tentativas fraudulentas. Eles analisam características da voz, como frequência, entonação e ritmo, para detectar discrepâncias que podem indicar fraudes.

Integração Simples: A biometria de voz pode ser implementada utilizando equipamentos comuns, como microfones e telefones, sem a necessidade de hardware especializado. Isso facilita sua adoção em diferentes plataformas e serviços.

6. ESTRUTURA DO SISTEMA IMPLEMENTADO

Nesta sessão, iremos descrever os principais pontos que foram considerados no processo de planejamento do projeto, tão quanto seus principais elementos técnicos que foram cruciais para a sua implementação.

Para manter o projeto em um escopo atingível, seguimos com quatro principais requisitos simples que iriam garantir a sua funcionalidade básica:

- Autenticação através de biometria facial
- Níveis de acesso
- Interface contendo login e visualização das informações
- Cadastro de novos usuários

O sistema foi estruturado com o seguinte caso de uso: Um sistema capaz de restringir o acesso a dados de propriedades rurais que estão sendo investigadas devido ao uso de agrotóxicos proibidos. Este acesso deve ser segmentado de acordo com o perfil no momento do login, mostrando apenas as informações pertinentes.

Para a interação com o nosso programa, foi criada uma interface simples utilizando uma das mais famosas tecnologias para interface em Windows, a Windows Forms. Além de ser uma estrutura relativamente simples de ser

implementada, ela é extremamente leve amigável tanto para o usuário, quanto para o desenvolvedor.

Em seguida, estão todas as telas desenvolvidas e uma breve descrição de seus elementos.

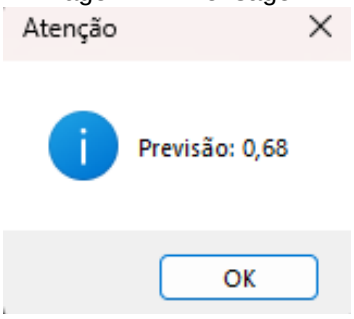
Imagem 6 - Reconhecimento da face.

Fonte: Elaboração própria.

Na aba de login, é onde a interação inicial irá ocorrer (Imagem 6). É de longe, a mais importante, pois é ela quem irá se comunicar com as outras janelas da aplicação e irá interagir com o banco de dados para definir o nível de acesso do usuário que está logado.

Ao digitar o CPF e clicar em “Iniciar captura”, uma verificação será realizada no banco de dados para termos certeza que o usuário está cadastrado. ;Se o usuário estiver de fato cadastrado, o sistema irá iniciar a câmera do dispositivo e o usuário poderá clicar em “Verificar”, capturando uma imagem temporária do frame que estiver na tela e comparando com a imagem que está atrelada ao usuário, armazenada no diretório da aplicação. Uma mensagem indicando o valor da previsão irá aparecer na tela do usuário (imagem 7), onde

Imagem 7 – Mensagem.



Fonte: Elaboração própria.

deve ser mais do que 0.6 para indicar como um “positivo” – ou seja, indicar que de fato é o usuário da foto que foi salva anteriormente.

Com a autenticação em um resultado positivo, a aplicação irá navegar automaticamente para a aba “Informações”, onde em seu carregamento ela irá se comunicar com o banco de dados SQLite e recuperar as informações do usuário autenticado, sendo elas:

- Perfil
- Nome

De acordo com o perfil, podemos ter três nívels de acesso:

- Nível 1 – Poderá visualizar informações públicas – Baixa
- Nível 2 – Informações Públicas e Confidenciais – Baixa e Média
- Nível 3 – Informações Públicas, Confidenciais e Altamente Confidenciais – Alta, Média e Baixa

Abaixo estão as três variações de acordo com os níveis de acesso:

Perfil Público – Acesso a Informações de classificação baixa, sem acesso a cadastros (Imagem 8).

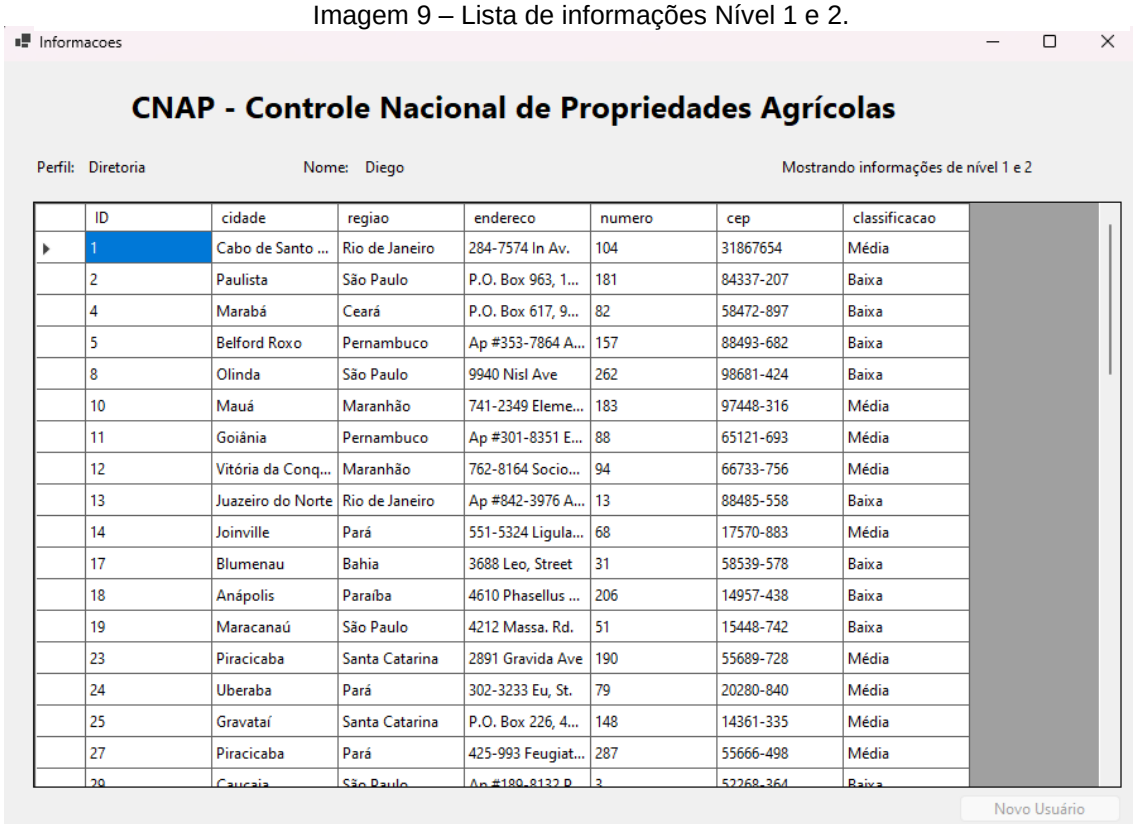
Imagem 8 – Lista de informações classificação baixa.

