



CIÊNCIA DA COMPUTAÇÃO

DESENVOLVIMENTO DE SISTEMA DE IDENTIFICAÇÃO E AUTENTICAÇÃO BIOMÉTRICA

Nome: Felipe de Sousa Gomes RA: N4750H0

Nome: Gabriel Bajona Sprovieri RA: F03BGE5

Nome: Heitor Augusto Oliveira Boracine RA: N441DC2

Turma: CC6A68

SÃO PAULO

2021

ÍNDICE

1. OBJETIVO DO TRABALHO.....	3
2. INTRODUÇÃO	4
3. FUNDAMENTOS DAS PRINCIPAIS TÉCNICAS BIOMÉTRICAS	6
3.1 Baixo nível de segurança.....	6
3.2 Médio nível de segurança	6
3.3 Alto nível de segurança:.....	7
3.4 Impressão Digital	7
3.5 Reconhecimento Facial.....	10
3.6 Reconhecimento de Íris e Retina	11
3.7 Reconhecimento de Voz	12
4 PLANO DE DESENVOLVIMENTO DA APLICAÇÃO.....	14
4.1 Pré-processamento de Imagem.....	18
4.2 Segmentação	18
4.3 Extração de Características	20
4.4 Classificação/Interpretação	20
5 PROJETO DO PROGRAMA.....	21
6 RELATÓRIO COM AS LINHAS DO CÓDIGO DO PROGRAMA	23
7 APRESENTAÇÃO DO PROGRAMA EM FUNCIONAMENTO	29
8 BIBLIOGRAFIA	34
9 FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS	35

1. OBJETIVO DO TRABALHO

Temos como objetivo neste trabalho mostrar uma técnica de segurança eletrônica muito utilizada hoje em dia, a biometria, que tem como principal utilidade o controle de acesso para indivíduos nos mais variados serviços a que essa tecnologia for empregada. Neste documento, mostraremos que nós desenvolvemos, utilizando a linguagem de programação Python, um sistema de “login” com identificação e autenticação biométrica com interface gráfica, cuja função será proteger uma rede, restringindo o acesso a um banco de dados do Ministério do Meio Ambiente e as informações nele contidas, referentes às propriedades rurais que utilizam agrotóxicos proibidos, por causarem grandes impactos nos lençóis freáticos, rios e mares, visando colocar em prática o aprendizado sobre os conteúdos abordados nas aulas de Processamento de Imagem e Visão Computacional. A categoria de acesso será dividida em 3 níveis, considerando as permissões de acesso de quem utilizará o serviço, sendo que quanto maior o nível de permissão do agente, mais informações consideradas sigilosas ele terá acesso. Para isto, criamos uma simulação de como é feita a autenticação biométrica.

2. INTRODUÇÃO

A biometria, de maneira simples, é o estudo estatístico das características físicas e comportamentais dos seres vivos, e como é possível diferenciar cada indivíduo através de características únicas de cada um. Sendo usada de maneira natural durante a antiguidade, como nos casos em que, tanto na pré-história em que mãos eram marcadas ao lado de pinturas nas paredes de cavernas como meio de deixarem suas assinaturas, quanto em artistas da Babilônia e China que deixavam suas impressões digitais em seus vasos, com o mesmo propósito. Outra maneira onde a biometria é usada, seria no fato de nós nos distinguirmos através do reconhecimento por meio dos nossos rostos e vozes.

Com o passar do tempo, isso que era algo natural ou até um mero capricho, passou a ser algo necessário para nós. Sendo usada de maneira mais efetiva, a biometria teve importantes papéis no desenvolvimento humano. Com um maior amadurecimento do poder judiciário no mundo, que levou a códigos judiciais que conferiam uma maior punição a infratores reincidentes e a melhora nos meios de transportes, que possibilitaram infratores se locomoverem para longe dos lugares onde haviam cometido crimes, bancos de dados formais deveriam ser criados para que esses criminosos fossem mais facilmente reconhecidos, através de características distintas deles.

No século XIX, Alphonse Bertillon, criminologista francês como auxílio para o meio judiciário, registrou as partes dos corpos de criminosos presos em fotografias e as guardavam em bancos de dados para uso futuro. Diferentemente de hoje, onde os dados obtidos através das diversas práticas de biometria são analisados por computadores e comparados com o banco de dados a qual estão associados, de maneira rápida, segura e precisa, as informações obtidas naquela época eram analisados por pessoas, de maneira semelhante ao reconhecimento facial usado atualmente, porém, esse método demorava muito tempo até uma conclusão ser alcançada e podendo acontecer erro de julgamento devido a um erro humano cometido por esses analisadores.

A partir de 1900, nos Estados Unidos, o processo de coleta de biometria se tornou algo metódico, visando criar uma base de dados para facilitar a identificação de criminosos. Com o passar das décadas o Federal Bureau of Investigation, (FBI) que foi criado pelo Congresso Nacional fez uso desse banco de dados adotando-o

para identificação de prisioneiros e foragidos. Em 1946, o FBI já possuía mais de 100 milhões de impressões digitais, que diferentemente de hoje, em que são registradas de maneira automatizadas através de sensores que além de acabar com os custos operacionais, são mais precisos e economizam tempo, eram, no começo, adquiridas por cartões de identificação. Igual à tecnologia que evoluiu, os bancos de dados também evoluíram, se unificando em um agregado no que é conhecido como o Sistema Integrado de Identificação Automatizada de Impressão Digital (IAFIS sigla em inglês).

Como vimos, a biometria tal qual como conhecemos hoje só foi ser desenvolvida quando foi necessário que criássemos maneiras mais eficazes e seguras de nos diferenciarmos uns dos outros, demonstrando características únicas, que dificilmente poderiam ser copiadas, fazendo assim, com que essas técnicas passassem a se integrar no cotidiano das pessoas. Sendo usada tanto em reconhecimento e identificação criminal, como já citado, a biometria também permite o controle de acesso a dados, lugares e dispositivos entre outras coisas, que sem o uso dela, teriam o processo de checagem de credenciais enganado por pessoas que, por exemplo, aprenderiam a imitar a assinatura de alguém. Considerando as características distintas entre as pessoas, os diferentes tipos de biometrias estão auxiliando na segurança tanto de instituições governamentais como para empresas privadas que não querem que seus segredos, dados e até informações de seus clientes sejam acessadas por pessoas mal-intencionadas.

3. FUNDAMENTOS DAS PRINCIPAIS TÉCNICAS BIOMÉTRICAS

Existem diversas maneiras de se checar a autenticidade de um determinado indivíduo, podemos então recorrer a processos que garantam maior segurança para nossas informações, tendo em vista o custo-benefício. Quanto mais segura é essa verificação, tende a ser mais cara, tanto para implementação, quanto para operação delas. Falaremos então sobre essas diversas técnicas.

3.1 Baixo nível de segurança

Começando pelas técnicas de baixo nível de segurança, temos aquelas utilizadas por redes sociais, sistemas de “login” simples encontrados em aplicativos e programas, tanto de computadores quanto celulares, que não requerem que tantos gastos com segurança sejam feitos, já que suas informações não são tão sigilosas. Exemplos dessas técnicas são: criação de “login” através de nome, senha, correio eletrônico, além também de Chaves de Seguranças, geradas automaticamente como substitutos para seu nome e senha. Tendo o usuário decorado essas informações, seus futuros “logins” serão feitos sem maiores problemas. O problema dessas técnicas é que são facilmente burladas, se quaisquer pessoas souberem dessas informações, tanto através de vazamento de informações quanto por simplesmente ouvirem esses dados, a entrada dessas pessoas a sua conta será algo fácil.

Uma maneira de quem se utiliza dessas técnicas achou para aumentar a segurança dela, foi a implementação de uma verificação em duas etapas, ou chamada autenticação por dois fatores. Essa segurança a mais ajuda a garantir que, embora seus dados sejam descobertos, permitindo o acesso de terceiros a sua conta, uma nova camada de proteção impedirá que eles consigam avançar mais. Essa verificação funciona tanto por mensagem de texto em SMS e correio eletrônico, quanto por chamada telefônica.

3.2 Médio nível de segurança

Aumentando a segurança temos métodos que se tornam mais difíceis de serem burlados, já que para alguém conseguir suas credenciais de acesso necessitariam de

algo que está em sua posse, na sua casa, longe das mãos deles. Com um gasto maior, são comumente usadas por empresas e órgãos governamentais, onde as informações e acessos que querem restringir são de mais importância. Como exemplos de técnicas temos: Tokens e os Cartões de Acesso (Crachás). Os Tokens, algo como um pendrive que possui códigos criptografados, cuja função é permitir o acesso de seu portador a sistemas compatíveis com ele. Os cartões de acesso funcionam da mesma maneira, porém possuem circuitos integrados com os códigos. Por mais que o uso desse método seja mais seguro do que o método anterior, sua insegurança está no fato de que caso esse objeto seja adquirido por outros, eles terão o mesmo acesso que o dono legítimo.

