

**Curso de Ciência da Computação**

**Atividades Práticas Supervisionadas - APS**

**DESENVOLVIMENTO DE UM SISTEMA DE IDENTIFICAÇÃO E AUTENTICAÇÃO BIOMÉTRICA**

**Guilherme Augusto Sbizero Correa RA: F235289**

**Gabriel Macedo Ramos RA: F281060**

São Paulo

2022

**Resumo**

Biometria é o uso de características biológicas em mecanismos de identificação. Entre essas características tem-se a íris (parte colorida do olho), a retina (membrana interna do globo ocular), a impressão digital, a voz, o formato do rosto e a geometria da mão.

O uso de características biológicas para identificação se mostra como uma ideia viável porque cada pessoa possui as características mencionadas diferentes das outras.

Com a biometria, o problema de roubo de senhas ou cartões com chips é extinto ou, pelo menos amenizado. Embora nada impeça os dispositivos de identificação biométrica de serem enganados, é muito difícil copiar uma característica física e, dependendo do que é usado na identificação, a cópia é impossível (como a íris do olho).

O uso da biometria para identificação de pessoas já é realidade e é pouco provável que outro conceito a substitua.

É certo que a biometria vai ser cada vez mais parte do dia a dia das pessoas. Prova disso é que as tecnológicas envolvidas ganham aprimoramentos constantes.

Palavra-chave: biometria, identificação, reconhecimento facial, autenticação biométrica.

**SUMÁRIO**

1. **OBJETIVO 4**
2. **INTRODUÇÃO 5**
3. **FUNDAMENTOS DAS PRINCIPAIS TÉCNICAS BIOMÉTRICAS 7**
4. **PLANO DE DESENVOLVIMENTO DA APLICAÇÃO 15**
5. **PROJETO 19**
6. **RELATÓRIO COM LINHAS DE CÓDIGO DO PROGRAMA 24**
7. **APRESENTAÇÃO DO PROGRAMA FUNCIONANDO EM UM COMPUTADOR 54**
8. **BIBLIOGRAFIA 65**
9. **FICHAS DE ATIVIDADES PRÁTICA SUPERVISIONADAS 67**

**1 OBJETIVO**

Desenvolver, utilizando a linguagem de programação Java/Python, um programa de identificação e autenticação biométrica com interface gráfica, para restringir o acesso dos usuários a um determinado banco de dados. Esta restrição deve ser feita levando-se em consideração os níveis de permissão de acesso que os usuários têm em determinadas informações, que serão divididas em 3 níveis.

O banco de dados que deve ser protegido pertence ao Ministério do Meio Ambiente. Contendo informações sigilosas sobre propriedades rurais que fazem uso de agrotóxicos proibidos, causando grandes impactos ambientais.

São objetivos específicos desta atividade:

* Pesquisar e dissertar sobre os conceitos gerais da biometria;
* Definir o tipo de autenticação biométrica que será utilizada;
* Definir estrutura do sistema;
* Criar a interface gráfica;
* Implementar o projeto utilizando a linguagem de programação Java.

**2 INTRODUÇÃO**

Com a cada vez maior informatização da sociedade e a transferência de informações para o mundo digital, é de vital importância conseguir proteger estes dados. Os métodos tradicionais de proteção, que utilizam um nome de usuário e senha para impedir acessos não autorizados, tem demonstrado ser insuficiente nesta tarefa, pois sua segurança é muito baixa. O principal tópico de segurança para proteger serviços de rede ou alguma determinada área do sistema, é a autenticação e identificação dos usuários. Se esta etapa não conseguir impedir acessos indevidos, então dificilmente outro método de segurança implementado terá eficiência nesta tarefa. É neste cenário onde a biometria surge como um dos principais, mais eficazes, seguros e confiáveis métodos de identificação e autenticação indivíduos. Biometria (palavra derivada do grego bio, que significa vida, e metria, que significa medição) é a medição e a análise estatística das características físicas e comportamentais dos indivíduos. A premissa básica da autenticação biométrica é que todos são únicos e que um indivíduo pode ser identificado por suas características físicas ou traços comportamentais. A tecnologia tem sido usada fortemente como o principal meio de controle de acesso e/ou para identificação de indivíduos sob vigilância. O uso da impressão digital para assinar documentos foi pioneiro no conceito de biometria, sendo utilizada por diversos povos em diferentes épocas, desde os antigos babilônios, egípcios, assírios, japoneses e chineses. Eles utilizam a impressão digital para marcar seus produtos e lacrar documentos. A impressão digital ajudava a identificar bons e maus negociantes com os quais os mercadores já haviam realizado algum tipo de negócio. Os chineses costumavam com o uso de papel e tinta, marcar pés e mãos das crianças para diferenciá-las, podendo ser considerado um dos primeiros exemplos de uso da certidão de nascimento. Os avanços comerciais e de automatizações relacionadas à utilização da biometria tiveram início na década de setenta. Nesta época, surgiu um sistema conhecido como Identimat, esse sistema foi instalado em vários locais secretos para controle de acesso. Funcionava medindo a palma da mão e analisando o tamanho dos dedos. O Identimat teve sua produção encerrada na década de oitenta, mas seu pioneirismo foi importante na divulgação e aceitação da tecnologia biométrica 4 perante a população. Junto ao desenvolvimento da tecnologia baseada na mão, a biometria baseada em impressão digital começa a ganhar maior espaço. Durante esse período, algumas empresas estavam trabalhando com a identificação automática das impressões digitais para ajudar as forças policiais. A comparação das imagens das digitais armazenadas em registros criminais, era, até então, realizada manualmente o que demandava muito tempo e esforço. Outros métodos foram criados e os antigos continuaram a ser melhorados, enquanto a adoção dos baseados impressões digitais avançava. O primeiro sistema a analisar o padrão único da retina iniciou sua utilização na metade dos anos oitenta. No mesmo período na Universidade de Cambridge, foi desenvolvida a tecnologia baseada na íris. No Brasil em 2004 foi inaugurado a AFIS (Automated Fingerprint Identification System, ou, Sistema Automatizado de Identificação de Impressões Digitais), que foi interligado com o sistema de Informações Criminais (Sinic) criando o Sistema de Identificação Nacional (SIN). O SIN foi inaugurado com 800 mil impressões digitais de criminosos. Em 2007 o governo brasileiro iniciou a emissão do passaporte biométrico. Contendo diversos itens de segurança, o novo sistema de passaporte coleta assinatura, foto e dez impressões digitais roladas. Nos últimos anos está sendo implementada a utilização da biometria em eleições, com o intuito de aumentar a segurança do processo eleitoral, buscando evitar fraudes. Muitos países têm desenvolvido grandes inovações nesta área, tanto nos processos de expedição dos documentos eleitorais quanto nos procedimentos da própria votação em si. O maior exemplo são as urnas eletrônicos com autenticação biométrica.

**3 FUNDAMENTOS DAS PRINCIPAIS TÉCNICAS BIOMÉTRICAS**

A autenticação ou identificação de um determinado indivíduo pode ser feita de diversas formas, podemos classificá-las em três grandes grupos: por quilo que se possui, por aquilo que se sabe que é.

**Por que se sabe:** a autenticação é realizada utilizando algo que o usuário conhece. Exemplos são os nomes de acesso (nomes de usuário), senhas e chaves criptográficas. Em termos de segurança são os níveis mais baixos.