ID	cidade	regiao	endereco	numero	cep	classificacao
2	Paulista	São Paulo	P.O. Box 963, 1...	181	84337-207	Baixa
4	Marabá	Ceará	P.O. Box 617, 9...	82	58472-897	Baixa
5	Belford Roxo	Pernambuco	Ap #353-7864 A...	157	88493-682	Baixa
8	Olinda	São Paulo	9940 Nisl Ave	262	98681-424	Baixa
13	Juazeiro do Norte	Rio de Janeiro	Ap #842-3976 A...	13	88485-558	Baixa
17	Blumenau	Bahia	3688 Leo, Street	31	58539-578	Baixa
18	Anápolis	Paraíba	4610 Phasellus ...	206	14957-438	Baixa
19	Maracanaú	São Paulo	4212 Massa. Rd.	51	15448-742	Baixa
29	Caucaia	São Paulo	Ap #189-8132 P...	3	52268-364	Baixa
32	Barra do Corda	Ceará	Ap #285-8622 ...	158	68566-158	Baixa
35	Itajaí	Bahia	Ap #266-4805 ...	142	74765-285	Baixa
43	Curitiba	Pernambuco	9320 Accumsan...	108	58517-554	Baixa
45	Águas Lindas d...	Minas Gerais	792-4720 Egest...	221	37517312	Baixa
46	Cametá	Minas Gerais	Ap #771-7502 D...	10	47294-716	Baixa
47	Petrópolis	Rio de Janeiro	265-5342 Sed A...	241	51288-743	Baixa
49	Ribeirão Preto	Paraná	3908 Ligula. Av...	6	66884-610	Baixa
50	Campina Grande	Paraná	397-6411 Tincid...	43	67404-062	Baixa
53	Petrópolis	Pará	P.O. Box 303, 5...	3	67263-225	Baixa

Fonte: Elaboração própria.

Perfil Diretoria – Acesso a informações de Nível 1 e 2, sem acesso a cadastros (Imagem 9).

Imagem 9 – Lista de informações Nível 1 e 2.



ID	cidade	regiao	endereco	numero	cep	classificacao
1	Cabo de Santo ...	Rio de Janeiro	284-7574 In Av.	104	31867654	Média
2	Paulista	São Paulo	P.O. Box 963, 1...	181	84337-207	Baixa
4	Marabá	Ceará	P.O. Box 617, 9...	82	58472-897	Baixa
5	Belford Roxo	Pernambuco	Ap #353-7864 A...	157	88493-682	Baixa
8	Olinda	São Paulo	9940 Nisl Ave	262	98681-424	Baixa
10	Mauá	Maranhão	741-2349 Eleme...	183	97448-316	Média
11	Goiânia	Pernambuco	Ap #301-8351 E...	88	65121-693	Média
12	Vitória da Conq...	Maranhão	762-8164 Socio...	94	66733-756	Média
13	Juazeiro do Norte	Rio de Janeiro	Ap #842-3976 A...	13	88485-558	Baixa
14	Joinville	Pará	551-5324 Ligula...	68	17570-883	Média
17	Blumenau	Bahia	3688 Leo, Street	31	58539-578	Baixa
18	Anápolis	Paraíba	4610 Phasellus ...	206	14957-438	Baixa
19	Maracanaú	São Paulo	4212 Massa. Rd.	51	15448-742	Baixa
23	Piracicaba	Santa Catarina	2891 Gravida Ave	190	55689-728	Média
24	Uberaba	Pará	302-3233 Eu, St.	79	20280-840	Média
25	Gravataí	Santa Catarina	P.O. Box 226, 4...	148	14361-335	Média
27	Piracicaba	Pará	425-993 Feugiat...	287	55666-498	Média
29	Caucaia	São Paulo	Ap #189-8132 P...	3	52268-364	Baixa

Fonte: Elaboração própria.

Perfil Ministro – Acesso a todas as informações e pode cadastrar novos usuários (Imagem 10).

Imagem 10 – Tela do perfil ministro.

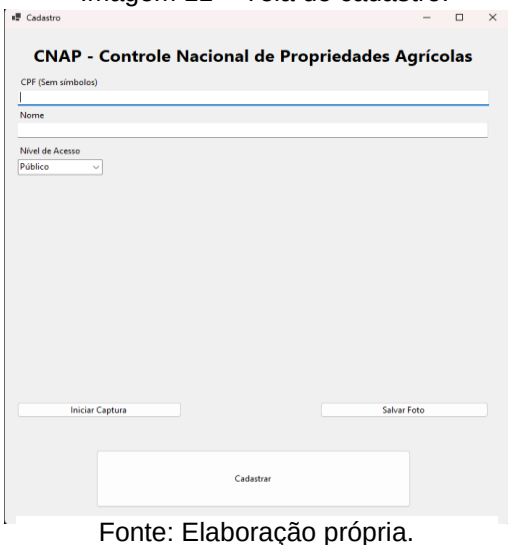
ID	cidade	regiao	endereco	numero	cep	classificacao
1	Cabo de Santo ...	Rio de Janeiro	284-7574 In Av.	104	31867654	Média
2	Paulista	São Paulo	P.O. Box 963, 1...	181	84337-207	Baixa
3	Divinópolis	Pará	138-4033 Imper...	287	44754-573	Alta
4	Marabá	Ceará	P.O. Box 617, 9...	82	58472-897	Baixa
5	Belford Roxo	Pernambuco	Ap #353-7864 A...	157	88493-682	Baixa
6	Valparaíso de G...	Pará	3873 Tristique R...	53	74775-027	Alta
7	Ponta Grossa	Ceará	9102 Erat St.	166	61266-881	Alta
8	Olinda	São Paulo	9940 Nisl Ave	262	98681-424	Baixa
9	Chapadinha	São Paulo	163-6852 Quisq...	279	96289-688	Alta
10	Mauá	Maranhão	741-2349 Eleme...	183	97448-316	Média
11	Goiânia	Pernambuco	Ap #301-8351 E...	88	65121-693	Média
12	Vitória da Conq...	Maranhão	762-8164 Socio...	94	66733-756	Média
13	Juazeiro do Norte	Rio de Janeiro	Ap #842-3976 A...	13	88485-558	Baixa
14	Joinville	Pará	551-5324 Ligula...	68	17570-883	Média
15	Maringá	Rio de Janeiro	Ap #704-3336 D...	53	67452-197	Alta
16	Balsas	Goiás	2928 Enim, St.	69	60358-128	Alta
17	Blumenau	Bahia	3688 Leo, Street	31	58539-578	Baixa
18	Anápolis	Paraíba	4610 Phasellus ...	206	14957-438	Baixa