3.3 Alto nível de segurança:

Chegando nessa categoria a segurança que temos é muito maior, pois são implementadas técnicas que utilizam de nossas características únicas, tanto físicas quanto comportamentais para nos diferenciar de outras pessoas. Ela possui o maior gasto entre as técnicas citadas e é também empregada por empresas e órgãos governamentais, porém, dessa vez para protegerem informações e acessos de mais alto valor, onde caso sejam obtidas por terceiros, seriam muito prejudiciais para as empresas. Como foco deste capítulo, iremos nos aprofundar nos fundamentos das principais técnicas biométricas, mais especificamente as de alto nível, já que é uma técnica usada em uma autenticação biométrica.

Alguns exemplos dessa categoria são: impressão digital, reconhecimento facial, reconhecimento de íris e retina, e reconhecimento de voz.

3.4 Impressão Digital

A biometria por impressão digital é uma das mais populares biometrias hoje em dia, isso se dá devido ao uso dela em “smartphones” como principal forma de bloqueio, para realizar operações em caixas eletrônicos, ou até mesmo no nosso sistema eleitoral, nas urnas eletrônicas.

Além de garantir segurança e agilidade na identificação de um indivíduo, ela é uma técnica de baixo custo se comparada às outras. Outro fator a se destacar é que

ela não é um método intrusivo, visto que só é necessário colocar o dedo em um sensor para que sua impressão digital seja lida e identificada.

Os dispositivos usados para a coleta de impressões digitais podem ser: ópticos, ultrassônicos ou capacitivos. O sensor óptico emite uma luz que ao refletir em seu dedo, “enxerga”, as características das suas digitais. Os sensores capacitivos medem a energia elétrica emitida por seu dedo para pegar as informações de digitais. Por fim, os sensores ultrassônicos enviam sinais sonoros, em ondas, para coletar a impressão digital, o mais caro, já que pode captar além da pele, coletando assim, muito mais informação e podendo até saber como, por exemplo, se é um dedo de alguém que está vivo.

As impressões digitais são formadas por elevações na pele, as papilas dérmicas, com padrões únicos, possuindo assim unicidade. Elas se mantêm praticamente intactas durante toda a vida de um indivíduo, porém, devido a machucados ou ao uso de produtos químicos fortes, as impressões podem ser modificadas, alterando o padrão único de uma pessoa, para outro, ou até nenhum padrão, ou seja, sem impressão digital. Caso alguém nasça com a Síndrome de Nagali, decorrente do mau funcionamento da proteína queratina 14, as pontas de seus dedos serão lisas, sem qualquer impressão digital.

Para a identificação de uma impressão digital deve-se analisar diversos fatores, que dividem as impressões em 4 tipos idealizados por Juan Vucetich, eles são: O Arco, A Presilha Interna, a Presilha Externa e o Verticilo.



Figura 1 – Tipos de Impressão



Presilha Interna I2

Figura 2 – Tipos de Impressão



Figura 3 – Tipos de Impressão



Figura 4 – Tipos de Impressão

O Arco, geralmente não possuindo um delta, figura em formato de triângulo presente no encontro das papilas, possui as linhas atravessando o campo digital, em formato de um arco, indo de um lado para o outro, com trajetórias paralelas e arredondadas.

A Presilha Interna possui um delta à direita e suas linhas partem da esquerda, curvando-se indo em direção à esquerda novamente, formando um laço. A presilha Externa é semelhante à Interna, mudando o delta para a esquerda e tendo o laço saindo da direita e voltando para a origem, também em formato de laço.

O Verticilo possui tanto um delta à esquerda, quanto a direita, com pelo menos uma linha livre e curva na frente de cada um. Seu padrão é em formato de espiral, onde diversos círculos rodeiam um ponto central.

Outro ponto a se observar em relação às impressões, são os chamados Pontos Característicos, imperfeições presentes nas cristas papilares, o ponto mais alto das papilas, em contraponto com os sulcos interpapilares, os mais baixos. Essas características que conseguem de fato nos diferenciar, nos dando impressões únicas. Os tipos são:




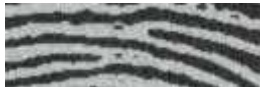

Ponto	Ilha	Cortada	Extremidade de linha	Bifurcação
				

Figura 5 – Tipos de Pontos Característicos

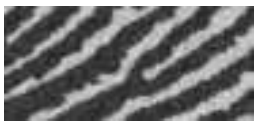

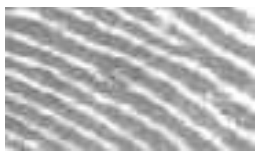

Confluência	Arpão	Ponte	Lago
			

Figura 6 – Tipos de Pontos Característicos

Um fato importante com relação à biometria por impressão digital no Brasil, é que para atestar a identidade de alguém, a legislação brasileira exige que se tenha pelo menos 12 Pontos Característicos, na mesma localização, sendo eles do mesmo tipo e sem a existência de nenhum ponto discrepante.

3.5 Reconhecimento Facial

O reconhecimento facial funciona mapeando padrões no rosto de uma pessoa, padrões esses que não mudam, como determinadas distâncias entre as partes que compõem uma face e seus respectivos tamanhos, tais como olhos, narizes, sobrancelhas, bocas e até a divisória entre a testa e o começo do cabelo.

Para capturar o rosto de alguém é utilizada uma câmera, que irá registrar esse rosto, em seguida um “software” especializado irá marcar os padrões e mandará para um banco de dados para serem reconhecidos através de cálculos.

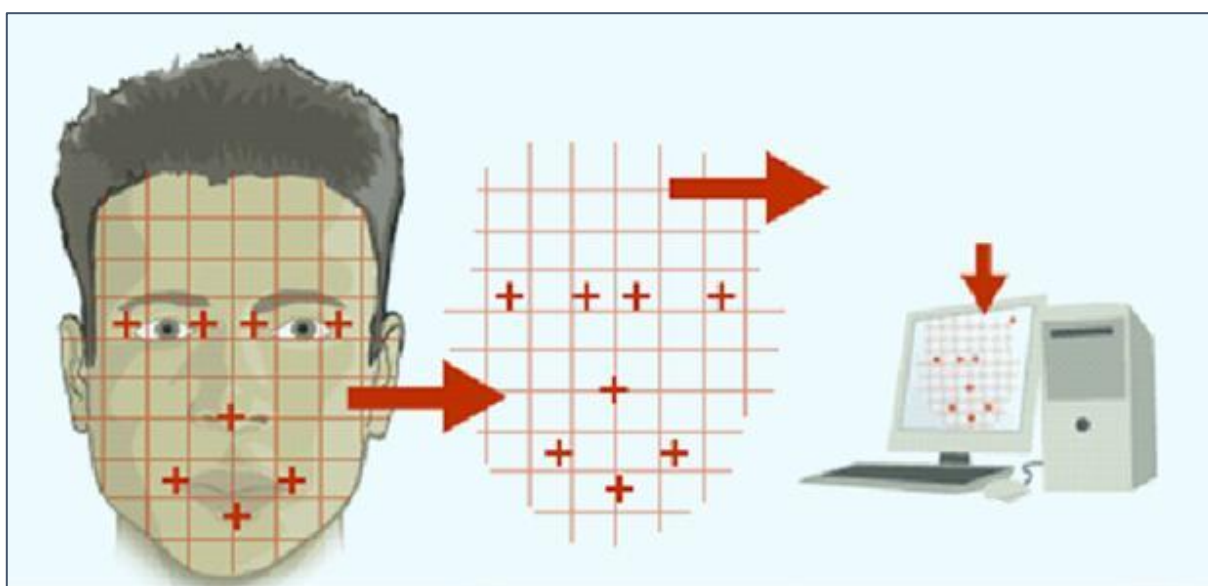


Figura 7 – Pontos para a o reconhecimento facial

Hoje em dia a tecnologia de reconhecimento facial é muito melhor do que antes, atualmente, usa-se modelos 3D para a identificação, em vez de 2D, como era no começo, isso fez com que fosse possível usar a tecnologia mesmo com o rosto da pessoa analisada em diferentes ângulos e com diferentes luminosidades.

Em relação a seu uso, a tecnologia de reconhecimento facial tem baixo custo, visto que, só é necessário uma câmera e um “software” compatível para o reconhecimento funcionar, além disso, é uma técnica nada intrusiva, já que pode ser usada até a metros do indivíduo.

3.6 Reconhecimento de Íris e Retina

A íris é um músculo no olho, responsável pela sua coloração. É na íris que se encontra a pupila, cuja função é controlar a quantidade de luz que vai para o olho.

Permanecendo igual durante toda nossa vida a íris é usada para reconhecimento como uma técnica muito segura, tendo como desvantagem que é muito cara para ser implementada, além de ser intrusiva. Ganhando sua forma de maneira aleatória no período de gestação, a íris possui características, estruturas e padrões únicos para cada pessoa e são elas que serão usadas para comparação.

O reconhecimento de retina é quase igual ao de íris, mas ao invés de utilizar os padrões presentes na íris para o reconhecimento, ele utiliza os padrões na disposição dos vasos sanguíneos que irrigam a retina. Por não ser um processo simples, tendo luzes de infravermelho de baixa intensidade sendo direcionadas para os olhos, se torna intrusiva e bastante incômoda.