**Por aquilo que se possui:** estes métodos realizam a autenticação baseada em algo que o usuário possui. Geralmente são utilizados dispositivos que contêm memória ou capacidade de processamento. Os exemplos mais conhecidos são os Tokens, Smart Cards (cartões bancários, cartão de identidade pessoal, “chip” de celulares), cartões magnéticos e crachás. Estes métodos possuem nível de segurança média.

**Por aquilo que você é:** a autenticação é baseada naquilo que o usuário é. Ou seja, é nesta categoria que se encaixa a biometria. Podendo ser utilizada uma característica física ou uma característica comportamental única, que permita identificar e distinguir um indivíduo do outro. Exemplos de características biométricas são a impressão digital, a íris, a retina, a voz, a assinatura etc. São considerados os métodos que oferecem o mais alto nível de segurança. O emprego da biométrica em tecnologias de autenticação já faz parte do dia a dia da maior parte da população. Seu uso mais visível são os caixas eletrônicos dos bancos (que estão adotando este método) e as urnas eletrônicas utilizadas nas votações eleitorais. Também é utilizada como método de verificação de funcionários, validação de associados de planos de saúde, controle de acesso em locais de entrada restrita, segurança de redes, comércio eletrônico, acesso virtual, catraca eletrônica etc. A lista de usos somente tende a aumentar conforme a sociedade automatiza e informatiza seus processos. Um sistema de autenticação biométrica é dividido em duas fases: o registro do perfil do usuário e a sua autenticação. Na primeira fase é realizado o cadastramento da amostra biométrica dos usuários. Isto é feito utilizando-se um dispositivo que permita a captura destas características biométricas, como, por exemplo, leitor de digital, microfone, câmera de vídeo etc. 6 Após a captura, a amostra é transformada em um algoritmo matemático que será armazenado em um banco de dados. Toda vez que for preciso autenticar um usuário, será capturada uma nova amostra biométrica que será comparada com o modelo que está armazenado. Com relação aos métodos utilizados na identificação biométrica, eles podem ser divididos em dois grandes grupos: aqueles que utilizam características físicas e aqueles que utilizam características comportamentais.

**3.1 Características Físicas**

Utilizam a forma ou composição do corpo como identificador único dos indivíduos.

**3.2 Impressões Digitais**

Método automatizado utilizado para identificação ou confirmação de individuo baseado em uma comparação entre dois dedos. É o tipo mais conhecido e usado de biometria atualmente. As razões para sua popularidade são sua facilidade de aquisição, uso estabelecido, sua aceitação em comparação com os demais e o fato de que há dez fontes biométricas por indivíduo.

A impressão digital é formada por diversas linhas, criadas a partir das elevações da pele. Ela é única para cada indivíduo, mesmo irmãos gêmeos possuem impressões digitais diferentes. Sendo assim um dos métodos de identificação mais seguros existentes. Tendo sido descoberto e utilizado a mais de mil anos.

Esta característica individual sofre poucas alterações durante a vida de uma pessoa. Alguns fatores externos podem modificá-los, como por exemplo, o uso de produtos químicos ou trabalhos manuais que acabem danificando as linhas da impressão digital.

A identificação biométrica utilizando este, método, funciona através da extração dos pontos de minúcias da impressão digital. Após a extração estes valores são processados realizando-se diversos cálculos a partir dos quais os sistemas computacionais identificam o indivíduo dono da impressão digital.

Minúcias é o nome dado ao conjunto das características de uma impressão digital. Na figura 1 são mostrados exemplos de minúcias.

Figura 1 – Tipos de minúcias

Calendário

Descrição gerada automaticamente com confiança média

Fonte: GTA – Grupo de Teleinformática e Automação da UFRJ

Existem três padrões básicos da impressão digital: o arco, o laço e a espiral. Algumas imagens de impressões digitais que apresentam estes padrões podem ser vistas na Figura 2.

Foto em preto e branco

Descrição gerada automaticamente

Fonte: Biometric Solutions (adaptada pelos autores)

Um arco é um padrão onde a linha da digital entra em um dos lados do dedo, cresce ao chegar no meio formando um arco e sai pelo outro lado. No laço, mais famoso padrão de digital, a linha entra por um dos lados, forma uma curva e sai pelo mesmo local pelo qual entrou. Já a espiral é um padrão onde são formados círculos ao redor de um ponto central. Com relação aos dispositivos utilizados na coleta da impressão digital, eles são de três tipos: ótico, capacitivo e ultrassônico. O primeiro, e o mais utilizado, trabalha com uma fonte emissora de luz e utiliza a reflexão da luz sobre o dedo para realizar a leitura da digital. Os dispositivos capacitivos medem o calor emitido pela digital. E o último, o ultrassônico, como o próprio nome indica, envia sinais sonoros e coleta a impressão digital analisando o sinal retornado. Ou seja, funciona como um radar.

**3.1.2 Reconhecimento de íris**

Método automatizado utilizado para identificação ou confirmação de um indivíduo analisando padrões aleatórios da íris. O reconhecimento por íris é relativamente novo, sendo somente comercialmente desenvolvido na última década principalmente devido a limitações de patente.

A íris é um músculo dentro do olho que regula o tamanho da pupila, controlando a quantidade de luz que entra no olho. A íris é a parte colorida do olho e cada uma possui sua própria estrutura, o que permite sua utilização na identificação e autenticação de indivíduos.

Esta característica individual não se modifica com o passar dos anos, mantendo-se a mesma por toda a vida.

**3.1.3 Reconhecimento facial**

O reconhecimento fácil utiliza a geometria espacial de diferentes características da face (confira a Figura 3). Estas características não são modificadas, mesmo que se realize uma cirurgia plástica. Alguns exemplos de medidas são a distância entre os olhos; a distância entre os olhos, nariz e boca; e a distância entre as linhas dos cabelos, os olhos, a boca e o queixo.

Figura 3 – Reconhecimento facial

Uma imagem contendo parede de papel, relógio

Descrição gerada automaticamente

Fonte: Tutorials Point

Uma grande entre reconhecimento facial e os demais métodos é que o reconhecimento facial pode ser capturado à distância, como, por exemplo, por câmera se segurança, sendo possível sua aplicação sem o conhecimento do sujeito. Sendo adequado para encontrar crianças perdidas e procurar criminosos.

É um dos métodos menos intrusivos, pois não é necessário utilizar informações consideradas extremamente pessoais, como a impressão digital ou a composição da íris.

Outra vantagem é que se pode utilizar, em teoria, quaisquer câmeras digitais como dispositivo de captura da amostra biométrica. Bastando que se tenha um programa de identificação e autenticação biométrica que suporte aquela câmera.

**3.1.4 Geometria das veias**

Tal como as impressões digitais, o padrão das veias corporais é diferente entre os indivíduos, sendo um excelente critério para a identificação biométrica. O reconhecimento é confirmado a partir dos vasos sanguíneos que fiquem na superfície da pele. Geralmente a parte do corpo utilizada para este método são as mãos. Atualmente, os dois maiores exemplos de instituições que utilizam este método são o FBI e a CIA, ambas dos Estados Unidos da América.

**3.2 Características Comportamentais**

Utilizam o comportamento como identificador único dos indivíduos.

**3.2.1 Padrão de digitação**

Método utilizado para a identificação usando como critério os padrões de digitação do indivíduo. As medidas utilizadas por este critério são tempo de permanência (duração que uma tecla é pressionada) e o tempo de não-permanência (duração entre o soltar de uma tecla e o pressionar de outra).