Fonte: Elaboração própria.

Como podemos observar, somente o usuário com denominados como “Ministro” podem cadastrar um novo usuário, que é o último recurso que implementamos.

Na aba de cadastro, o ministro poderá efetuar o cadastro de um novo usuário (Imagem 11) através das informações CPF, Nome, Nível de Acesso e claro, uma foto para futuras autenticações (Imagem 12).

Imagem 11 – Tela de cadastro.



Fonte: Elaboração própria.

Imagem 12 – Fotografia.

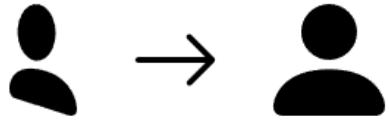
Fonte: Elaboração própria.

Após a captura da foto, a imagem é armazenada no diretório da aplicação com o CPF do usuário cadastrado, e o seu nome, CPF e nível de acesso são armazenados no banco de dados local.

Em relação ao reconhecimento facial, podemos dividi-lo em três etapas sequenciais e de suma importância para esta funcionalidade, onde cada uma desempenha uma determinada função. Sendo elas:

1) Detecção da Face – Responsabilidade de encontrar um rosto em uma imagem
2) Alinhamento da Face (Imagem13) – Responsabilidade de alinhar este rosto em uma outra imagem, para tentar minimizar o erro por conta de distorções e posicionamento.

Imagem 13 – Alinhamento de face.



Fonte: Face Recognition Library, 2024.

3) Reconhecimento – Responsável por de fato reconhecer um rosto, comparando duas imagens.

Alguns modelos realizam a inversão da ordem de aplicação dos passos 1 e 2. No nosso caso, esta ordem se mantém.

Este processo é implementado na biblioteca FaceAiSharp através dos seguintes passos:

1) Detecta se existe um rosto na imagem através de cinco pontos (Imagem 14), e o recorta
    a. Olhos (2)
    b. Nariz (1)
    c. Extremidades da boca (2)

    Formando uma imagem parecida com a que está abaixo:

Imagem 14 – Detectação por pontos.

Fonte: Face Recognition Library, 2024.

2) Realiza o alinhamento dos pontos detectados (Imagem 15):

Imagem 15 – Alinhamento dos pontos.

Fonte: Face Recognition Library, 2024.

3) Gera um vetor com dimensão de 512 dimensões com as distâncias específicas entre os pontos em relação à imagem.

    Exemplo de vetor gerado:

    -0,029764613 0,13904491 -0,017976629 0,010621089 0,015310788 -0,077746354
    0,026660273 -0,03839961 -0,06403088 0,023788495 -0,1461524 -0,010910285
    -0,001902924 -0,07354331 -0,06590692 0,09289711 0,0023482481 0,035271123

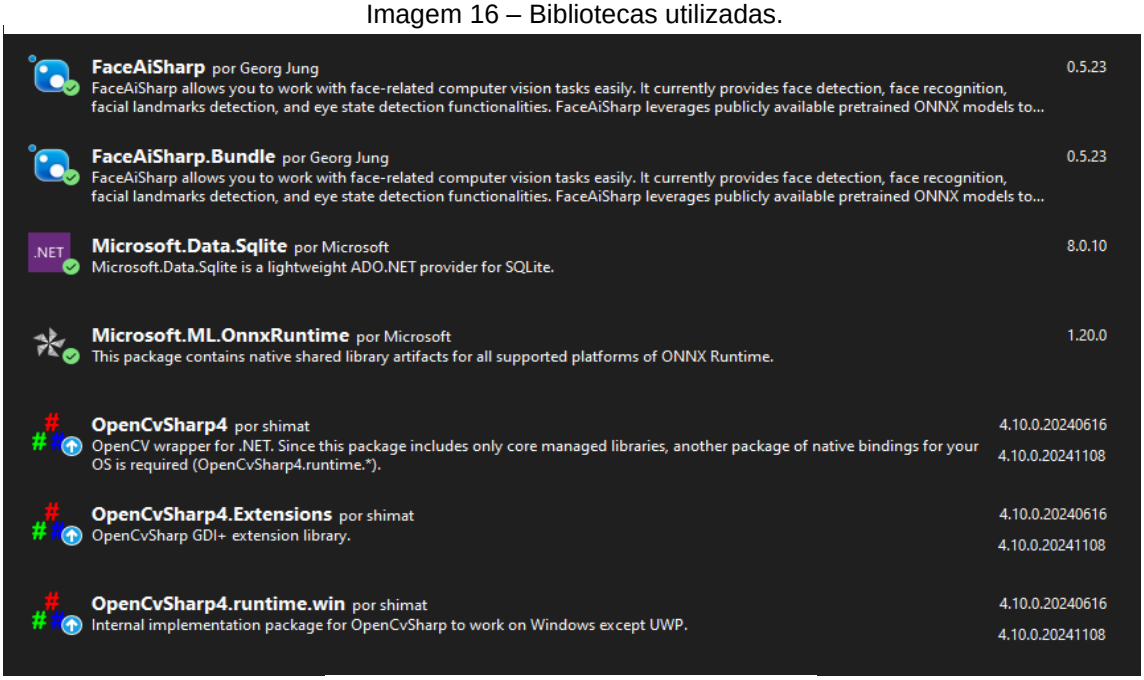
<... more numbers between -1 and 1 ...>

Para de fato realizar o reconhecimento, a biblioteca coleta o vetor armazenado e realiza uma operação denominada de Similaridade por Cosseno, uma medida de proximidade/similaridade que calcula a distância entre dois vetores normalizados. Esta medida fornece um valor no intervalo [-1, 1], mas, a biblioteca implementa esta medida somente com valores inteiros, tornando-se [0, 1].