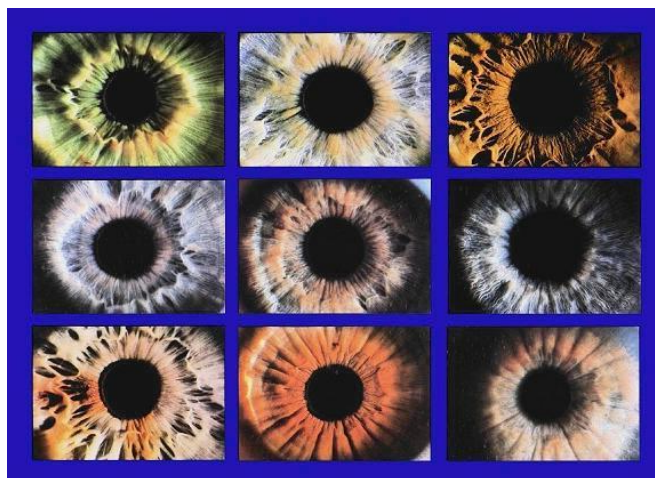


Figura 8 – Diferentes padrões de íris

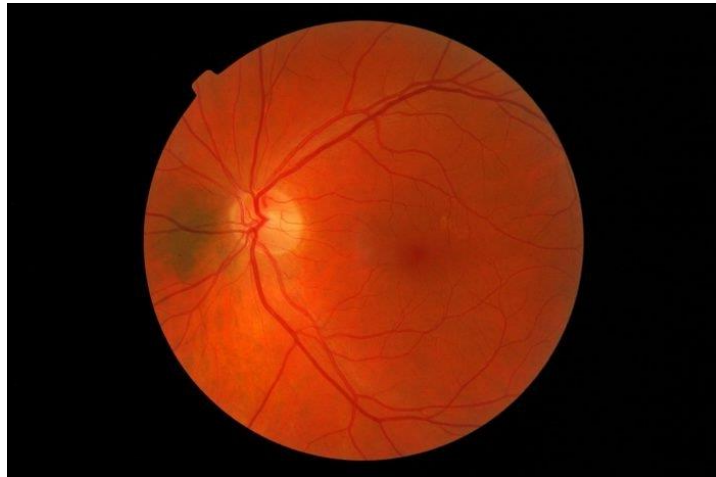


Figura 9 – Vasos sanguíneos que irrigam a retina

3.7 Reconhecimento de Voz

O reconhecimento de voz é a tecnologia que permite a captação de uma voz e a conversão dela, em dados, que serão analisados para se achar pontos únicos, tanto os aspectos físicos como os comportamentais. Sendo os aspectos físicos: características da voz, como volume graves e agudos que a pessoa reproduz enquanto fala utilizando de suas cordas vocais e a laringe. Já os aspectos comportamentais são a maneira como a pessoa se porta enquanto fala, as gírias que reproduz, as maneiras diferentes ou até erradas de se falar uma palavra, o sotaque, a entonação, bem como a movimentação de sua boca.

Essa técnica não é nada intrusiva, visto que, sua voz pode ser captada a distância, além disso, ela tem baixos custos sendo necessário somente algum dispositivo de captação de som, como um microfone, além é claro de um “software” compatível. Sua principal desvantagem se dá pela presença de ruídos no ambiente que podem atrapalhar na análise da voz e estado da pessoa que irá ter sua voz lida, visto que, um resfriado ou até mesmo o envelhecimento de uma pessoa pode diminuir a taxa de acertos dos sensores.



Figura 10 – Imagem ilustrativa de dados das ondas sonoras

Como visto, as diferentes técnicas biométricas de alta segurança seguem um mesmo padrão em seus processos e exigem que os dados coletados tenham unicidade para poderem ser elegíveis para o uso, com os seus processos sendo: a Captura, a Extração, a Criação de Padrão e a Comparação.

A primeira etapa da Captura consiste na sua interação com o “hardware” que irá “capturar” suas informações. Esses “hardwares” podem ser desde leitores de impressão digital, até câmeras e microfones.

Na próxima etapa, os dados capturados são extraídos e traduzidos em uma linguagem que o “software” possa usar. Dependendo da técnica, o “software” terá sua própria e diferente maneira de ler esses dados.

A terceira etapa é a de Criação de um padrão, os dados coletados pela etapa anterior são analisados e padrões presentes nas informações são achados pelos sistemas biométricos e separados para uma comparação posterior.

Para a última etapa, como dito, os padrões achados são comparados com os bancos de dados em busca de similaridades, tendo a pessoa que está percorrendo esse processo, sua identidade confirmada em caso de positivo e negada em caso de negativo.

4 PLANO DE DESENVOLVIMENTO DA APLICAÇÃO

O projeto tem como foco desenvolver um sistema capaz de identificar e autenticar um usuário por meio biométrico, com sua impressão digital. O acesso será feito primeiramente com usuário e senha, e logo após a autenticação, a biometria armazenada no banco de dados será analisada e o acesso será feito identificando os padrões por um algoritmo, caso a impressão digital do usuário seja compatível com a imagem armazenada.

Todos os passos terão interfaces intuitivas, para que o usuário possa acessar o sistema de forma simples, fazendo seu acesso de usuário.

O projeto será desenvolvido em um sistema, integrando o banco de dados para armazenar os “logins”, senhas e impressões digitais, e o programa de autenticação, que solicitará estas informações. Utilizando estas duas formas de autenticação, a segurança do sistema será maior, para ser evitada falhas e acessos não autorizados a sistemas de maior nível referente ao do usuário.

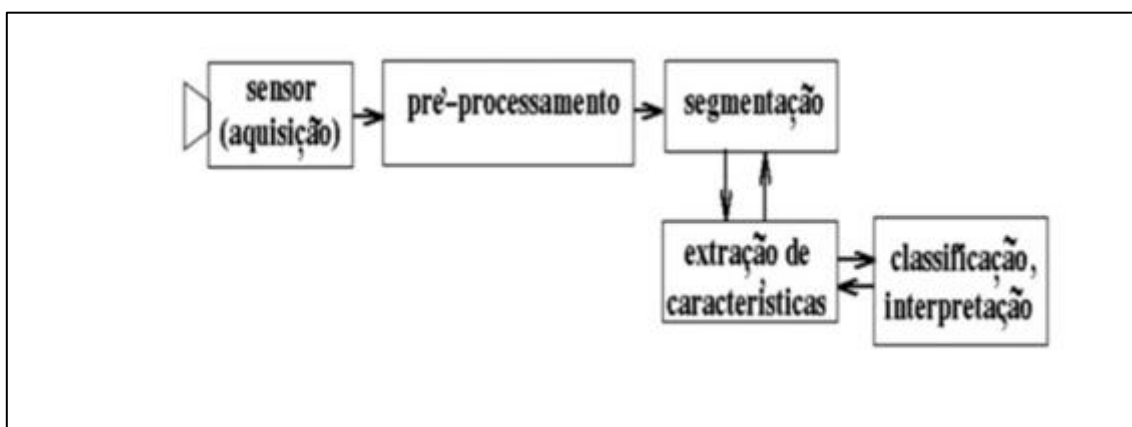


Figura 11 – Fases da autenticação biométrica

A linguagem utilizada para o desenvolvimento será Python, uma linguagem de alto nível de programação, onde podemos utilizar bibliotecas para auxiliar na criação dos outros componentes necessários, o banco de dados e o autenticador de biometria. O banco de dados será feito com o programa SQLite, um banco de dados relacional que dispensa o uso de um servidor para funcionar, e que utiliza a linguagem C. Já na parte do autenticador, será usada a OpenCV, uma biblioteca multiplataforma, criada originalmente pela Intel, para o desenvolvimento de aplicativos no âmbito da Visão Computacional e processamento de imagem.



Figura 12 – Ferramentas usadas na programação

A digital foi extraída utilizando carvão e papel sulfite, onde o carvão foi usado para marcar o dedo, e a sulfite para carimbar e obter a impressão. Assim, utilizando-se de um digitalizador, foi obtida uma imagem da digital, podendo assim ser armazenada no banco de dados.



Figura 13 – Impressões usadas nos testes do programa

Para entendermos agora como será feita a autenticação via impressão digital, precisamos entender como funciona a Visão Computacional. A Visão computacional é uma tecnologia que constrói inteligências artificiais para obter informações de imagens ou quaisquer dados multidimensionais. Assim, para obter as informações, a imagem é passada por etapas de pré-processamentos, e dentre estas etapas há a de separação de regiões ou elementos presentes na imagem que queremos identificar e obter informações. Após esta etapa, algumas técnicas são utilizadas e aplicadas na imagem, com intuito de destacar bordas, formas geométricas e tratar de ruídos, de modo a realçar e facilitar a obtenção das informações pelo sistema da Visão Computacional.

Agora na questão da resolução de uma imagem, temos que considerar a forma em que se foi adquirida, pois, para cada situação há uma forma de calcular sua resolução, como, por exemplo, a Resolução Espacial, que considera o nível de detalhamento dos píxeis da imagem, quanto maior sua amostragem, maior a quantidade de píxeis e maior será a qualidade da imagem; A Resolução de Bit, que também é conhecida como resolução de intensidade, nela se determina a quantidade de valores de intensidade ou cor que um píxel pode representar; A Resolução Temporal, que utiliza um sistema de captura contígua de imagens em um dado intervalo de tempo, representando os vídeos.