Este padrão foi utilizado na segunda guerra mundial e ficou conhecido como The Fist of the Sender (O punho do remetente). Tendo sido utilizado pelas agências de inteligência militar para distinguir, baseado no ritmo de escrita, se um código morse teria sido enviado por um aliado ou inimigo de guerra.

Como atualmente, na maior parte das residências existe ao menos um teclado, este tipo de método biométrico é o mais fácil de ser implementado, se considerarmos a questão de aquisição do dispositivo de leitura biométrica.

**3.2.2 Reconhecimento de assinaturas**

Método de baixo nível que leva como critério a assinatura pessoal que cada pessoa opta por utilizar como meio de identificação pessoal. Costuma ser muito confundida com os autógrafos, sendo estes utilizados por artistas e pessoas públicas. Geralmente grandes artistas possuem uma assinatura, onde a mantém privada, e um autógrafo que é utilizado de forma pública.

Figura 4 – Primitivas de “início e fim abruptos”. Imagem original(a), imagem esqueletizada(b), pontos de início e fim do segmento no grid(c), pontos de início e fim na imagem original(d)

Gráfico

Descrição gerada automaticamenteFonte: GTA – Grupo de Teleinformática e Automação da UFRJ (adaptada pelos autores)

O reconhecimento de assinaturas é o método mais utilizado na comprovação de documentos, principalmente em Bancos e cartórios. Ele utiliza diversas características para realizar a análise a assinatura. Entre elas pode-se citar a velocidade, a pressão, a direção e o sentido da escrita. Na Figura 4 está exemplificado parte da análise automatizada de uma digital.

**3.2.3 Reconhecimento de voz**

Refere-se ao método automatizado para reconhecimento da identidade de um indivíduo baseado em sua voz. A sua principal desvantagem reside no fato de que nem todo ambiente pode implementar este método. Pois quanto maior a poluição sonora menor será a precisão do reconhecimento da voz. Outra desvantagem é que o estado se saúde do indivíduo, como gripe ou estresse, pode dificultar sua identificação.

A voz possui dois fatores biométricos, fisiológico e comportamental:

• O componente fisiológico da fala é a forma física da voz do sujeito.

• O componente comportamental trata-se do movimento da mandíbula, lábios, língua etc.

Existem dois tipos de reconhecimento de voz:

• Dependente de texto: O sujeito tem que pronunciar uma frase fixa (senha de acesso) que é a mesma tanto para o registro quanto para a verificação.

• Independente de texto: Baseado em qualquer palavra dita pelo sujeito.

O tipo dependente de texto tem uma melhor performance, porém o outro método é mais flexível, podendo ser utilizado até mesmo com indivíduos que não queiram cooperar, como é o caso criminosos.

**3.3 Classificação dos sistemas biométricos**

Os sistemas biométricos podem ser classificados e comparados através das características humanas que eles utilizam e em relação ao próprio conjunto de dispositivos e processos necessários para o seu funcionamento. A seguir estão algumas categorias de classificação.

**Universalidade:** Está relacionada ao fato de todas as pessoas serem dotadas da característica que será utilizada na identificação individual. Nem sempre a 12 característica será universal. A impressão digital, por exemplo, é uma das que mais pontuam neste quesito, pois o número de indivíduos que não possuem nenhum dedo na mão é irrisório. No sentido oposto, a biometria através da forma como uma pessoa anda, não é universal, pois a medição não pode ser realizada em portadores de deficiência física. Além de ser muito dependente do estado de saúde do indivíduo.

**Unicidade:** Mede o quanto a característica se diferencia entre duas pessoas. Deve-se buscar métodos onde a probabilidade de duas pessoas ter a mesma medida da característica seja extremamente baixa.

**Permanência:** Indica se a característica varia com o tempo. Por exemplo, mesmo com o envelhecimento, o DNA é uma medida que dificilmente sofre alterações. Já a voz, é mais suscetível de sofrer alterações durante a vida e por causa de doenças (o mais comum seria o resfriado).

**Coletabilidade:** Está relacionada as etapas do processo biométrico, indicando o quanto de tempo e esforço são necessários para sua execução. A autenticação biométrica baseada em DNA é extremamente demorada, o que é uma grande desvantagem deste método. Já a impressão digital pode ser rapidamente obtida, sem grande esforço.

**Performance:** É a medida do custo do dispositivo, do processamento e da quantidade de tempo utilizada para realizar a autenticação dos indivíduos.

**Precisão:** Com que exatidão o sistema biométrico consegue diferenciar os indivíduos.

**Aceitabilidade:** Refere-se ao quão bem o sistema biométrico foi aceito pelos seus usuários. Diversas características devem ser levadas em consideração para aumentar a aceitação, sendo as principais a privacidade e o conforto dos usuários.

**Proteção:** Define o nível de segurança do sistema. Ou seja, o quão difícil é enganar o processo de autenticação.

**4 PLANO DE DESENVOLVIMENTO**

Neste projeto será desenvolvido um sistema de identificação e autenticação biométrica através da impressão digital. Combinando a utilização de nome de usuário com a biometria através da impressão digital. Combinando a utilização do nome de usuário com a biometria, fazendo uma comparação 1:1 na autenticação.

Serão desenvolvidas interfaces gráficas para intermediar todos os processos que dependem da interação dos usuários. Simples e diretas focando nas funções principais da aplicação.

O sistema será formado por dois programas o Gerenciador de Usuários, que cadastrará os usuários e alterar seus dados, e uma aplicação cliente, Banco de Dados, que implementará a autenticação biométrica para restringir o acesso aos dados sigilosos do Ministério do Meio Ambiente.

Para atingir está finalidade será utilizado uma biblioteca chamada OpenCV desenvolvida pela Intel em 2000, ela é uma biblioteca multiplataforma totalmente livre para o uso acadêmico e comercial, para desenvolvimento de aplicativos para a área de Visão Computacional. Para ler as digitais será feita uma leitura da imagem dela, com isso restringindo o acesso ao banco de dados.

Para o Ministro do Meio Ambiente pode ser utilizado a imagem de sua digital ou a utilização de uma senha, aumentando a segurança das informações restritas. Garantindo que cada usuário possa acessar somente os recursos para quais tem autorização.

Diagrama

Descrição gerada automaticamente

Fonte: Elaborada pelos autores

O sistema biométrico trabalha com reconhecimento de padrões, adquirindo as informações biométricas (através da leitura da imagem), gerando um modelo (template) a partir destes dados e armazenando este modelo para posteriormente ser utilizado para comparação e verificação do usuário.

A autenticação dos usuários pode ser realizada de duas formas: 1:1 e 1:N. O primeiro método utiliza somente a impressão digital. Ele identifica o usuário comparando o modelo da impressão digital coletada com todos os modelos salvos no banco de dados. O que, dependendo da quantidade de usuários cadastrados, consumirá muitos recursos do sistema e demorará mais tempo para concluir a verificação.

O segundo método, 1:1, é o que será utilizado nesta aplicação. Ele realiza a verificação do usuário utilizando também um outro dado armazenado, que neste caso é o *nome de usuário*. Desta forma o modelo da impressão digital coletada será comparado somente com o modelo armazenado para o *nome de usuário* especificado. O que deixará a verificação mais rápida, principalmente quando se tem centenas de funcionários cadastrados, como é o caso Ministério do Meio Ambiente.