Este valor é o que denominamos de “Previsão” anteriormente, onde quanto mais próximo de 1, mais chances de que as faces que foram comparadas pertencem, de fato, à mesma pessoa.

No Visual Studio, as bibliotecas são gerenciadas através dos NuGet Packages, que nada mais é que uma coletânea das mais diversas bibliotecas que podemos obter através da IDE. No nosso projeto, os pacotes (ou bibliotecas) utilizados, foram os seguintes:

Imagem 16 – Bibliotecas utilizadas.



Fonte: Elaboração própria.

- FaceAiSharp: A biblioteca principal que utilizamos para o reconhecimento facial.
- FaceAiSharp.Bundle: Contém funções adicionais para a biblioteca original.
- Microsoft.Data.Sqlite: Conector C# para o banco de dados SQLite

- Microsoft.ML.OnnxRuntime: Requisito para a biblioteca FaceAiSharp, onde ela utiliza de um dos modelos pré treinados de Machine Learning da ONNX – Open Neural Network Exchange.
- OpenCvSharp4 – Uma das bibliotecas mais famosas para visão computacional. Utilizamos ela para realizar a comunicação com a câmera do dispositivo.
- OpenCvSharp4.Extensions – Funções essenciais para a biblioteca base, facilitando o desenvolvimento.
- OpenCvSharp4.runtime.win – Requisito para a compatibilidade da biblioteca OpenCvSharp4 com o Windows.

As bibliotecas foram de suma importância para a realização do projeto, visto que são elas que proporcionam as principais funcionalidades para o programa.

Conforme mencionado anteriormente, utilizamos um banco de dados SQLite. As tabelas utilizadas, foram:

- tblInvestigacoes – Utilizada para armazenar dados de endereços fictícios
    - ID
    - Cidade
    - Regiao
    - Endereco
    - Numero
    - CEP
    - Classificacao
- tblUsuarios – Utilizado para armazenar as informações dos usuários
    - CPF
    - NivelAcesso
    - Nome

O banco de dados ficou armazenado no diretório da aplicação para maior comodidade no desenvolvimento, em: **database/CNPAdb.db.**

6.1. Resultados

Com a finalização da implementação, foi possível constatar que o grande número de tecnologias e recursos gratuitos disponíveis hoje em dia, viabiliza a grande maioria dos projetos dependendo de seu escopo e dimensionalidade.

Ao utilizar recursos gratuitos, fica explícito a viabilidade da utilização dessas tecnologias para projetos em baixa ou média escala, garantindo as suas funcionalidades principais com custos minimizados.

Nesta solução em particular, conseguiu-se implementar de forma satisfatória um sistema que cumpre o nosso objetivo principal – criar uma aplicação que utiliza como método de autenticação, características biométricas do usuário.

6.2. Considerações Finais

Embora tenhamos implementado com sucesso o nosso escopo, recomendamos que recursos mais escaláveis sejam utilizados para a implementação de futuras melhorias e novas funcionalidades, como:

- Mais acuracidade nos reconhecimentos
- Maior quantidade de informações
- Implementação de novas funcionalidades como:
    - Gerenciamento das Investigações
    - Armazenamento de outras características dos usuários
    - Criptografia das informações de login

O nosso protótipo pode ser considerado como uma implementação de uma primeira versão de um sistema que no futuro, pode acarretar em uma solução robusta com aplicações em outras áreas que lidam com informações confidenciais como um todo.

7. RELATÓRIO COM AS LINHAS DE CÓDIGO DO PROGRAMA

Quando trabalhamos com Windows Forms utilizando a IDE Visual Studio, as interfaces/janelas seguem a seguinte estrutura ao serem criadas:

Pagina.Designer.cs – Armazena os elementos de interface e layout da página, como controles e botões, juntamente com seus elementos de inicialização.

Pagina.cs – Implementa a parte lógica destinada à página.

Pagina.resx – Armazena recursos e dicionários de linguagem para facilitar na tradução de recursos e recursos.

Iremos detalhar os aspectos relacionados aos arquivos de lógica (terminados somente como .cs), visto que é onde se encontra as informações pertinentes ao nosso escopo.

Em termos de arquitetura, nosso programa possui a seguinte estrutura:

Classes Principais	Utilizadas para a implementação das ações que serão realizadas nas interfaces.	**Login.cs**	Classe que realiza as interações de login
		Informacao.cs	Responsável por mostrar as informações para o usuário.
		Cadastro.cs	Utilizada para cadastrar um novo usuário.
Classes Auxiliares	Responsáveis pela implementação de funções auxiliares, manipuladas pelas classes principais	**Reconhecimento.cs**	Utilizada para implementar toda a parte de reconhecimento facial
		AcessarBanco.cs	Utilizada para realizar a interface com o banco de dados e suas devidas manipulações.

7.1. Classes Principais

7.1.1. Login.cs

```
1. using MathNet.Numerics;
2.
3. namespace CNPA
4. {
5.     public partial class Login : Form
6.     {
7.         public Login()
8.         {
9.             InitializeComponent();
10.        }
11.
12.        // private static string projDir =
Directory.GetParent(Environment.CurrentDirectory).Parent.Parent.FullName;
13.        private static string projDir =
Path.GetDirectoryName(Application.ExecutablePath);
14.        private string imgDir = projDir + @"\resources\imagens\";
15.
16.        private string nivelAcesso, nome;
```

```
17.         private void btnIniciarCaptura_Click(object sender, EventArgs e)
18.         {
19.             AcessarBanco db = new AcessarBanco();
20.             string[] dados = db.GetUsuario(txtCPF.Text);
21.
22.             if (dados[0] != null)
23.             {
24.                 nome = dados[0];
25.                 nivelAcesso = dados[1];
26.                 Reconhecimento.IniciarCaptura(pictureBox1);
27.             }
28.         }
29.
30.         private void btnVerificar_Click(object sender, EventArgs e)
31.         {
32.             Reconhecimento.CapturarImagem("temp");
33.
34.             string path1 = @$"{imgDir}{txtCPF.Text}.jpg";
35.             string path2 = @$"{imgDir}\temp.jpg";
36.
37.             Reconhecimento re = new Reconhecimento(path1, path2);
38.             double dot = re.Comparar();
39.
40.             MessageBox.Show("Previsão: " + dot.Round(2), "Atenção",
MessageBoxButtons.OK, MessageBoxIcon.Information);
41.             if (dot >= 0.60)
42.             {
43.                 MessageBox.Show("Autenticação bem sucedida!", "Atenção",
MessageBoxButtons.OK, MessageBoxIcon.Information);
44.                 Informacoes proxForm = new Informacoes(nivelAcesso, nome);
45.                 proxForm.Show();
46.                 this.Close();
47.             }
48.             else if (dot > 0.28 && dot < 0.60)
49.             {
50.                 txtResultado.Text = "Por favor, tente novamente!";
51.             }
52.             else if (dot <= 0.28)
53.             {
54.                 txtResultado.Text = "Não é a mesma pessoa.";
55.             }
56.         }
57.     }
58. }
```