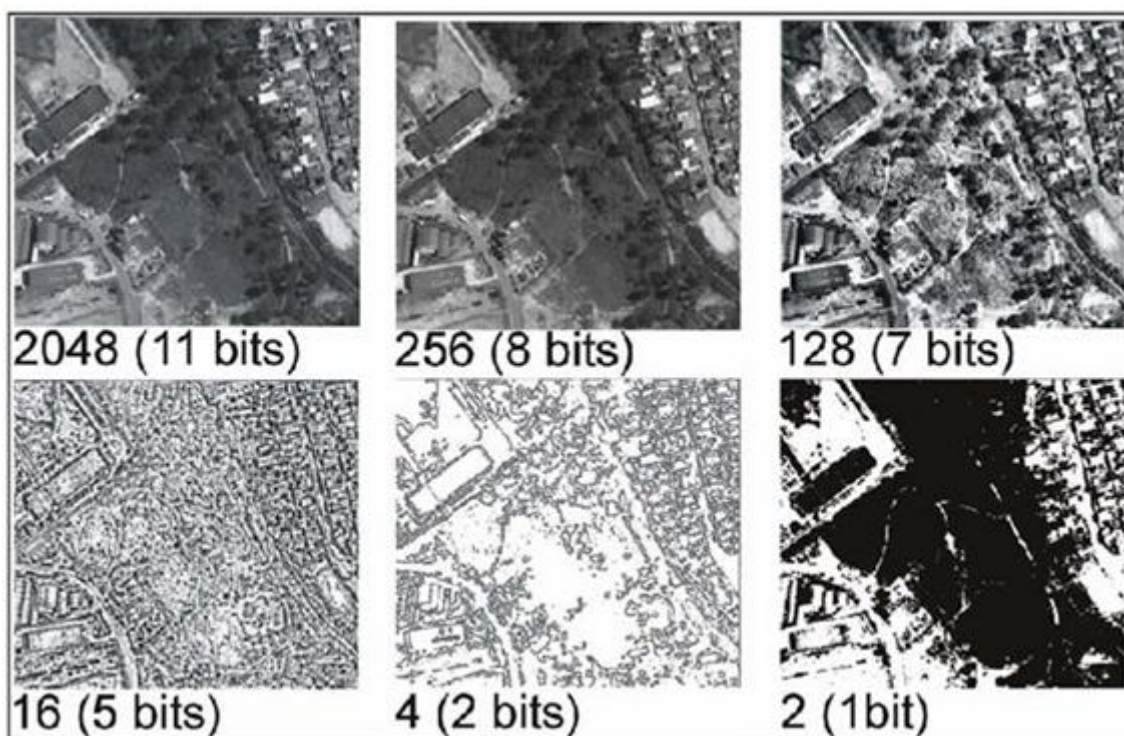


Figura 14 – Diferentes resoluções para a mesma imagem

Sabendo das resoluções, podemos passar para outra parte do pré-processamento da imagem, o HSV (Hue, Saturation ou Value) e a utilização do Histograma. No HSV, Hue (matiz) mexe com a escala das cores da imagem, a Saturation (saturação) altera a intensidade das cores, para mais fraco, ou mais forte, enquanto a Value (valor) aumenta ou diminui o brilho, assim, este recurso é usado na edição das imagens. Agora, usaremos o histograma para exemplificar a diferença de imagens coloridas das que apenas contém preto e branco. O Histograma de cores em uma imagem preta e branca, ou imagem binária, é um vetor contendo os 256 tons de cinza de uma imagem com escala de preto e branco, geralmente BMP, pois garante fidelidade dos píxeis e com a biblioteca chamada Matplotlib, é possível converter esse vetor em uma imagem.

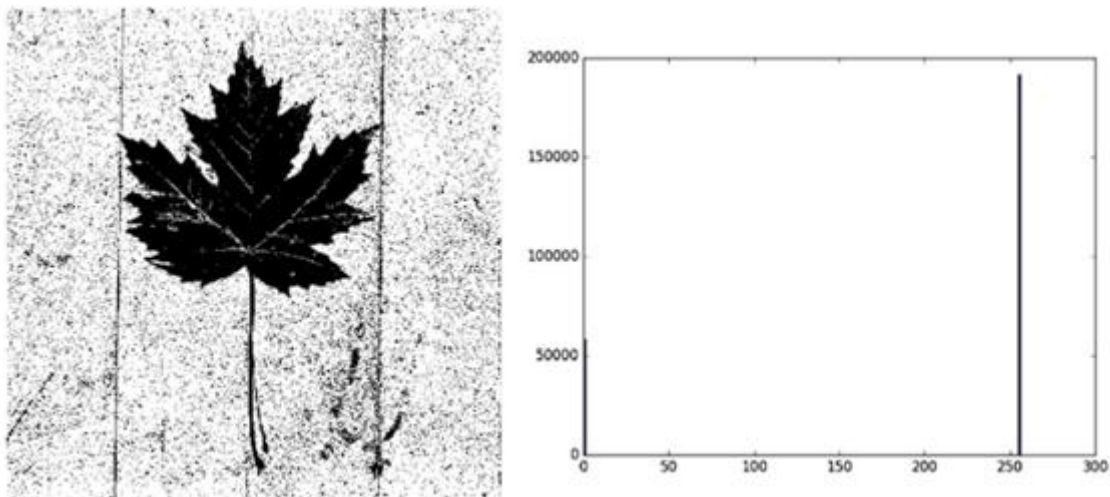


Figura 15 - Histograma de uma imagem binária

Percebe-se que os píxeis em preto são três vezes maiores que os píxeis brancos. Informações como esta podem ajudar a reconhecer objetos em uma imagem.

Já o Histograma de cores de uma imagem colorida iremos utilizar a mesma imagem da binária para fins de comparação. Pode-se observar que o canal vermelho é maior entre 200 e 250, isto porque ela contém tons avermelhados, próximos do laranja, diferente dos canais verde e azul.

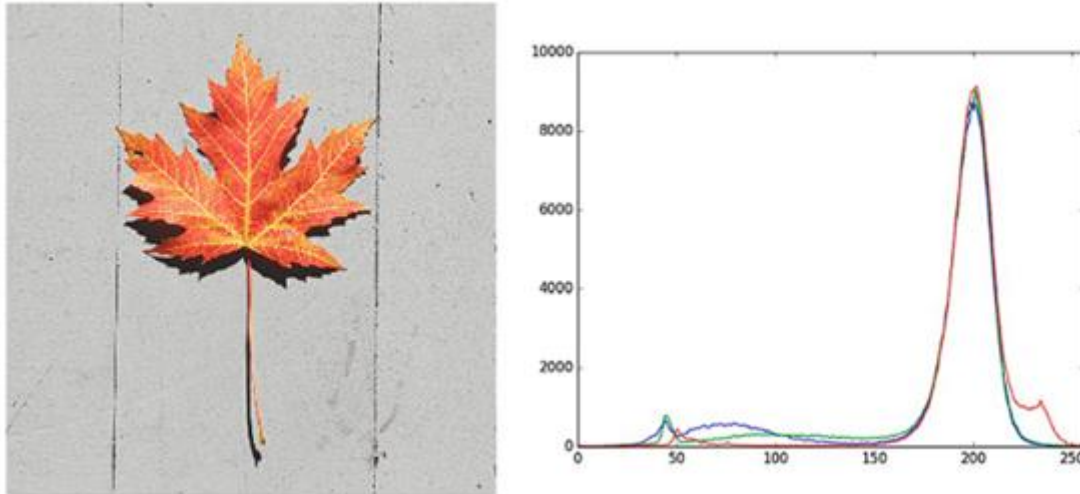


Figura 16 - Histograma de uma imagem colorida

4.1 Pré-processamento de Imagem

Essa primeira etapa consiste em realçar objetos de interesse em imagens e utiliza métodos com operações aritméticas, geométricas, ajuste de contraste e tratamento de ruído.

Para a biometria é aplicado uma abertura da imagem, que realiza uma operação de erosão seguida pela operação de dilatação e o fechamento da abertura usada para preencher a imagem corrigindo pontos no objeto de interesse danificadas pelo processo de binarização, que será explicado no próximo tópico.

4.2 Segmentação

A segmentação de objetos em uma imagem é uma das principais etapas de um sistema baseado em Visão Computacional, pois consiste em separar a área que representa o objeto de interesse em uma nova imagem, podendo assim extrair características a partir dela.

As formas mais conhecidas são: por binarização, por cor, por bordas e por movimento.

A técnica de binarização (também chamada limiarização) é utilizada na conversão de uma imagem em binária. Ela é usada na conversão das imagens para preto e branco para destacar os elementos da imagem.