**4.1 Ambiente de Desenvolvimento**

O sistema será desenvolvido na linguagem de programação Java utilizando o paradigma de Orientação a Objetos. Como IDE (Intergrated Development Environment) foi utilizado o Apache NetBeans IDE versão 12.3 junto com a Java Plataform Standard Edition Development Kit na versão 15.0.2.

Para realizar o controle das versões do sistema foi empregue o GIT. Permitindo que todos os membros da equipe possam manipular os arquivos do projeto simultaneamente, sem que estas alterações sobrescrevam as de outro membro. Garantido maior produtividade, velocidade e segurança no desenvolvimento do projeto.

O GIMPfoi o editor de imagens utilizado na manipulação das figuras deste sistema. Ele é um programa multiplataforma, *open source* e contém as principais funcionalidades e características do Photoshop, além das suas próprias ferramentas. Um de seus diferenciais em relação ao programa da Adobe é ser gratuito.

**4.2 Interface Gráfica**

A interface gráfica será desenvolvida fazendo uso da biblioteca gráfica Swing. Todas as JRE, a partir da 1.2, trazem esta biblioteca como o padrão gráfico. Sua principal vantagem reside no fato de ser multiplataforma. Permitindo que as interfaces possam ser utilizadas em qualquer sistema operacional que suporte a JRE, apresentando os componentes da janela com os mesmos atributos (cores, tamanhos, margens, espaçamento, etc.), independente da plataforma em que está sendo executada.

**4.3 Leitor Biométrico**

Para a realização deste projeto a leitura biométrica será feita através de imagens adquiridas no google, onde serão cadastradas e será feita a leitura e comparação com as que existem no banco de dados.

**4.4 Computador e Sistema Operacional**

As configurações do Notebook utilizado neste projeto, tanto para o desenvolvimento do sistema quanto em seu teste, está na tabela abaixo

|  |  |
| --- | --- |
| **Notebook Lenovo Ideapad S145** |  |
| Processador | AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz |
| Memória RAM | 12,0 GB (utilizável: 9,88 GB) |
| HD | 1 tb |
| Monitor | 15.6 polegadas |
| Sistema Operancional | Windows 11 Home Single Language 64 bits |

Fonte: Elaborada pelos autores

**4.5 Banco de Dados**

Como o SDK utilizado no sistema somente permite a armazenamento dos *templates* no banco de dados proprietário da Neurotechnology, este será o utilizado.

Além dos *templates* será preciso armazenar os dados dos usuários, como seu nome, seu nome de usuário e seu nível de acesso. Isto será realizado através do salvamento do objeto do usuário em um arquivo. Este arquivo será armazenado em formato binário, utilizando a funcionalidade de Serialização disponibilizada pelo Java.

Desta forma o sistema terá dois bancos de dados, um contendo os *templates* e outro os dados dos usuários. Os dois serão arquivos e estarão armazenadas na pasta do sistema. Desta forma torna extremamente fácil mover a aplicação de um computador para outro, ou até mesmo, no futuro, centralizar o banco de dados em uma única máquina que terá conexão com várias aplicações de cadastro e validação de usuário.

**5 PROJETO DO PROGRAMA**

Os arquivos do sistema foram organizados em 4 diretórios: libs, src, facial e digitais APS. Como visto na figura 11

Diagrama

Descrição gerada automaticamente

Fonte: Elaborada pelos autores

O arquivo principal se chama Aps2022\_6SemestreApplication.java que está na pasta source dentro da pasta com, na pasta java, no diretório main e na pasta src. Assim que o abrir no Visual Studio Code click no botão run java para abrir o programa.

**5.1 Tela de Login**

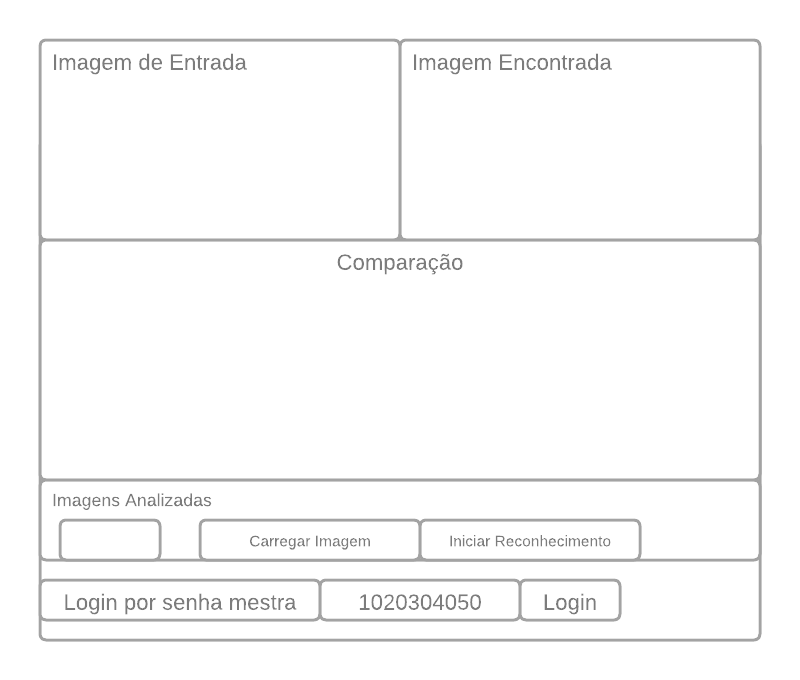
A janela de login é dividida em quatro partes, a primeira é onde ficará a imagem da digital que será utilizada para leitura, ao lado aparecerá a imagem encontrada no banco de dados.

Na segunda parte aparecerá a comparação das imagens, a que foi escolhida e a que foi encontrada.

Na terceira parte aparecerá o número de imagens pesquisadas, ao lado tem um botão chamado “Carregar Imagem” que irá abrir o menu do Explorador de Arquivos para selecionar a imagem da digital, ao lado também tem um botão chamado “Iniciar Reconhecimento” que após selecionar a imagem da digital click nele para iniciar o reconhecimento da digital.

Na quarta e última parte é onde localiza-se uma label para que quando digitada a senha de acesso que é “1020304050” e clicar no botão escrito “Login” entrará com acesso de nível 3 ao banco de dados do ministério do meio ambiente.

Confira na figura 12 abaixo

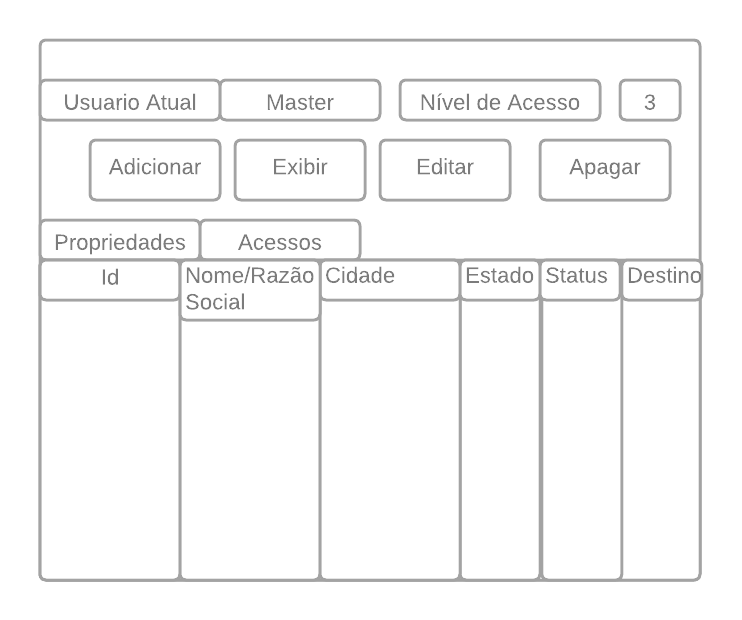


Fonte: Elaborada pelos autores

**5.2 Tela Acesso Banco de Dados**

Nesta janela a parte superior é dividida por duas labels, a primeira com o nome do atual usuário e a segunda label indicando o nível de acesso do usuário. Abaixo consiste por quatro botões “Adicionar” que ao clicar nele te encaminha para a janela de Cadastro de Agrotóxicos onde deverão ser preenchidos os dados do agrotóxico, se ele é permitido ou banido (não permitido por causam grandes impactos nos lenções freáticos, rios e mares) e então click no botão “Salvar” para salvar os dados no banco de dados. Veja na figura a seguir