7.1.2. Informacao.cs

```
namespace CNPA
{
    public partial class Informacoes : Form
    {

        public Informacoes(string perfil, string nome)
        {
            InitializeComponent();

            txtPerfil.Text = perfil;
            txtNome.Text = nome;
            VerificaAcesso(perfil);

            AcessarBanco db = new AcessarBanco();
            dataGridView1.DataSource = db.GetInvestigacoes(perfil);
        }

        private void VerificaAcesso(string perfil)
        {
            string texto = "";
            switch (perfil)
            {
                case "Público":
                    texto = "Mostrando apenas informações públicas.";
                    break;
```

```
                case "Diretoria":
                    texto = "Mostrando informações de nível 1 e 2";
                    break;
                case "Ministro":
                    texto = "Mostrando todas as informações.";
                    btnCadastrar.Enabled = true;
                    break;
            }

            txtStatus.Text = texto;
        }

        private void btnCadastrar_Click(object sender, EventArgs e)
        {
            Cadastro novoForm = new Cadastro();
            novoForm.Show();
        }

        private void Informacoes_FormClosed(object sender, FormClosedEventArgs e)
        {
            Reconhecimento.FinalizarCaptura();
        }
    }
}
```

7.1.3. Cadastro.cs

```
namespace CNPA
{
    public partial class Cadastro : Form
    {
        public Cadastro()
        {
            InitializeComponent();
        }

        private void btnIniciarCaptura_Click(object sender, EventArgs e)
        {
            Reconhecimento.IniciarCaptura(pictureBox1);
        }

        private void Cadastro_FormClosed(object sender, FormClosedEventArgs e)
        {
            Reconhecimento.FinalizarCaptura();
        }

        private void btnCapturar_Click(object sender, EventArgs e)
        {
            Reconhecimento.CapturarImagem(txtCPF.Text);
            lblStatus.Text = "Foto salva com sucesso.";
        }

        private void btnCadastrar_Click(object sender, EventArgs e)
        {
            AcessarBanco db = new AcessarBanco();

            db.InserirUsuario(txtCPF.Text,txtNome.Text, comboAcesso.Text);

            MessageBox.Show("Usuário cadastrado com sucesso!","Aviso",
MessageBoxButtons.OK, MessageBoxIcon.Information);

        }
    }
}
```

7.2. Classes Auxiliares

7.2.1. Reconhecimento.cs

```
using OpenCvSharp;
```

```
using FaceAiSharp;
using SixLabors.ImageSharp;
using SixLabors.ImageSharp.PixelFormats;
using Image = SixLabors.ImageSharp.Image;

namespace CNPA
{
    public class Reconhecimento
    {
        private Image<Rgb24> img1, img2;
        private double ponto;
        private static VideoCapture capture;

        public Reconhecimento(string caminhoImg1, string caminhoImg2)
        {
            img1 = Image.Load<Rgb24>(caminhoImg1);
            img2 = Image.Load<Rgb24>(caminhoImg2);
            capture = new VideoCapture(0);
        }

        public static void IniciarCaptura(PictureBox pBox)
        {
            capture = new VideoCapture(0);
            Mat image = new Mat();

            while (true)
            {
                capture.Read(image);
                if (image.Empty()) return;
                pBox.Image = OpenCvSharp.Extensions.BitmapConverter.ToBitmap(image);
                int key = Cv2.WaitKey(30);
                if (key == 27) break;
            }
        }

        public static void FinalizarCaptura()
        {
            try
            {
                capture.Release();
            }
            catch (Exception)
            {
                Application.Exit();
            }
        }

        public static void CapturarImagem(string cpf)
        {

            //string projDir =
Directory.GetParent(Environment.CurrentDirectory).Parent.Parent.FullName;
            string projDir = Path.GetDirectoryName(Application.ExecutablePath);

            if (!capture.IsOpened())
                throw new Exception("Não foi possível acessar a câmera.");

            using var frame = new Mat();
            capture.Read(frame);
            if (frame.Empty())
                throw new Exception("Não foi possível capturar a imagem.");

            string caminhoImagem = projDir+@"\resources\imagens\"+cpf+".jpg";
            Cv2.ImWrite(caminhoImagem, frame);

        }
        public double Comparar()
        {
            // Detector de faces
            IFaceDetectorWithLandmarks det =
FaceAiSharpBundleFactory.CreateFaceDetectorWithLandmarks();
            // Reconhecedor de faces
```

```
            IFaceEmbeddingsGenerator rec =
FaceAiSharpBundleFactory.CreateFaceEmbeddingsGenerator();

            // Detectando faces
            var primeira = det.DetectFaces(img1).First();
            var segunda = det.DetectFaces(img2).First();

            // Alinhando as faces e realizando reconhecimento
            rec.AlignFaceUsingLandmarks(img1, primeira.Landmarks!);
            rec.AlignFaceUsingLandmarks(img2, segunda.Landmarks!);

            // Gerando as matrizes
            var embedding1 = rec.GenerateEmbedding(img1);
            var embedding2 = rec.GenerateEmbedding(img2);

            // Comparando faces e gerando uma acurácia
            var ponto = FaceAiSharp.Extensions.GeometryExtensions.Dot(embedding1,
embedding2);

            return ponto;
        }
    }
}
```

7.2.2. AcessarBanco.cs

```
using Microsoft.Data.Sqlite;
using OpenCvSharp;
using SQLitePCL;
using System.Data;
using static System.Runtime.InteropServices.JavaScript.JSType;
using static System.Windows.Forms.LinkLabel;
using System.Windows.Forms.Design.Behavior;
using System.Windows.Forms;

namespace CNPA
{
    public class AcessarBanco
    {
        //private static string projDir =
Directory.GetParent(Environment.CurrentDirectory).Parent.Parent.FullName;
        private static string projDir =
Path.GetDirectoryName(Application.ExecutablePath);
        private string dbDir = projDir+@"\database\CNPAdb.db";
        public DataTable GetInvestigacoes(string perfil)
        {
            string comando = "";

            switch (perfil)
            {
                case "Público":
                    comando = "SELECT * FROM tblInvestigacoes WHERE
classificacao='Baixa'";
                    break;
                case "Diretoria":
                    comando = "SELECT * FROM tblInvestigacoes WHERE
classificacao='Baixa' OR classificacao='Média'";
                    break;
                case "Ministro":
                    comando = "SELECT * FROM tblInvestigacoes";
                    break;

            }

            DataTable dataTable = new DataTable();

            using (var connection = new SqliteConnection($"Data Source={dbDir}"))
            {
                connection.Open();
                var command = connection.CreateCommand();
                command.CommandText = comando;

```

```
43.                 using (var reader = command.ExecuteReader())
44.                 {
45.                     dataTable.Load(reader);
46.                 }
47.             }
48.
49.             return dataTable;
50.         }
51.
52.         public void InserirUsuario(string cpf, string nome, string acesso)
53.         {
54.
55.             using (var connection = new SqliteConnection($"Data Source={dbDir}"))
56.             {
57.                 connection.Open();
58.                 var command = connection.CreateCommand();
59.                 command.CommandText = @"INSERT INTO tblUsuarios(CPF,Nome,NivelAcesso)
VAlUES($cpf,$nome,$acesso)";
60.
61.                 command.Parameters.AddWithValue("$cpf", cpf);
62.                 command.Parameters.AddWithValue("$nome", nome);
63.                 command.Parameters.AddWithValue("$acesso", acesso);
64.
65.                 try
66.                 {
67.                     command.ExecuteNonQuery();
68.                 }
69.                 catch (SqliteException ex)
70.                 {
71.                     MessageBox.Show("Usuário já existe!", "Erro",
MessageBoxButtons.OK, MessageBoxIcon.Error);
72.                     Application.Exit();
73.                 }
74.             }
75.
76.         }
77.
78.         public string[] GetUsuario(string cpf)
79.         {
80.             string comando = "SELECT Nome, NivelAcesso FROM tblUsuarios WHERE
cpf=$cpf";
81.             string[] resultado = new string[2];
82.
83.             using (var connection = new SqliteConnection($"Data Source={dbDir}"))
84.             {
85.                 connection.Open();
86.                 var command = connection.CreateCommand();
87.                 command.CommandText = comando;
88.                 command.Parameters.AddWithValue("$cpf", cpf);
89.
90.                 using (var reader = command.ExecuteReader())
91.                 {
92.                     if (reader.Read())
93.                     {
94.                         resultado[0] = reader.GetString(0);
95.                         resultado[1] = reader.GetString(1);
96.                     }
97.                     else
98.                     {
99.                         MessageBox.Show("Usuário não encontrado.", "Alerta",
MessageBoxButtons.OK, MessageBoxIcon.Warning);
100.                    }
101.                }
102.            }
103.
104.            return resultado;
105.        }
106.    }
107. }
108.
```

8. REFERÊNCIAS BIBLIOGRAFICAS

A BIOMETRIA e suas aplicações. Revista Brasileira de Ciências Policiais, Brasília, Brasil, v. 11, n. 2, p. 79–102, 2020. DOI: 10.31412/rbcp.v11i2.710. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/710. Acesso em: 12 nov. 2024.

LI, S. Z.; JAIN, A. K. *Handbook of Biometrics*. Springer, 2015. KALYANI, K. *Biometric Iris Recognition: Security and Privacy Concerns*. Elsevier, 2017.

MALTONI, D.; MAIO, D.; JAIN, A. K.; PRABHAKAR, S. *Handbook of Fingerprint Recognition*. Springer Science & Business Media, 2009.

TONHÁ, V. R. *Sistema de Autenticação de Compras Eletrônicas Utilizando Tecnologia Smart Card e Biometria Digital*. Brasília, DF, 2011.

FERREIRA, Autor. *Referência ao conceito de impressão digital com tinta*, 1999.

DUARTE, Autor. *Leitura de impressões digitais por dispositivos eletrônicos*, 2004. p. 3.

PANKATI, Autor. *Características invariáveis das impressões digitais e suas implicações biométricas*, 2000. p. 3.

TAVARES JUNIOR, Autor. *Registro de impressões digitais por contato direto e glândulas sudoríparas*, 1991. p. 30.

JACQUET, M.; CHAMPOD, C. Facial Recognition in Forensic Science: A Critical Overview. Academic Press, 2020.

SUMARES, S. Biometric Surveillance in Large-Scale Events: Case Study of the Champions League. *Journal of Security Studies*, 2018.

MITRA, P.; GOFMAN, M. Biometric Technologies for Securing Mobile Devices. *Journal of Computer Security*, 2016.

WIKIPÉDIA. Biometria. Disponível em: https://pt.wikipedia.org/wiki/Biometria. Acesso em: 12 nov. 2024.

WIKIPÉDIA. Similaridade por cosseno. Disponível em: https://pt.wikipedia.org/wiki/Similaridade_por_cosseno. Acesso em: 12 nov. 2024.

ONNX AI. Disponível em: https://onnx.ai/. Acesso em: 12 nov. 2024.

Face Recognition Library. Disponível em: https://facerec.gjung.com/. Acesso em: 12 nov. 2024.

GitHub. FaceAiSharp. Disponível em: https://github.com/georg-jung/FaceAiSharp. Acesso em: 12 nov. 2024.

NuGet. Disponível em: https://www.nuget.org/. Acesso em: 12 nov. 2024.
Microsoft C#. Disponível em: https://dotnet.microsoft.com/pt-br/languages/csharp. Acesso em: 12 nov. 2024.