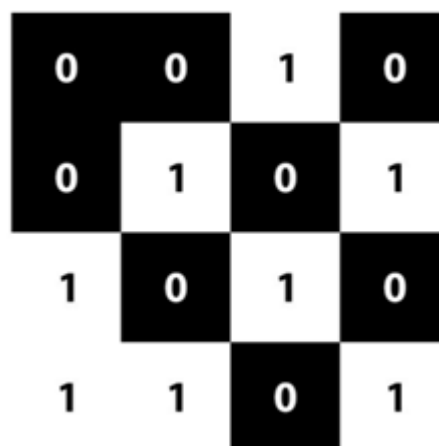


Figura 17 – Exemplo de Imagem Binária

No caso da biometria, destaca as ilhas, bifurcação, lago, ponte, linhas etc., de uma imagem biométrica, passado por pré-processamentos de imagens como dilatação, erosão, abertura e fechamento da imagem para definir melhor suas características e eliminar ruídos.



Figura 18 - Impressão digital

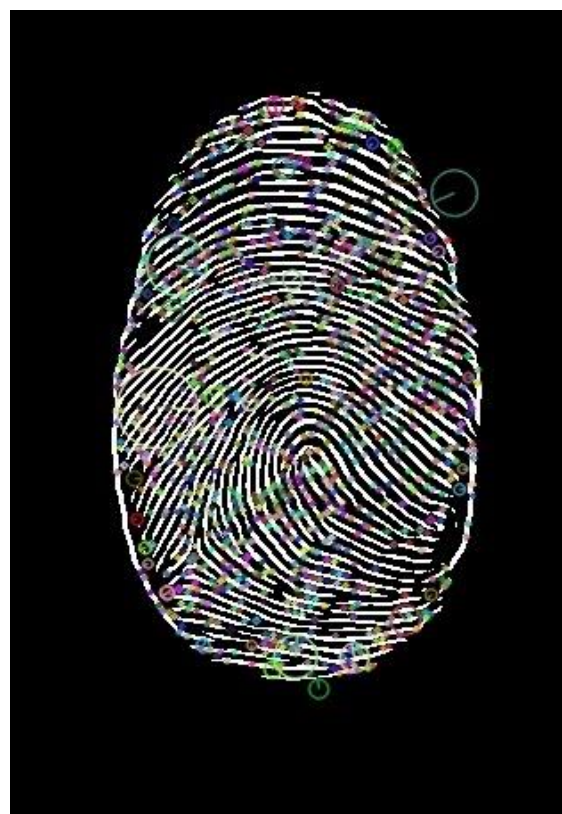


Figura 19 – Pontos Característicos sendo achados na impressão

4.3 Extração de Características

A biblioteca OpenCV dispõe de algumas ferramentas para extrair as características de uma imagem como ORB, SURF, FAST e a utilizada na aplicação de biometria a SIFT (Scale-Invariant Feature Transform), que coloca *keypoints* nas coordenadas de uma imagem, e *descriptors* que descreve a localização, e a partir deles é possível fazer uma comparação com outra imagem analisada para verificar a porcentagem/nível de *match* declarada pelo desenvolvedor.

4.4 Classificação/Interpretação

A ferramenta SIFT também dispõe os métodos `cv2.drawMatches` que exige os parâmetros de duas imagens, os *keypoints*, um *array* que faz o *loop* das distâncias entre esses pontos sendo a distância definida, pelo desenvolvedor, e entrega a compatibilidade entre as duas imagens requisitadas. Podemos comparar elas em um gráfico da biblioteca *pyplot*.

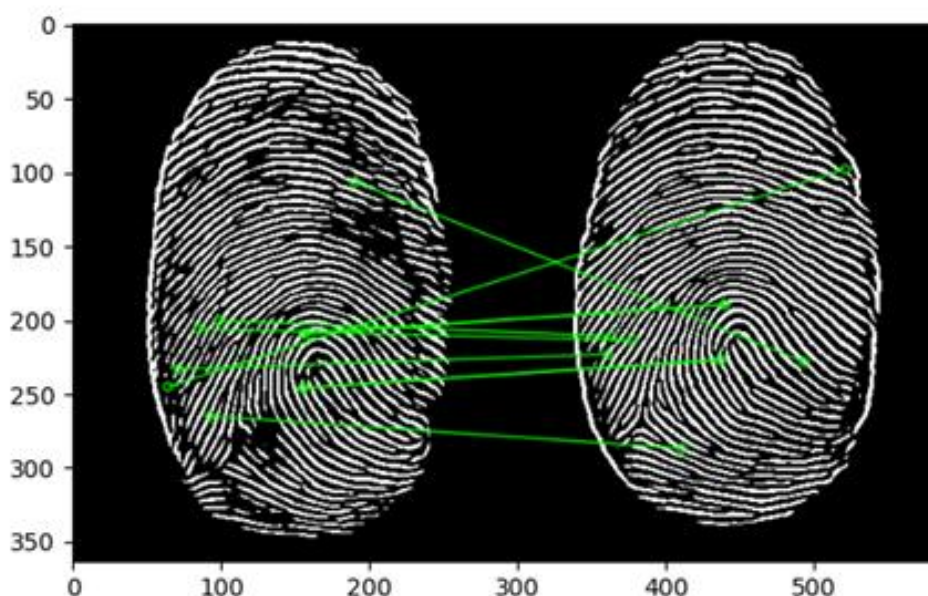


Figura 20 – Comparação de duas impressões

5 PROJETO DO PROGRAMA

O programa foi desenvolvido em três principais módulos, a inicialização com o “login” e senha padrão dos agentes para acessar a aplicação inicial, uma simulação recebendo uma foto biométrica captada por um dos membros e fazendo uma autenticação para poder abrir a tela inicial com as informações dos níveis de acesso 1, 2 e 3.

Desenvolvido em *Python*, foi utilizado as bibliotecas *PyQt5*, para ler as telas produzidas no “software” *Qt Designer* e abri-las no *User Interface*, a *cv2*, que é a biblioteca do *OpenCV*, para executar e processar imagens, *numpy* que é uma ferramenta para trabalhar com vetores e matrizes, *SQLite3* para armazenar os dados de “login” e senha dos agentes, *time* para aplicar um tempo de execução enquanto simula a autenticação biométrica, *fingerprint_enhancer* que é uma *lib* que já executa o pré-processamento de imagem e aplica a binarização da imagem e a *pyplot* do *matplotlib* para visualizar um gráfico e comparar às duas imagens.

O *Qt Designer* é um programa desenvolvido em C++ para desenhar as interfaces das telas e depois poder integrar os componentes através de suas variáveis de aplicação, junto a linguagem de programação que faz a leitura da página, sendo possível também estilizar em CSS alguns elementos. Usamos a fonte *Poppins* e alteramos alguns estilos dos botões, usamos os *lineEdit* para receber os campos de “login” e exibição do tipo de acesso e o usuário.

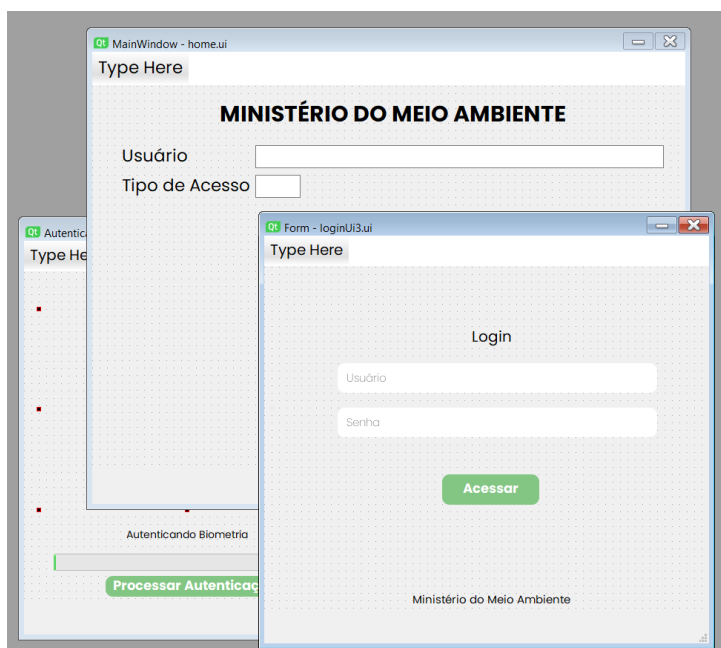


Figura 21 – Diferentes telas do programa

Através dessa ferramenta é possível mostrar ao usuário o processamento das imagens executando o *OpenCV* para validar a autenticação e alterando a *label* com as etapas de verificação.

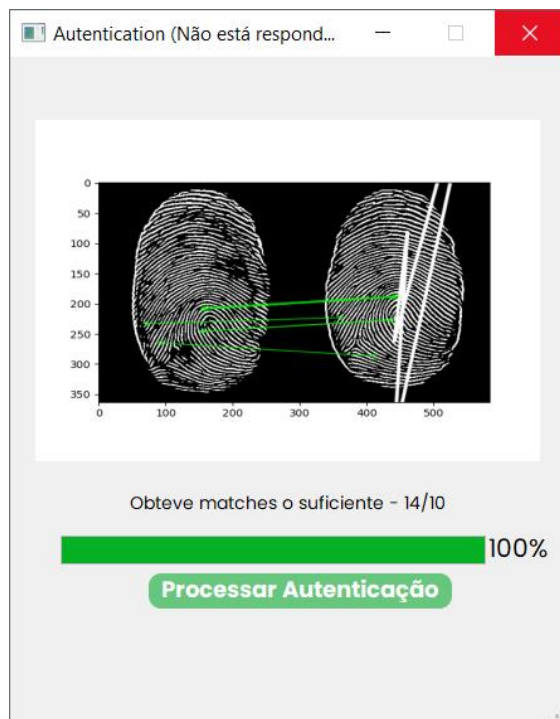


Figura 22 – Processamento da impressão digital

O programa ao todo contém quatro principais funções: *chama_tela_home*, que recebe os dados de usuário para fazer o “login”, autentica com o banco de dados, e pula para a etapa de processamento de imagem; *tipo_de_acesso* que mostra sobre as propriedades rurais que utilizam agrotóxicos proibidos por causarem grandes impactos nos lenções freáticos, rios e mares dependendo do nível de restrição; *autenticar* que faz a simulação do processamento de imagem com todas as etapas e descreve o nível de *match* e assim acessa a tela inicial com as informações e nível de acesso; e *logout* para sair do programa.