Figura 13



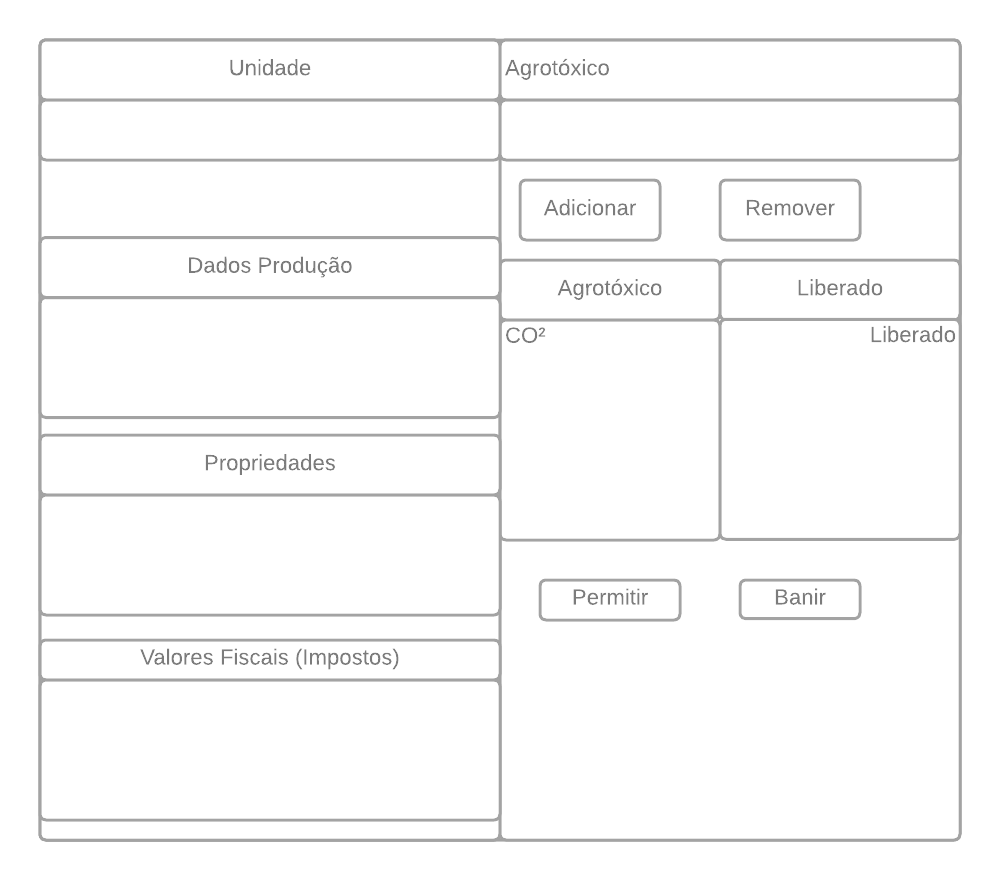
Fonte: Elaborada pelos autores

**5.3 Tela Cadastro Agrotóxico**

Clicando no botão “Exibir” após selecionar uma linha da tabela onde irá mostrar os dados da fornecedora dos agrotóxicos, o botão “Editar” os dados cadastrados e o botão “Apagar” após selecionar uma linha irá excluí-la.

Na parte central da janela aparecem dois botões “Propriedades” e “Acessos”, o primeiro é dividido por Id da empresa no sistema, Nome ou Razão Social dela, Cidade onde está localizada a sua sede, o Estado da sede, Destino é para onde os agrotóxicos da empresa serão vendidos, se será no mercado interno ou no mercado externo e por último o Status dos produtos cadastrados se são permitidos ou banidos. Confira a figura a seguir

Figura 14



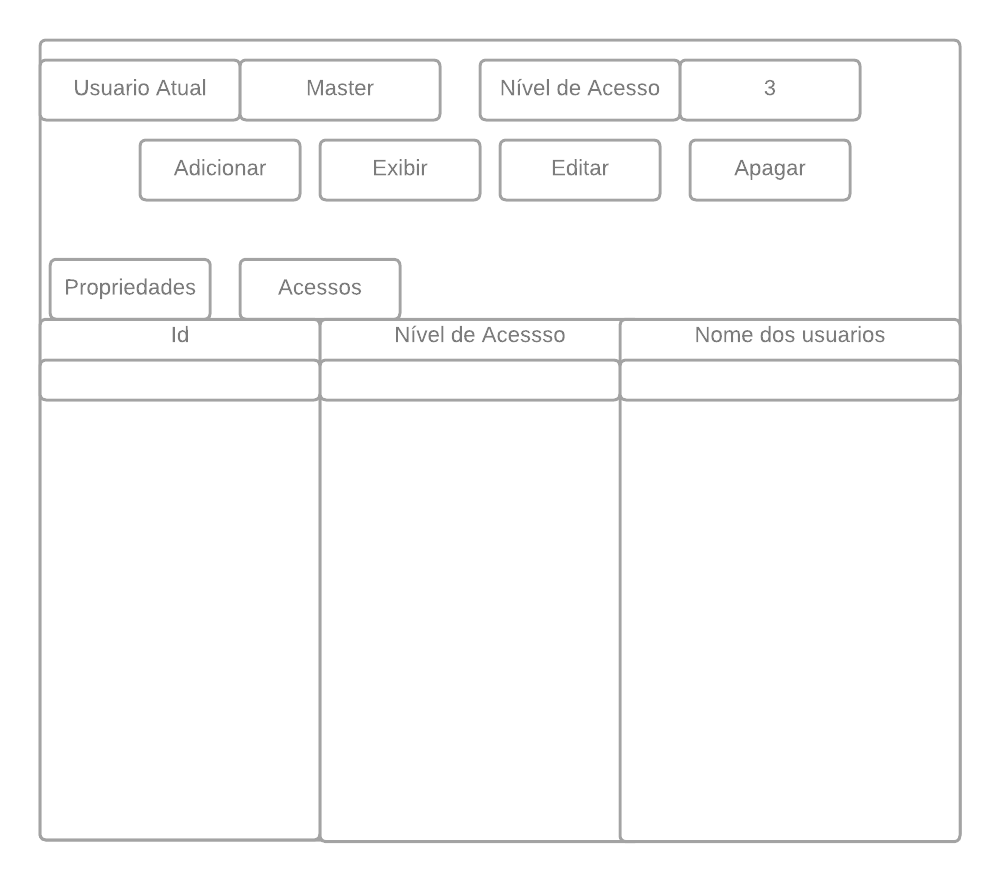
Fonte: Elaborada pelos autores

**5.4 Tela Cadastro Usuários**

Já na parte de Acessos ela é dividida por Id do Usuário, o Nível de Acesso dele ao sistema e seu Nome, em cima aparecem duas labels com o nome do atual usuário e seu nível de acesso, abaixo existem 4 botões com nomes de “Adicionar”, “Exibir”, “Editar” e “Apagar”.