Microsoft .NET Desktop Overview. Disponível em: https://learn.microsoft.com/pt-br/dotnet/desktop/winforms/overview/?view=netdesktop-8.0. Acesso em: 12 nov. 2024.

TechTarget. Biometric Authentication. Disponível em: https://www.techtarget.com/searchsecurity/definition/biometric-authentication. Acesso em: 12 nov. 2024.

ISA Global Cyber Alliance. 5 Benefits of Implementing Biometric Authentication in Cybersecurity. Disponível em: https://gca.isa.org/blog/5-benefits-of-implementing-biometric-authentication-in-cybersecurity. Acesso em: 12 nov. 2024.

Cloudflare. What is Authentication? Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/what-is-authentication/. Acesso em: 12 nov. 2024.

VEXELS. Impressão digital detalhada alinhada. Disponível em: https://br.vexels.com/png-svg/previsualizar/142169/impressao-digital-detalhada-alinhada. Acesso em: 12 nov. 2024.

DRAFT. O que é reconhecimento facial. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 12 nov. 2024.

CLEARSALE. Biometria comportamental: o que é e como funciona. Disponível em: https://blogbr.clear.sale/biometria-comportamental#:~:text=Trata%2Dse%20de%20uma%20tecnologia,em%20ambientes%20f%C3%ADsicos%20e%20digitais. Acesso em: 12 nov. 2024.

LEXISNEXIS RISK SOLUTIONS. What is behavioral biometrics. Disponível em: https://risk.lexisnexis.com.br/insights-resources/article/what-is-behavioral-biometrics. Acesso em: 12 nov. 2024.

ITFORUM. Biometria comportamental: como combater fraudes digitais. Disponível em: https://itforum.com.br/noticias/biometria-comportamental-fraudes-digital/. Acesso em: 12 nov. 2024.

FACEPHI. Biometria comportamental e a verificação de identidade. Disponível em: https://pt.facephi.com/blog/biometria-comportamental-verificacao-identidade/. Acesso em: 12 nov. 2024.

CISO ADVISOR. Biometria comportamental e a eficácia na prevenção a fraudes. Disponível em: https://www.cisoadvisor.com.br/security-room-posts/biometria-

comportamental-e-a-eficacia-na-prevencao-a-fraudes/. Acesso em: 12 nov. 2024.

ID R&D. Biometria de voz. Disponível em: https://www.idrnd.ai/pt-br/biometria-de-voz/. Acesso em: 12 nov. 2024.

REVISTA TI. Biometria de voz ajuda no combate ao uso malicioso da IA generativa. Disponível em: https://revistati.com.br/opiniao/biometria-de-voz-ajuda-no-combate-ao-uso-malicioso-da-ia-generativa#:~:text=A%20biometria%20de%20voz%20pode,falsos%20para%20acessar%20informa%C3%A7%C3%B5es%20sens%C3%ADveis. Acesso em: 12 nov. 2024.

MINDS DIGITAL. Biometria de voz: o que é? Disponível em: https://minds.digital/biometria-de-voz-o-que-e/#:~:text=O%20que%20%C3%A9%20biometria%20de%20voz?&text=e%20eficiente.,m%C3%ADnima%20fric%C3%A7%C3%A3o%20e%20m%C3%A1xima%20efici%C3%AAncia. Acesso em: 12 nov. 2024.

A5 SOLUTIONS. Fique por dentro das vantagens da biometria de voz. Disponível em: https://a5solutions.com/fique-por-dentro-das-vantagens-da-biometria-de-voz/#:~:text=A%20biometria%20de%20voz%20%C3%A9,Vamos%20explorar!. Acesso em: 12 nov. 2024.

MELO JUNIOR, Wilson. Autenticação de Sistemas Baseados em Biometria Comportamental. Disponível em: https://www.researchgate.net/profile/Wilson-Melo-Junior/publication/384374503_Autenticacao_de_Sistemas_Baseados_em_Biometria_Comportamental/links/6704324cf599e0392fc182a5/Autenticacao-de-Sistemas-Baseados-em-Biometria-Comportamental.pdf. Acesso em: 12 nov. 2024.

BOSON TREINAMENTOS. O que é biometria? Conceitos e tecnologias. Disponível em: https://www.bosontreinamentos.com.br/seguranca/o-que-e-biometria-conceitos-e-tecnologias/. Acesso em: 12 nov. 2024.

9. FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS

FICHA ATIVIDADES PRÁTICAS SUPERVISIONADAS – APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos individuais e em grupo, práticas de ensino e outros)

NOME: Diego Freire de Almeida

RA: N8059D-2 **CURSO:** Ciência da Computação

CAMPUS: Jundiaí **SEMESTRE:** 6º Semestre **TURNO:** Noturno

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ASSINATURA DO ALUNO**	**ASSINATURA DO PROFESSOR**
08/10/2024	Discussão inicial no Discord para definição sobre o tema do trabalho	5		
08/10/2024	Pesquisa sobre visão computacional	3		
10/10/2024	Pesquisa sobre visão computacional	5		
11/10/2024	Pesquisa sobre visão computacional	4		
11/10/2024	Reunião do grupo para a definição do projeto	4		
14/10/2024	Elaboração do conteúdo do trabalho escrito	8		
15/10/2024	Elaboração do conteúdo do trabalho escrito	8		
16/10/2024	Pesquisa sobre o método para reconhecimento facial	4		
16/10/2024	Desenvolvimento do Projeto	4		
17/10/2024	Desenvolvimento do Projeto	6		
18/10/2024	Desenvolvimento do Projeto	5		
18/10/2024	Desenvolvimento do Projeto	4		
19/10/2024	Reunião do grupo no Discord	2		
20/10/2024	Desenvolvimento do Projeto	5		
21/10/2024	Desenvolvimento do Projeto	5		
22/10/2024	Desenvolvimento do Projeto	3		
22/10/2024	Finalização e formatação do trabalho em norma ABNT	2		

TOTAL DE HORAS: 77 Horas

FICHA ATIVIDADES PRÁTICAS SUPERVISIONADAS – APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos individuais e em grupo, práticas de ensino e outros)

NOME: Kaiky de Lara Sales

RA: N9218H-8 **CURSO:** Ciência da Computação

CAMPUS: Jundiaí **SEMESTRE:** 6º Semestre **TURNO:** Noturno

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ASSINATURA DO ALUNO**	**ASSINATURA DO PROFESSOR**
08/10/2024	Discussão inicial no Discord para definição sobre o tema do trabalho	5		
08/10/2024	Pesquisa sobre visão computacional	3		
10/10/2024	Pesquisa sobre visão computacional	5		
11/10/2024	Pesquisa sobre visão computacional	4		
11/10/2024	Reunião do grupo para a definição do projeto	4		
14/10/2024	Elaboração do conteúdo do trabalho escrito	8		
15/10/2024	Elaboração do conteúdo do trabalho escrito	8		
16/10/2024	Pesquisa sobre o método para reconhecimento facial	4		
16/10/2024	Desenvolvimento do Projeto	4		
17/10/2024	Desenvolvimento do Projeto	6		
18/10/2024	Desenvolvimento do Projeto	5		
18/10/2024	Desenvolvimento do Projeto	4		
19/10/2024	Reunião do grupo no Discord	2		
20/10/2024	Desenvolvimento do Projeto	5		
21/10/2024	Desenvolvimento do Projeto	5		
22/10/2024	Desenvolvimento do Projeto	3		
22/10/2024	Finalização e formatação do trabalho em norma ABNT	2		

TOTAL DE HORAS: 77 Horas

FICHA ATIVIDADES PRÁTICAS SUPERVISIONADAS – APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos individuais e em grupo, práticas de ensino e outros)

NOME: Leonardo de Souza Rodrigues

RA: F344HB-2 **CURSO:** Ciência da Computação

CAMPUS: Jundiaí **SEMESTRE:** 6º Semestre **TURNO:** Noturno

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ASSINATURA DO ALUNO**	**ASSINATURA DO PROFESSOR**
08/10/2024	Discussão inicial no Discord para definição sobre o tema do trabalho	5		
08/10/2024	Pesquisa sobre visão computacional	3		
10/10/2024	Pesquisa sobre visão computacional	5		
11/10/2024	Pesquisa sobre visão computacional	4		
11/10/2024	Reunião do grupo para a definição do projeto	4		
14/10/2024	Elaboração do conteúdo do trabalho escrito	8		
15/10/2024	Elaboração do conteúdo do trabalho escrito	8		
16/10/2024	Pesquisa sobre o método para reconhecimento facial	4		
16/10/2024	Desenvolvimento do Projeto	4		
17/10/2024	Desenvolvimento do Projeto	6		
18/10/2024	Desenvolvimento do Projeto	5		
18/10/2024	Desenvolvimento do Projeto	4		
19/10/2024	Reunião do grupo no Discord	2		
20/10/2024	Desenvolvimento do Projeto	5		
21/10/2024	Desenvolvimento do Projeto	5		
22/10/2024	Desenvolvimento do Projeto	3		
22/10/2024	Finalização e formatação do trabalho em norma ABNT	2		

TOTAL DE HORAS: 77 Horas

FICHA ATIVIDADES PRÁTICAS SUPERVISIONADAS – APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos individuais e em grupo, práticas de ensino e outros)

NOME: Nicolas Pimenta da Silva

RA: N86357-9 **CURSO:** Ciência da Computação

CAMPUS: Jundiaí **SEMESTRE:** 6º Semestre **TURNO:** Noturno

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ASSINATURA DO ALUNO**	**ASSINATURA DO PROFESSOR**
08/10/2024	Discussão inicial no Discord para definição sobre o tema do trabalho	5		
08/10/2024	Pesquisa sobre visão computacional	3		
10/10/2024	Pesquisa sobre visão computacional	5		
11/10/2024	Pesquisa sobre visão computacional	4		
11/10/2024	Reunião do grupo para a definição do projeto	4		
14/10/2024	Elaboração do conteúdo do trabalho escrito	8		
15/10/2024	Elaboração do conteúdo do trabalho escrito	8		
16/10/2024	Pesquisa sobre o método para reconhecimento facial	4		
16/10/2024	Desenvolvimento do Projeto	4		
17/10/2024	Desenvolvimento do Projeto	6		
18/10/2024	Desenvolvimento do Projeto	5		
18/10/2024	Desenvolvimento do Projeto	4		
19/10/2024	Reunião do grupo no Discord	2		
20/10/2024	Desenvolvimento do Projeto	5		
21/10/2024	Desenvolvimento do Projeto	5		
22/10/2024	Desenvolvimento do Projeto	3		
22/10/2024	Finalização e formatação do trabalho em norma ABNT	2		

TOTAL DE HORAS: 77 Horas

FICHA ATIVIDADES PRÁTICAS SUPERVISIONADAS – APS

Atividades Práticas Supervisionadas (laboratórios, atividades em biblioteca, Iniciação Científica, trabalhos individuais e em grupo, práticas de ensino e outros)

NOME: Vitor dos Santos Rosa

RA: G521CE-3 **CURSO:** Ciência da Computação

CAMPUS: Jundiaí **SEMESTRE:** 6º Semestre **TURNO:** Noturno

			ASSINATURA	
DATA	**ATIVIDADE**	**TOTAL DE HORAS**	**ASSINATURA DO ALUNO**	**ASSINATURA DO PROFESSOR**
08/10/2024	Discussão inicial no Discord para definição sobre o tema do trabalho	5		
08/10/2024	Pesquisa sobre visão computacional	3		
10/10/2024	Pesquisa sobre visão computacional	5		
11/10/2024	Pesquisa sobre visão computacional	4		
11/10/2024	Reunião do grupo para a definição do projeto	4		
14/10/2024	Elaboração do conteúdo do trabalho escrito	8		
15/10/2024	Elaboração do conteúdo do trabalho escrito	8		
16/10/2024	Pesquisa sobre o método para reconhecimento facial	4		
16/10/2024	Desenvolvimento do Projeto	4		
17/10/2024	Desenvolvimento do Projeto	6		
18/10/2024	Desenvolvimento do Projeto	5		
18/10/2024	Desenvolvimento do Projeto	4		
19/10/2024	Reunião do grupo no Discord	2		
20/10/2024	Desenvolvimento do Projeto	5		
21/10/2024	Desenvolvimento do Projeto	5		
22/10/2024	Desenvolvimento do Projeto	3		
22/10/2024	Finalização e formatação do trabalho em norma ABNT	2		

TOTAL DE HORAS: 77 Horas