O repositório no *github* com os arquivos podem ser encontrados no link: <https://github.com/felipegomesk7m/python-fingerprint>

6 RELATÓRIO COM AS LINHAS DO CÓDIGO DO PROGRAMA

```

from PyQt5 import QtGui, uic, QtWidgets
import cv2
import numpy as np
import sqlite3
import time
import fingerprint_enhancer
from matplotlib import pyplot as plt

def chama_tela_home():
    user = loginUi3.lineEdit_user.text()
    password = loginUi3.lineEdit_password.text()
    try:
        db=sqlite3.connect("Cadastros_Agentes.db")
        cursor=db.cursor()
        cursor.execute("SELECT Senha FROM Cadastro_Agentes WHERE
Usuário = '{}';".format(user));
        senha_bd = cursor.fetchall()

        if user == "" and password == "":
            loginUi3.loginInvalido.setText("Campos Vazios")
        elif senha_bd[0][0] == password:
            loginUi3.close()
            if user == 'fgomes96':
                tipo_de_acesso(1)
            elif user == 'hboracine01':
                tipo_de_acesso(2)
            elif user == 'gbajona01':
                tipo_de_acesso(3)
        else:
            loginUi3.loginInvalido.setText("Dados de Login ou Senha Incorretos")
    except:

```

```

loginUi3.loginInvalido.setText("Dados de Login ou Senha Incorretos")
finally:
    db.close()

def tipo_de_acesso(acesso):
    acesso_bd = acesso
    if acesso_bd == 1:
        autenticar()
        home.lineEdit.setText('Felipe Gomes')
        home.lineEdit_2.setText('1')
        home.label_4.setText('Informações do nível 1 - Produção agrícola\n Nome
da unidade produtora (produtor agrícola) – Bom Futuro\n Endereço do produtor
agrícola - Av. dos Florais, S/N - Ribeirão do Lipa, Cuiabá - MT\n Produto(s) agrícolas
produzidos – Soja, milho e algodão\n Produção anual em quilogramas –
Aproximadamente 1,7 milhão de toneladas\n Destino da produção (mercado interno
ou exportação)\n Número de empregados da unidade produtora - 5 mil\n Quantidade
de máquinas e implementos agrícolas – Em torno de 400 máquinas, sendo elas tanto
para colheita,\nquanto caminhões de transporte\n Nível de automação da unidade
produtora – Alto nível, sendo a maior produtora agrícola do Brasil')
    elif acesso_bd == 2:
        autenticar()
        home.lineEdit.setText('Heitor Boracine')
        home.lineEdit_2.setText('2')
        home.label_4.setText('Incentivos fiscais recebidos – Anistia, antecipação de
receitas, refinanciamento tributário, entre outros.\n Impostos municipais pagos – IPTU
(Imposto Predial Territorial Urbano)\n *poderá incidir caso trata-se de propriedade
localizada em zona urbana ou urbanizada*;\n ISSQN (Imposto Sobre Serviços de
Qualquer Natureza).\n Impostos estaduais recolhidos – ICMS (Imposto sobre
Circulação de Mercadorias);\n IPVA (Imposto sobre Propriedade de Veículos
Automotores).\n Impostos federais pagos – IRPJ (Imposto de Renda);\n IE (Imposto
de Exportação);\n ITR (Imposto Territorial Rural)\n *poderá incidir caso trata-se de
propriedade localizada em zona rural*; Cofins, PIS PASEP, CSLL, INSS.\n Taxas
federais pagas – Taxa de licenciamento ambiental para instalação e operação da
empresa.')

```



```

elif acesso_bd == 3:
    autenticar()
    home.lineEdit.setText('Gabriel Bajona')
    home.lineEdit_2.setText('3')
    home.label_4.setText('Agrotóxicos empregados nas produções agrícolas -
glifosato; mancozebe; acefato; óleo mineral; atrazina;\n Ação do sistema: quando da
ocorrência de agrotóxicos proibidos, notificar a unidade produtora quanto a interdição
da produção.')

```

```

def autenticar():
    biometria.show()
    biometria.progressBar.setRange(0,100)
    biometria.progressBar.setValue(0)
    biometria.label.setPixmap(QtGui.QPixmap(""))
    biometria.image.setPixmap(QtGui.QPixmap(""))

def progress():
    counter = 0
    biometria.image.setPixmap(QtGui.QPixmap('fingerprint.png'))
    biometria.text_progressbar.setText('Recebendo imagem por arquivo')

    while (int(counter) <= 100):
        MIN_MATCH_COUNT = 10
        if counter == 25:
            biometria.text_progressbar.setText('Aplicando Binarização')
            img1 = cv2.imread('fingerprint.png', 0)
            img2 = cv2.imread('fingerprint2.png')
            img1 = fingerprint_enhancer.enhance_Fingerprint(img1)
            img2 = fingerprint_enhancer.enhance_Fingerprint(img2)
            cv2.imwrite("img_binarizada.png", img1)
            biometria.image.setPixmap(QtGui.QPixmap('img_binarizada.png'))

        if counter == 50:

```

```

biometria.text_progressbar.setText('Extração de Características')
# Iniciando SIFT
sift = cv2.SIFT_create()
# Encontrando Keypoints e descriptors com SIFT
kp1, des1 = sift.detectAndCompute(img1, None)
kp2, des2 = sift.detectAndCompute(img2, None)
kp_img = cv2.drawKeypoints(img1, kp1, None, color=(0, 255,
0), flags=cv2.DRAW_MATCHES_FLAGS_DRAW_RICH_KEYPOINTS)
cv2.imwrite("keypoints.png", kp_img)
biometria.image.setPixmap(QtGui.QPixmap('keypoints.png'))
time.sleep(2)

if counter == 75:
    biometria.image.setPixmap(QtGui.QPixmap(""))
    FLANN_INDEX_KDTREE = 1
    index_params = dict(algorithm = FLANN_INDEX_KDTREE, trees = 10)
    search_params = dict(checks = 50)
    flann = cv2.FlannBasedMatcher(index_params, search_params)
    matches = flann.knnMatch(des1, des2, k=2)
    # Agrupando todos os matches
    good = []
    for m, n in matches:
        if m.distance < 0.7*n.distance:
            good.append(m)
    # Verificando os matches e entregando resultado
    if len(good) > MIN_MATCH_COUNT:
        src_pts = np.float32([ kp1[m.queryIdx].pt for m in good ]).reshape(-
1, 1, 2)
        dst_pts = np.float32([ kp2[m.trainIdx].pt for m in good ]).reshape(-1, 1, 2)
        M, mask = cv2.findHomography(src_pts, dst_pts, cv2.RANSAC, 5.0)
        matchesMask = mask.ravel().tolist()
        h, w = img1.shape
        pts = np.float32([ [0, 0], [0, h-1], [w-1, h-1], [w-1, 0] ]).reshape(-1, 1, 2)
        dst = cv2.perspectiveTransform(pts, M)

```

```

img2 = cv2.polylines(img2,[np.int32(dst)],True,255,3, cv2.LINE_AA)
print("Obteve matches o suficiente - {}/{}".format(len(good),
MIN_MATCH_COUNT))
biometria.text_progressbar.setText("Obteve matches o suficiente -
{}/{}".format(len(good), MIN_MATCH_COUNT))
else:
    print("Não obteve matches o suficiente - {}/{}".format(len(good),
MIN_MATCH_COUNT))
    biometria.text_progressbar.setText("Não obteve matches o suficiente -
{}/{}".format(len(good), MIN_MATCH_COUNT))
    matchesMask = None
    draw_params = dict(matchColor = (0,255,0),
        singlePointColor = None,
        matchesMask = matchesMask,
        flags = 2)
    img3 = cv2.drawMatches(img1,kp1,img2,kp2,good,None,**draw_params)
    plt.imshow(img3,)
    plt.savefig('Matches.png', format='png')
    biometria.label.setPixmap(QtGui.QPixmap('Matches.png'))
    time.sleep(2)

counter += 1
biometria.progressBar.setValue(int(counter))
time.sleep(0.1)

if counter == 100:
    biometria.text_progressbar.setText('Biometria Validada')
    biometria.image.setPixmap(QtGui.QPixmap('Matches.png'))
    time.sleep(5)
    biometria.close()
    home.show()

biometria.pushButton.clicked.connect(lambda: progress())

```

```
def logout():  
    home.close()  
    loginUi3.show()  
    loginUi3.lineEdit_user.setText("")  
    loginUi3.lineEdit_password.setText("")  
    loginUi3.loginInvalido.setText("")  
  
app=QtWidgets.QApplication([])  
loginUi3 = uic.loadUi('loginUi3.ui')  
home = uic.loadUi('home.ui')  
biometria = uic.loadUi('biometria.ui')  
loginUi3.btn_acessar.clicked.connect(chama_tela_home)  
home.pushButton.clicked.connect(logout)  
loginUi3.show()
```

7 APRESENTAÇÃO DO PROGRAMA EM FUNCIONAMENTO

Tela de “login” para iniciar a autenticação biométrica e acessar a tela inicial, para isso valida as informações dos campos com o banco de dados.