O Adicionar de leva para uma janela de cadastro de digital junto de seu nome e nível de acesso, o botão Exibir te exibe as propriedades da digital como nome do usuário dela e nível de acesso, o botão Editar lhe permite modificar o nome de usuário, nível de acesso e mudar a imagem da digital cadastrada e por último o botão Apagar que exclui todos os dados do usuário.

Figura 15

Fonte: Elaborada pelos autores.

**6 Relatório com as linhas de código do programa**

**Classe APS2022\_6SemestreApplication (Main):**

Texto

Descrição gerada automaticamente

Fonte: Elaborada pelo autor.

A classe Main, é responsável por inicializar a aplicação.

**Classe Aplicação:**

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Em conjunto com a classe Main essas classes são responsáveis por carregar recursos e iniciar a aplicação. Esta classe contém Stage primaryStage e objetos para operações CRUD com banco de dados EntityManager e EntittyManagerFactory.

**Classe Alerts:**

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Classe para facilitar a exibição e retorno de informações, todos os métodos são estáticos e podem ser utilizados em qualquer classe, desde que o thread responsável por chamar estes métodos sejam threads de aplicação. Nessa classe, temos o tratamento das exceções, retornando os respectivos erros ao usuário no caso de falha.

**Classe Biometria:**

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Esta classe contém os métodos necessários para processar e comparar impressões digitais. Realiza a comparação entre duas imagens utilizando os seguintes algoritmos: Good features to track para obter pontos de interesse(keypoints). SIFT para detecção de descritores (descriptors) dos pontos de interesse e utiliza BruteForce como combinador para comparar os descritores das duas imagens, utilizar um método BruteForce não produz os resultados mais rápidos, mas de acordo com testes realizados foi obtido uma maior precisão nos testes.

**Classe ControllerBD:**

Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Fonte: Elaborada pelo autor.

Essa Classe é utilizada para operações CRUD genéricas, esta classe não é Thread safe e possui somente um EntityManager.

**Classe Utilitários:**

**Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteInterface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente**Fonte: Elaborada pelo autor.

Esta classe contém diversos metódos estáticos necessarios para detecção de rostos e outros metódos auxiliares. Nessa classe, podemos observar metódos responsávels por alocar um vetor de bytes e rescontruir a imagem a partir do vetor de bytes, temos metodo conversor de pixels para um objeto JavaFX Image e outros utilitários, como detectar qual o contorno com maior tamanho, detectar a posição do rosto na imagem e detectar o rosto com maior resolução.

**Classe Acessos:**

Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente

Fonte: Elaborada pelo autor.

Essa classe é um modelo para objeto Acesso que é utilizado para representar dados na TableView CRegistro e este modelo esta mapeado com a tabela do banco de dados. Obtém um array de bytes contendo todos os pixels contidos na imagem, para a imagem ser reconstruida é necessário armazenar a quantidade de linhas, colunas e tipo de imagem. A partir dessa informações reconstroi a imagem, realizando a liberação do acesso.

**Classe Agrotoxico:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Essa classe é um Modelo para o objeto Acesso que é utilizado para representar uma lista de agrotóxicos e este modelo esta mapeado com a tabela do banco de dados AGROTOXICO. É através dessa classe que os dados referentes aos agrotóxicos são armazenados na base de dados da aplicação.

**Classe Cadastro:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

A classe Cadastro é responsável por obter os dados referente ao formulário de preenchimento. Modelo para o objeto Acesso que é utilizado para representar dados na TableView CRegistro e este modelo esta mapeado com a tabela do banco de dados CADASTRO.

**Classe TableHelpers:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Classe auxilar na criação das tabelas CRegistro.tablePro e CRegistro.tableAce.

**Classe CAcesso:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Classe que é utilizada como controlador de listeners para interface GUI(Inteface Gráfica do Usuário).

**Classe CCadastro:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Classe que é utilizada como controlador de listeners para interface GUI Cadastro.fxml. Nessa classe são declarados todas as variaveis do formulario, bem como também, as propriedades do design da inteface do usuário.

**Classe CLogin:**

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamenteTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Classe que é utilizada como controlador de listeners para interface GUI Login.fxml.

**Classe CRegistro:** Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente Fonte: Elaborada pelo autor.

Classe que é utilizada como controlador de listeners para interface GUI Registro.fxml.

**Classe SplashScreen:**

Texto

Descrição gerada automaticamenteFonte: Elaborada pelo autor.

Essa classe é responsável pela interface que é exibida ao iniciar a aplicação enquanto está sendo carregado as informações necessárias para o funcionamento.

**7 Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras.**

**TELA DE LOGIN**

Figura 16

Uma imagem contendo Calendário

Descrição gerada automaticamente

Fonte: Elaborada pelo Autor

Essa seria a tela inicial da aplicação, nessa tela temos algumas possibilidades. Temos a possibilidade de fazer o login com o usuário master, utilizando-se uma senha pré-definida, realizando o acesso as informações de todos os usuários e dados cadastrados. Temos a possibilidade de carregar uma imagem biometria e iniciar o reconhecimento da biometria para definir os níveis de acesso aos dados.

Nessa imagem, temos um exemplo de acesso via biometria cadastrada. É possível visualizar os pontos de comparação da biometria e assim garantindo o acesso ao respetivo nível concedido aos dados armazenados.

**ACESSO AUTORIZADO UTILIZANDO DIGITAL**

Figura 17

**Interface gráfica do usuário

Descrição gerada automaticamente com confiança média**

Fonte: Elaborada pelo Autor

Nessa imagem, temos um exemplo de acesso via biometria cadastrada. É possível visualizar os pontos de comparação da biometria e assim garantindo o acesso ao respetivo nível concedido aos dados armazenados.

**INTERFACE DE PROPRIEDADES REGISTRADAS**

Figura 18

**Tabela

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

A imagem, é seguido pelo login efetuado anteriormente. Temos informações do usuário conectado e a disposição dos dados armazenados. Temos informações das empresas cadastradas e seus respectivos endereços comerciais. Sendo possível adicionar, alterar, exibir ou apagar os dados, dependendo do nível de permissão do usuário.

**INTERFACE DE CADASTRO NÍVEL 1**

Nos próximos prints, temos as telas onde é possível o cadastramento das informações. Temos diversos campos que devem ser preenchidos com as informações relevantes dos produtos que serão administrados pelo Ministério do Meio Ambiente.

Figura 19

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

**INTERFACE DE CADASTRO NÍVEL 2**

Figura 20

**Interface gráfica do usuário

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

**INTERFACE DE CADASTRO NÍVEL 3**

Figura 20

**Tela de computador com fundo branco

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

**Interface Cadastro Agrotóxico**

Figura 21**Interface gráfica do usuário

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

**DIGITAL NÃO CADASTRADA**

Figura 22

**Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

Segue um exemplo de erro, no caso de a biometria não estar cadastrada na base de dados**.**

**LOGIN ATRÁVES DE SENHA**

Figura 23

**Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

O usuário Master, tem todos os níveis de acesso e permissões dentro da aplicação. É um usuário administrador.