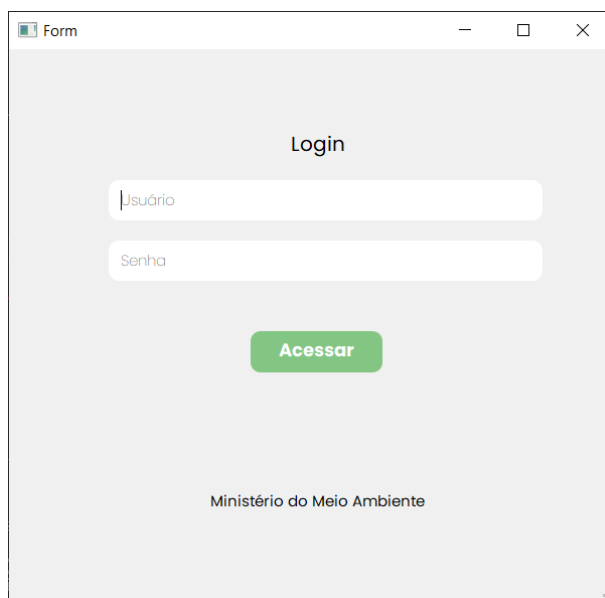
A screenshot of a web application window titled "Form". The window has a light gray background. At the top center, the word "Login" is displayed. Below it are two white input fields: the first is labeled "Usuário" and the second is labeled "Senha". Below the input fields is a green button with the text "Acessar" in white. At the bottom center, the text "Ministério do Meio Ambiente" is displayed.

Figura 23 – Tela de “Login”

Caso os dados estejam incorretos, o programa avisa que as informações estão inválidas. Para acessar deve utilizar os usuários fgomes96 com senha 123, hboracine01 com senha 345 ou gbajona01 com senha 789.

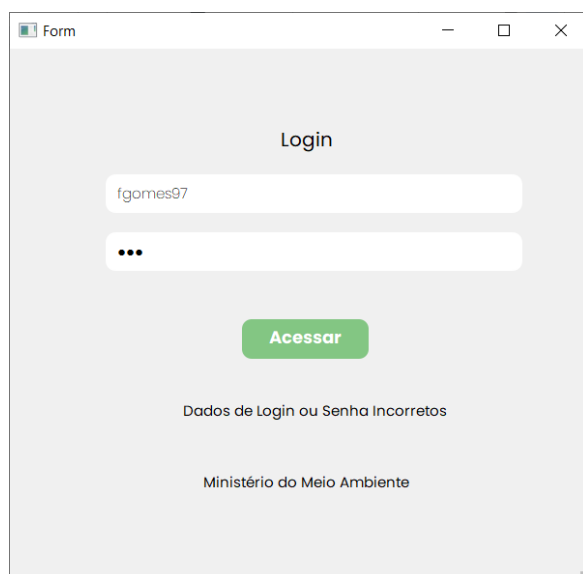
A screenshot of the same web application window as in Figure 23, but with error feedback. The "Usuário" field now contains the text "fgomes97". The "Senha" field is masked with three black dots. Below the "Acessar" button, the text "Dados de Login ou Senha Incorretos" is displayed in a smaller font. The "Ministério do Meio Ambiente" text remains at the bottom.

Figura 24 – Tela de “Login” preenchida com dados incorretos

Após o “login” é feita uma simulação de autenticação biométrica em uma barra de progresso obtida através de um arquivo.



Figura 25 – Processamento da autenticação biométrica

Aplicando Binarização e pré-processamentos com a lib fingerprint_enhance



Figura 26 – Aplicação da Binarização

Extraindo as características com SIFT do OpenCV



Figura 27 – Extração de características

Comparando as imagens e verificando a compatibilidade de matches sendo a mínima requerida 10, como obteve o sucesso de 14 matches o programa foi autenticado.

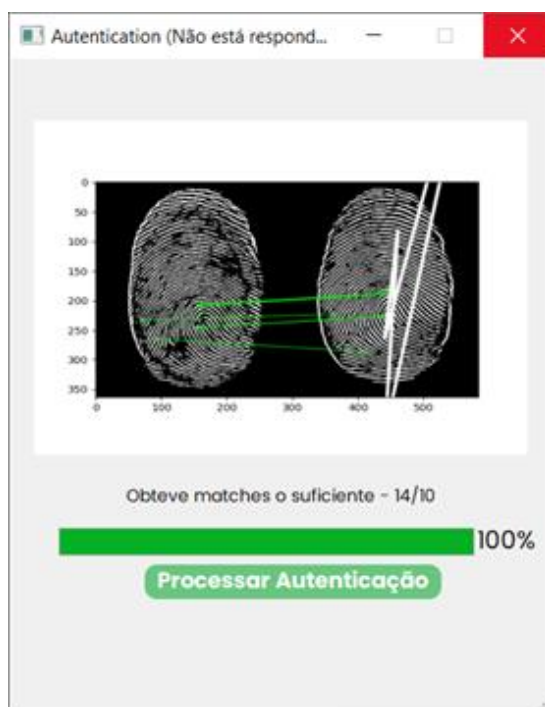


Figura 28 – Comparação da impressão

Tela inicial dos usuários logado com as informações.



MainWindow

MINISTÉRIO DO MEIO AMBIENTE

Usuário

Tipo de Acesso

Informações do nível 1 - Produção agrícola
 Nome da unidade produtora (produtor agrícola) - Bom Futuro
 Endereço do produtor agrícola - Av. dos Florais, S/N - Ribeirão do Lipo, Cuiabá - MT
 Produto(s) agrícolas produzidos - Soja, milho e algodão
 Produção anual em quilogramas - Aproximadamente 1,7 milhão de toneladas
 Destino da produção (mercado interno ou exportação)
 Número de empregados da unidade produtora - 5 mil
 Quantidade de máquinas e implementos agrícolas - Em torno de 400 máquinas, sendo elas tanto para colheita, quanto caminhões de transporte
 Nível de automação da unidade produtora - Alto nível, sendo a maior produtora agrícola do Brasil

Logout

Figura 29 – Tela dos níveis de acesso (1)



MainWindow

MINISTÉRIO DO MEIO AMBIENTE

Usuário

Tipo de Acesso

Incentivos fiscais recebidos - Anistia, antecipação de receitas, refinanciamento tributário, entre outros.
 Impostos municipais pagos - IPTU (Imposto Predial Territorial Urbano)
 poderá incidir caso trata-se de propriedade localizada em zona urbana ou urbanizada;
 ISSQN (Imposto Sobre Serviços de Qualquer Natureza);
 Impostos estaduais recolhidos - ICMS (Imposto sobre Circulação de Mercadorias);
 IPVA (Imposto sobre Propriedade de Veículos Automotores).
 Impostos federais pagos - IRPJ (Imposto de Renda);
 IE (Imposto de Exportação);
 ITR (Imposto Territorial Rural)
 poderá incidir caso trata-se de propriedade localizada em zona rural;
 Cofins, PIS PASEP, CSLL, INSS.
 Taxas federais pagas - Taxa de licenciamento ambiental para instalação e operação da empresa.

Logout

Figura 30 – Tela dos níveis de acesso (2)

MainWindow

MINISTÉRIO DO MEIO AMBIENTE

Usuário

Tipo de Acesso

Agrotóxicos empregados nas produções agrícolas - glifosato; mancozebe; acefato; óleo mineral; atrazina;
Ação do sistema: quando da ocorrência de agrotóxicos proibidos, notificar a unidade produtora quanto a interdição da produção.

[Logout](#)

Figura 31 – Tela dos níveis de acesso (3)

8 BIBLIOGRAFIA

Sinfic. História Geral da Biometria. Disponível em:

<<http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=25030>>. Acesso em: 17 out. 2021

Blog Giga Security. Biometria: entenda como ela revolucionou a segurança eletrônica. Disponível em:

<<https://blog.gigasecurity.com.br/biometria-entenda-como-ela-revolucionou-a-seguranca-eletronica/#:~:text=O%20uso%20da%20biometria%20como,estabelecer%20na%20d%C3%A9cada%20de%201970>>. Acesso em: 17 out. 2021

Blog Giga Security. Noções de segurança eletrônica: o que eu preciso saber sobre o tema?. Disponível em:

<<https://blog.gigasecurity.com.br/nocoas-de-seguranca-eletronica/>>. Acesso em: 17 out. 2021

GTA UFRJ. Biometria - Assinatura. Disponível em:

<https://www.gta.ufrj.br/grad/10_1/1a-versao/assinatura/historico.html>. Acesso em: 17 out. 2021

Canaltech. O que é biometria?. Disponível em:

<<https://canaltech.com.br/seguranca/O-que-e-biometria/>>. Acesso em: 17 out. 2021

Tecnoblog. O que é biometria? Os 6 tipos mais usados na tecnologia. Disponível em: <<https://tecnoblog.net/273655/o-que-e-biometria-tecnologia/>>. Acesso em: 17 out. 2021

Ebox Digital. Quais são os 7 tipos de autenticação de documentos? Entenda aqui.