**INTERFACE DE CADASTRO DE ACESSO COM CADASTRO FACIAL**

Figura 24

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

Na aba “Acesso”, é onde podemos definir os níveis de acessos e as permissões que o usuário poderá utilizar dentro da aplicação. Seja na visualização dos dados cadastrados ou mesmo na alteração ou exclusão desses dados.

**TELA DE LOGIN COM RECONHECIMENTO FACIAL**

Figura 25

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

Fonte: Elaborada pelo Autor

Temos a possibilidade de realizar o reconhecimento facial e cadastrar a face para futuros acessos. Sendo possível visualizar a comparação entre as faces.

**8 BIBLIOGRAFIA**

AGÊNCIA BRASIL. **Polícia Federal inaugura amanhã moderno sistema de identificação digital**. Disponível em: [<h](http://memoria.ebc.com.br/agenciabrasil/)t[tp://memoria.ebc.com.br/agenciabrasil/](http://memoria.ebc.com.br/agenciabrasil/) noticia/2004-08-02/policia-federal-inaugura-amanha-moderno-sistema-de- identificacao-digital>. Acesso em: 20 nov. 2016.

ARAÚJO, Paulo Gabriel Ribacionka Góes de. **Sistema de controle de acesso via smart card com autenticação biométrica da impressão digital**. 2010. 105 f.

Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Centro Universitário de Brasília (UniCEUB), Brasília, 2010. Disponível em:

[<h](http://www.repositorio.uniceub.br/bitstream/123456789/3382/3/20516507.pdf)t[tp://www.repositorio.uniceub.br/bitstream/123456789/3382/3/20516507.pdf](http://www.repositorio.uniceub.br/bitstream/123456789/3382/3/20516507.pdf)>. Acesso em: 20 nov. 2016.

BIER, Carlos Eduardo. **Bioengine SDK: Identificação Biométrica 1:N**. Disponível em: <https://[www.profissionaisti.com.br/2011/06/bioengine-sdk-identificacao-](http://www.profissionaisti.com.br/2011/06/bioengine-sdk-identificacao-) biometrica-1n/>. Acesso em: 20 nov. 2016.

BIOMETRIC SOLUTIONS. **Face Recognition**. Disponível em:

[<h](http://www.biometric-solutions.com/face-recognition.html)t[tp://www.biometric-solutions.com/face-recognition.html](http://www.biometric-solutions.com/face-recognition.html)>. Acesso em: 20 nov. 2016.

BIOMETRIC SOLUTIONS. **Fingerprint Recognition**. Disponível em:

[<h](http://www.biometric-solutions.com/fingerprint-recognition.html)t[tp://www.biometric-solutions.com/fingerprint-recognition.html](http://www.biometric-solutions.com/fingerprint-recognition.html)>. Acesso em: 20 nov. 2016.

BIOMETRIC SOLUTIONS. **Iris Recognition**. Disponível em: <http://www.biometric- solutions.com/iris-recognition.html>. Acesso em: 20 nov. 2016.

BIOMETRIC SOLUTIONS. **Keystroke Dynamic**. Disponível em:

[<h](http://www.biometric-solutions.com/keystroke-dynamics.html)t[tp://www.biometric-solutions.com/keystroke-dynamics.html](http://www.biometric-solutions.com/keystroke-dynamics.html)>. Acesso em: 20 nov. 2016.

BIOMETRIC SOLUTIONS. **Speaker Recognition**. Disponível em:

[<h](http://www.biometric-solutions.com/speaker-recognition.html)t[tp://www.biometric-solutions.com/speaker-recognition.html](http://www.biometric-solutions.com/speaker-recognition.html)>. Acesso em: 20 nov. 2016.

BURSZTYN, Victor Soares. **Biométria: Análise de Assinaturas**. Disponível em:

[<h](http://www.gta.ufrj.br/grad/08_1/assinat/)t[tp://www.gta.ufrj.br/grad/08\_1/assinat/](http://www.gta.ufrj.br/grad/08_1/assinat/)>. Acesso em: 20 nov. 2016.

FARIA, Alessandro de Oliveira. **Biometria: Processamento de imagens capturadas em leitores de impressão digital**. Disponível em:

[<h](http://www.linhadecodigo.com.br/artigo/1162/biometria-processamento-de-imagens-)t[tp://www.linhadecodigo.com.br/artigo/1162/biometria-processamento-de-imagens-](http://www.linhadecodigo.com.br/artigo/1162/biometria-processamento-de-imagens-) capturadas-em-leitores-de-impressao-digital.aspx>. Acesso em: 20 nov. 2016.

GTA – UFRJ. **Biometria – Assinatura**. Disponível em:

[<h](http://www.gta.ufrj.br/grad/10_1/1a-versao/assinatura/historico.html)t[tp://www.gta.ufrj.br/grad/10\_1/1a-versao/assinatura/historico.html](http://www.gta.ufrj.br/grad/10_1/1a-versao/assinatura/historico.html)>. Acesso em: 20 nov. 2016.

GTA – UFRJ. **Impressão Digital: Constituição**. Disponível em:

[<h](http://www.gta.ufrj.br/grad/07_2/leonardo/Constituio.html)t[tp://www.gta.ufrj.br/grad/07\_2/leonardo/Constituio.html](http://www.gta.ufrj.br/grad/07_2/leonardo/Constituio.html)>. Acesso em: 20 nov. 2016.

NEUROTECHNOLOGY. **Free Fingerprint Verification SDK**. Disponível em:

[<h](http://www.neurotechnology.com/free-fingerprint-verification-sdk.html)t[tp://www.neurotechnology.com/free-fingerprint-verification-sdk.html](http://www.neurotechnology.com/free-fingerprint-verification-sdk.html)>. Acesso em: 20 nov. 2016.

ROUSE, Margaret. **Biometrics**. Disponível em:

[<h](http://searchsecurity.techtarget.com/definition/biometrics)t[tp://searchsecurity.techtarget.com/definition/biometrics>.](http://searchsecurity.techtarget.com/definition/biometrics) Acesso em: 20 nov. 2016.

TUTORIALS POINT. **Biometrics: Physiological Modalities**. Disponível em:

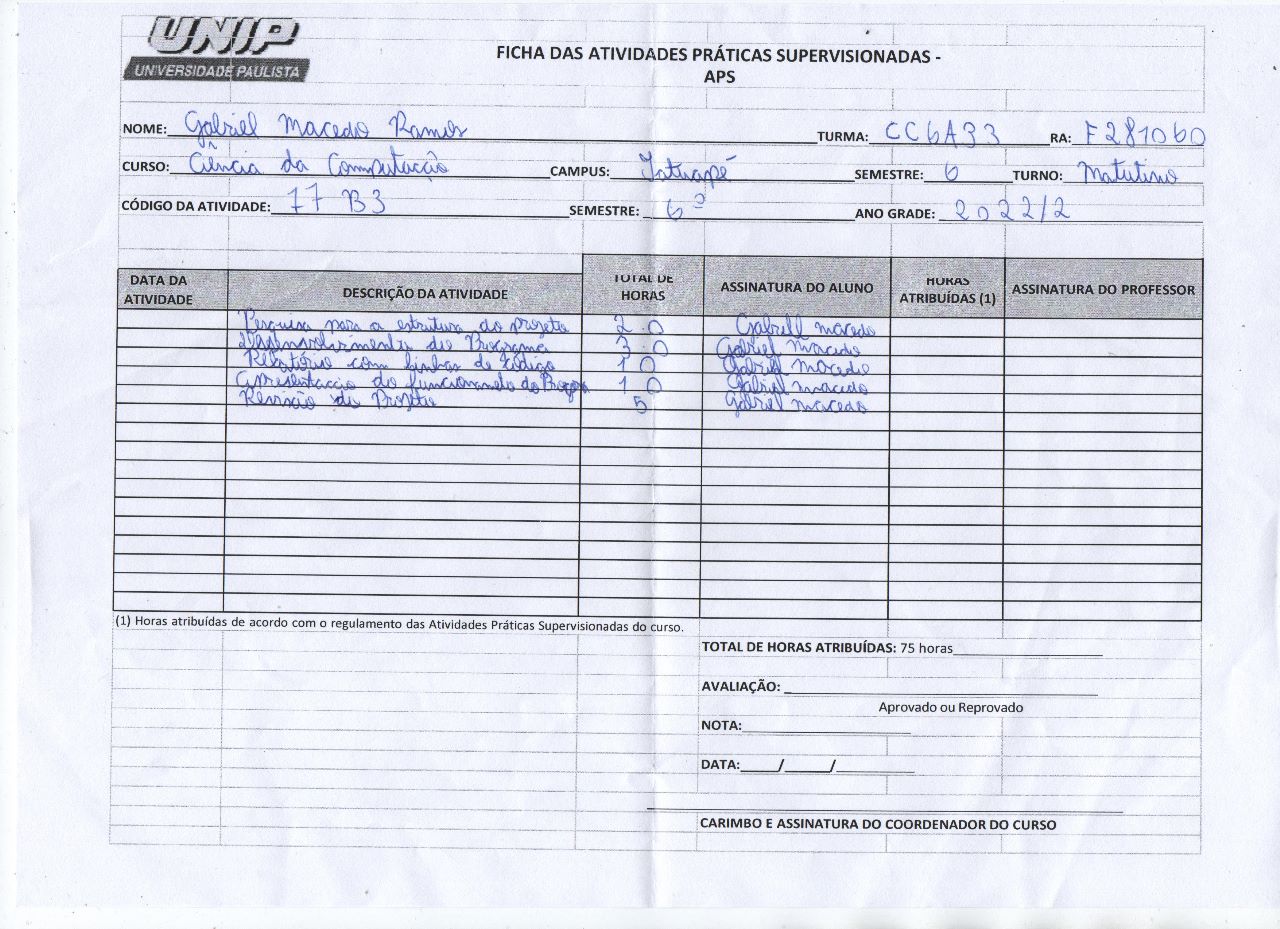
<https://[www.tutorialspoint.com/biometrics/physiological\_modalities.htm>.](http://www.tutorialspoint.com/biometrics/physiological_modalities.htm) Acesso em: 20 nov. 2016.

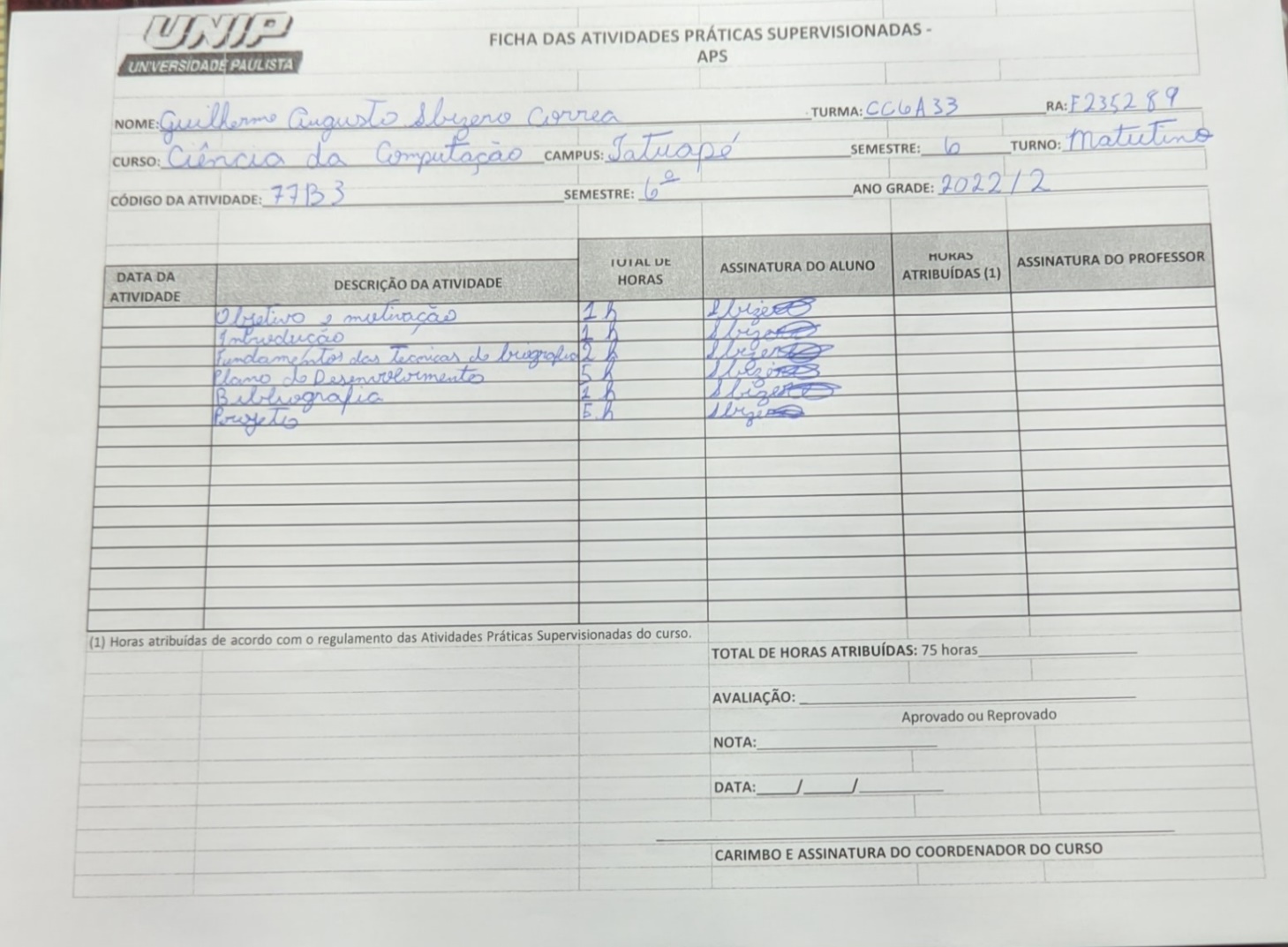
VIVA O LINUX. **Como funcionam os sistemas de biometria: um estudo geral**. Disponível em: <https://[www.vivaolinux.com.br/artigo/Como-funcionam-os-sistemas-](http://www.vivaolinux.com.br/artigo/Como-funcionam-os-sistemas-) de-biometria-um-estudo-geral>. Acesso em: 20 nov. 2016.

WILSON, Tracy V. **How Biometrics Works**. Disponível em:

[<h](http://science.howstuffworks.com/biometrics.htm)t[tp://science.howstuffworks.com/biometrics.htm>](http://science.howstuffworks.com/biometrics.htm). Acesso em: 20 nov. 2016.

1. **FICHAS DE ATIVIDADES PRÁTICA SUPERVISIONADAS**

****

****