Disponível em: <<https://www.eboxdigital.com.br/blog/quais-sao-os-7-tipos-de-autenticacao-de-documentos-entenda-aqui>>. Acesso em: 17 out. 2021

Tecmundo. Como funciona o reconhecimento facial. Disponível em:

<<https://www.tecmundo.com.br/camera-digital/10347-como-funcionam-os-sistemas-de-reconhecimento-facial.htm>>. Acesso em: 17 out. 2021

GTA UFRJ. Biometria - Reconhecimento de Íris. Disponível em:

<https://www.gta.ufrj.br/grad/08_1/iris/index.html>. Acesso em: 17 out. 2021

OpenCV. Feature Matching + Homography to find Objects. Disponível em:

<https://docs.opencv.org/3.4/d1/de0/tutorial_py_feature_homography.html>. Acesso em: 25 nov. 2021

OpenCV. Introduction to SIFT (Scale-Invariant Feature Transform). Disponível em:

<https://docs.opencv.org/4.x/da/df5/tutorial_py_sift_intro.html>. Acesso em: 25 nov. 2021

OpenCV. Feature Matching. Disponível em:

<https://docs.opencv.org/3.4/dc/dc3/tutorial_py_matcher.html>. Acesso em: 25 nov. 2021

Blog Francium. Feature detection and matching with OpenCV. Disponível em:

<<https://blog.francium.tech/feature-detection-and-matching-with-opencv-5fd2394a590>>. Acesso em: 25 nov. 2021

Barelli, Felipe. Introdução à Visão Computacional. São Paulo: Casa do Código, 2018.

9 FICHA DE ATIVIDADES PRÁTICAS SUPERVISIONADAS



FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Felipe de Sousa Gomes TURMA: CC6A68 RA: N4750H0

CURSO: Ciência da Computação CAMPUS: Paraíso SEMESTRE: 6º TURNO: Manhã

CÓDIGO DA ATIVIDADE: 77B3 SEMESTRE: Sexto ANO GRADE: 2021

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
25/09/2021	Iniciamos a montagem do nosso grupo	5h	Felipe Gomes		
27/09/2021	Começamos a pesquisar sobre o tema	5h	Felipe Gomes		
28/09/2021	Separamos as funções de cada membro do grupo	5h	Felipe Gomes		
10/10/2021	Pesquisamos maneira de capturar impressões digitais	5h	Felipe Gomes		
15/10/2021	Escrevemos o tópico Objetivo do Trabalho	5h	Felipe Gomes		
17/10/2021	Iniciamos a escrita do tópico das técnicas biométricas	5h	Felipe Gomes		
25/10/2021	Começamos a programar o sistema de login	5h	Felipe Gomes		
06/11/2021	Checamos as informações de nível de acesso	5h	Felipe Gomes		
08/11/2021	Começamos a fazer a interface gráfica do nosso sistema de login	5h	Felipe Gomes		
10/11/2021	Começamos a escrever o plano de desenvolvimento	5h	Felipe Gomes		
11/11/2021	Terminamos de escrever o tópico da técnicas biométricas	5h	Felipe Gomes		
13/11/2021	Começamos a escrever o Projeto do Programa	5h	Felipe Gomes		
14/11/2021	Terminamos de escrever o plano de desenvolvimento	5h	Felipe Gomes		
15/11/2021	Terminamos de escrever o Projeto do Programa	5h	Felipe Gomes		
16/11/2021	Terminamos todos tópicos do trabalho	5h	Felipe Gomes		
17/11/2021	Fizemos uma revisão final em todos os textos do trabalho	5h	Felipe Gomes		

(1) Horas atribuídas de acordo com o regulamento das Atividades Práticas Supervisionadas do curso.

TOTAL DE HORAS ATRIBUÍDAS: 80h

AVALIAÇÃO: _____

Aprovado ou Reprovado

NOTA: _____

DATA: ____/____/____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO



FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Gabriel Bajona Sprovieri TURMA: CC6A68 RA: F03BGE5

CURSO: Ciência da Computação CAMPUS: Paraíso SEMESTRE: 6º TURNO: Manhã

CÓDIGO DA ATIVIDADE: 77B3 SEMESTRE: Sexto ANO GRADE: 2021

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
25/09/2021	Iniciamos a montagem do nosso grupo	5h	Gabriel B. Sprovieri		
27/09/2021	Começamos a pesquisar sobre o tema	5h	Gabriel B. Sprovieri		
28/09/2021	Separamos as funções de cada membro do grupo	5h	Gabriel B. Sprovieri		
10/10/2021	Pesquisamos maneira de capturar impressões digitais	5h	Gabriel B. Sprovieri		
15/10/2021	Escrevemos o tópico Objetivo do Trabalho	5h	Gabriel B. Sprovieri		
17/10/2021	Iniciamos a escrita do tópico das técnicas biométricas	5h	Gabriel B. Sprovieri		
25/10/2021	Começamos a programar o sistema de login	5h	Gabriel B. Sprovieri		
06/11/2021	Checamos as informações de nível de acesso	5h	Gabriel B. Sprovieri		
08/11/2021	Começamos a fazer a interface gráfica do nosso sistema de login	5h	Gabriel B. Sprovieri		
10/11/2021	Começamos a escrever o plano de desenvolvimento	5h	Gabriel B. Sprovieri		
11/11/2021	Terminamos de escrever o tópico da técnicas biométricas	5h	Gabriel B. Sprovieri		
13/11/2021	Começamos a escrever o Projeto do Programa	5h	Gabriel B. Sprovieri		
14/11/2021	Terminamos de escrever o plano de desenvolvimento	5h	Gabriel B. Sprovieri		
15/11/2021	Terminamos de escrever o Projeto do Programa	5h	Gabriel B. Sprovieri		
16/11/2021	Terminamos todos tópicos do trabalho	5h	Gabriel B. Sprovieri		
17/11/2021	Fizemos uma revisão final em todos os textos do trabalho	5h	Gabriel B. Sprovieri		

(1) Horas atribuídas de acordo com o regulamento das Atividades Práticas Supervisionadas do curso.

TOTAL DE HORAS ATRIBUÍDAS: 80h

AValiação: _____

Aprovado ou Reprovado

NOTA: _____

DATA: ____/____/____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO



FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

NOME: Heitor Augusto Oliveira Boracine TURMA: CC6A68 RA: N441DC2

CURSO: Ciência da Computação CAMPUS: Paraíso SEMESTRE: 6º TURNO: Manhã

CÓDIGO DA ATIVIDADE: 77B3 SEMESTRE: Sexto ANO GRADE: 2021

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
25/09/2021	Iniciamos a montagem do nosso grupo	5h	Heitor A. O. Boracine		
27/09/2021	Começamos a pesquisar sobre o tema	5h	Heitor A. O. Boracine		
28/09/2021	Separamos as funções de cada membro do grupo	5h	Heitor A. O. Boracine		
10/10/2021	Pesquisamos maneira de capturar impressões digitais	5h	Heitor A. O. Boracine		
15/10/2021	Escrevemos o tópico Objetivo do Trabalho	5h	Heitor A. O. Boracine		
17/10/2021	Iniciamos a escrita do tópico das técnicas biométricas	5h	Heitor A. O. Boracine		
25/10/2021	Começamos a programar o sistema de login	5h	Heitor A. O. Boracine		
06/11/2021	Checamos as informações de nível de acesso	5h	Heitor A. O. Boracine		
08/11/2021	Começamos a fazer a interface gráfica do nosso sistema de login	5h	Heitor A. O. Boracine		
10/11/2021	Começamos a escrever o plano de desenvolvimento	5h	Heitor A. O. Boracine		
11/11/2021	Terminamos de escrever o tópico da técnicas biométricas	5h	Heitor A. O. Boracine		
13/11/2021	Começamos a escrever o Projeto do Programa	5h	Heitor A. O. Boracine		
14/11/2021	Terminamos de escrever o plano de desenvolvimento	5h	Heitor A. O. Boracine		
15/11/2021	Terminamos de escrever o Projeto do Programa	5h	Heitor A. O. Boracine		
16/11/2021	Terminamos todos tópicos do trabalho	5h	Heitor A. O. Boracine		
17/11/2021	Fizemos uma revisão final em todos os textos do trabalho	5h	Heitor A. O. Boracine		

(1) Horas atribuídas de acordo com o regulamento das Atividades Práticas Supervisionadas do curso.

TOTAL DE HORAS ATRIBUÍDAS: 80h

AVALIAÇÃO: _____

Aprovado ou Reprovado

NOTA: _____

DATA: ____/____/____

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO