Instituto Superior de Tecnologias Avançadas

Licenciatura em Engenharia Multimédia

AccessFace Sentinel

SISTEMA DE DETEÇÃO E RECONHECIMENTO FACIAL PARA CONTROLO DE ACESSO A UM DERTERMINADO LOCAL

Projeto Académico realizado por:

Gonçalo Silva da Conceição Santos Garcia, Nº 21406

Coordenador: Prof. Dr. Pedro Brandão

Orientadora: Prof. Dra. Dulce Mourato

Lisboa, Ano Letivo 2022/2023

Instituto Superior de Tecnologias Avançadas

Licenciatura em Engenharia Multimédia

AccessFace Sentinel

SISTEMA DE DETEÇÃO E RECONHECIMENTO FACIAL PARA CONTROLO DE ACESSO A UM DERTERMINADO LOCAL

Projeto Académico realizado por:

Gonçalo Silva da Conceição Santos Garcia, Nº 21406

Coordenador: Prof. Dr. Pedro Brandão

Orientadora: Prof. Dra. Dulce Mourato

Lisboa, Ano Letivo 2022/2023

Agradecimentos

Em primeiro lugar, agradeço especialmente à minha namorada e aos meus pais, por todo o apoio e incentivo fundamental ao longo de todos estes anos.

Quero ainda agradecer especialmente aos meus familiares e amigos por toda a paciência, apoio e amizade ao longo de todo este percurso.

Agradeço, à Professora Dra. Dulce Mourato por todo o apoio, disponibilidade e orientação concedida durante toda a realização deste projeto.

Agradeço a todos os Professores e Professoras que ao longo deste percurso foram fundamentais através do conhecimento e motivação transmitida assim como pela exigência e rigor aplicados.

Resumo

Este projeto académico teve como objetivo o desenvolvimento de um sistema de deteção e reconhecimento facial para controlo de acesso a um determinado local utilizando a linguagem de programação *Python* e as bibliotecas *OpenCv*, *Dlib* e *Face_recognition*. Este sistema utiliza o microcomputador *Raspberry Pi 4* como unidade central de processamento. Os sistemas de deteção e reconhecimento facial para controlo de acesso a um determinado local já existem no mercado há bastante tempo, mas normalmente não disponibilizam funcionalidades relacionadas com segurança. Todo o desenvolvimento deste sistema é baseado na deteção e reconhecimento facial e também no envio de um código único, de quatro dígitos, de verificação através de uma aplicação externa *Twilio*. O sistema vai reconhecer os indivíduos que estiverem diante do local pré-estabelecido, neste caso da porta. Apenas os utilizadores certificados com os seus rostos registados na Base de Dados, vão receber o código de verificação, que após a sua introdução correta, no sistema, o mesmo faz com que o local seja acedido de imediato, neste caso que a porta seja aberta com sucesso. O *Raspberry Pi 4* tem conectado um display, para visualização de resultados e introdução do código de verificação e um *Servo Motor* que é responsável pela simulação da abertura e fecho da porta.

Palavras-Chave: Deteção e Reconhecimento Facial, Autenticação em Dois Passos, *Dlib*, *Histogram of Oriented Gradients,* Controlo de Acesso.

Abstract

This academic project aimed to develop a facial detection and recognition system to control access to a given location using Python programming language the OpenCv, Dlib, and Face_recognition libraries. This system uses the Raspberry Pi 4 microcomputer as a central processing unit. Facial detection and recognition systems for controlling access to a given location have been on the market for a long time, but they normally do not provide security-related features. The entire development of this system is based on facial detection and recognition and also on sending a unique four-digit verification code through an external Twilio application. The system will recognize individuals who are in front of the door. Only users who have the values that represent their faces registered in the Database will receive the verification code, which, after being correctly entered into the system, causes the door to be opened successfully. The Raspberry Pi 4 has a display connected to view results and enter the verification code and a Servo Motor that is responsible for simulating the opening and closing of the door.

Keywords: Face Detection and Recognition, Multi-Factor Authentication, Dlib, Histogram of Oriented Gradients, Access Control.

Índice

1. Introdução 1

2. Revisão de Literatura 2

3. Materiais e Métodos de Desenvolvimento 10

4. Resultados e Discussão de Resultados 18

4.1. Hardware 18

4.2. AccessFace Sentinel 34

4.3. Base de Dados 36

4.4. Biblioteca Dlib e face_recognition 43

4.5. Testes e validação 51

5. Conclusão 64

Bibliografia 66

Índice de Figuras

Figura 1 14
Figura 2 15
Figura 3 16
Figura 4 17
Figura 5 19
Figura 6 19
Figura 7 20
Figura 8 20
Figura 9 21
Figura 10 21
Figura 11 22
Figura 12 22
Figura 13 23
Figura 14 25
Figura 15 25
Figura 16 26
Figura 17 27
Figura 18 27
Figura 19 28
Figura 20 29
Figura 21 30
Figura 22 33
Figura 23 35
Figura 24 35
Figura 25 36
Figura 26 36
Figura 27 37
Figura 28 38
Figura 29 39
Figura 30 40
Figura 31 41
Figura 32 41
Figura 33 41
Figura 34 42
Figura 35 42
Figura 36 42
Figura 37 43
Figura 38 44
Figura 39 44
Figura 40 45
Figura 41 45
Figura 42 46
Figura 43 47
Figura 44 48
Figura 45 48
Figura 46 49

Figura 47 50
Figura 48 52
Figura 49 55
Figura 50 57
Figura 51 59
Figura 52 60

Índice de Tabelas

Tabela 1.....55
Tabela 2.....58
Tabela 3.....60
Tabela 4.....61
Tabela 5.....62

Abreviaturas

HOG – Histogram of Oriented Gradients

MFA – Multi-Factor Authentication

SMS – Short Message Service

PCA – Principal Component Analysis

LBP - Local Binary Pattern

2FA - Autenticação de Dois Fatores

CNN - Convolutional Neural Network

API - Application Programming Interfaces

LCD – Liquid Crystal Display

USB – Universal Serial Bus

GPIO - General Purpose Input/Output

1. Introdução

A maioria dos sistemas de deteção e reconhecimento facial que existem no mercado muitas vezes ainda não têm implementado funcionalidades relacionadas com segurança. Este estudo é baseado no desenvolvimento de um sistema de deteção e reconhecimento facial para acesso a um determinado local, utilizando a *Multi-Factor Authentication* (MFA) que vai permitir responder às necessidades da empresa abordada neste estudo. O desenvolvimento de um sistema de deteção e reconhecimento facial que respondesse a todas as necessidades existentes foi o desafio deste estudo. Ao abordar alguns dos elementos desta empresa, foi possível verificar o que existe atualmente implementado e o que a empresa realmente necessita.

Através da investigação foi possível verificar as necessidades existentes da empresa abordada assim como quais seriam as melhores tecnologias a serem utilizadas pelo sistema. Para tal, foram efetuadas entrevistas a alguns funcionários desta empresa assim como observações de campo que permitiram registar informação suficiente para que tornasse possível o desenvolvimento e implementação deste sistema.

Foi verificado junto da empresa abordada a inexistência de um sistema de controlo de acesso, que é exigido por lei. Como tal, surgiu a possibilidade do desenvolvimento de um sistema de deteção e reconhecimento facial que respondesse às necessidades atuais desta empresa.

A recolha de dados possibilitou avaliar as necessidades e o nível de urgência existentes para que fosse implementado um sistema de deteção e reconhecimento facial que tivesse em conta as diferentes condições, como a fraca iluminação do local, os utilizadores terem diferentes expressões faciais quando expostos ao sistema, os utilizadores utilizarem diferentes acessórios no rosto quando expostos ao sistema e os utilizadores necessitarem de verificar a sua autenticidade diante do sistema.

Nos próximos capítulos são descritos os passos mais importantes assim como os detalhes que levaram ao sucesso deste sistema, uma vez que foi possível responder a um conjunto de necessidades identificadas no início desta investigação.

2. Revisão de Literatura

Qualquer pessoa pode ser reconhecida e a sua identificação verificada ao utilizar autenticação biométrica ou a tecnicamente o reconhecimento de características faciais com base nas características do rosto. A única preocupação a ter em conta foi o cumprimento estrito das regras de privacidade e proteção de dados pessoais (EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex. (2016). Regulamento (UE) 2016/679 Do Parlamento Europeu e Do Conselho, de 27 de Abril de 2016, Relativo à Proteção Das Pessoas Singulares No Que Diz Respeito Ao Tratamento de Dados Pessoais e à Livre Circulação Desses Dados e Que Revoga a Diretiva 95/46/CE (Regulamento Geral Sobre a Proteção de Dados)., 2016).

As pessoas identificam-se e expressam-se através dos seus rostos. Os rostos são a forma mais natural de um sistema de reconhecimento biométrico. A deteção facial funciona através do reconhecimento e da verificação de uma pessoa utilizando o seu rosto, detetando os pontos faciais em faces distintas e com câmaras, com poder computacional, em tempo real (Datta et al., 2015).

O reconhecimento facial tornou-se amplamente utilizado em muitos setores diferentes, incluindo segurança e vigilância, forças de segurança e verificação da identidade digital. Atualmente, existem várias abordagens disponíveis utilizadas no reconhecimento de características faciais devido aos tremendos avanços feitos nos algoritmos de reconhecimento facial nos últimos anos. No entanto, o reconhecimento facial ainda tem muitas barreiras para superar, como a iluminação inconsistente, obstáculos, fraudes e problemas de compatibilidade entre diversos componentes. O estudo de Ali et Al. (2020), vem revelar dados significativos, pois investiga o reconhecimento facial, concentrando-se naquilo que chamam de melhores métodos para o seu uso, em circunstâncias em que as condições de um determinado ambiente têm, como uma iluminação inconsistente entre outros desafios (Ali et Al., 2020). Os mesmos autores também têm em conta precauções de segurança como a autenticação de dois fatores para evitar ataques relacionados com o roubo de identidade, a praticidade e facilidade de uso do algoritmo em vários dispositivos, como *smartphones* e camaras de videovigilância e como o mesmo pode ser utilizado em diferentes áreas.

Nas últimas décadas, outro estudo de Li & Jain (2004) mostra que a tecnologia de reconhecimento facial melhorou de modo exponencial e cresceu em popularidade numa variedade de aplicações, incluindo sistemas de segurança, monitorização e identificação em dispositivos privados (Li & Jain, 2004).

Os sistemas de deteção e reconhecimento facial capturam detalhes faciais de uma imagem digital ou de um vídeo e analisam padrões nas imagens que correspondem às medições existentes na base de dados. A deteção e reconhecimento facial funciona através de um processo que envolve a deteção do rosto, a localização de coordenadas no rosto, a geração de valores que representam o rosto e a correspondência desses valores face aos existentes e registados na base dados. A deteção facial e o reconhecimento facial são utilizados de forma bidirecional, mas o reconhecimento facial é uma aplicação da deteção facial. O reconhecimento facial é a identificação de uma pessoa utilizando detalhes faciais por meio de software e hardware. O reconhecimento facial é um dos usos e aplicações dos sistemas e tecnologia de deteção facial.

É fundamental avaliar as melhores estratégias e táticas para um sistema de reconhecimento facial, bem como a sua viabilidade em vários contextos. Para fornecer uma melhor compreensão do assunto, foi possível analisar alguns dos desenvolvimentos atuais nesta área tendo como base diversos projetos de pesquisa. Além disso, tenta oferecer uma abordagem diferenciada, aliada a uma maior consciência do que é possível efetuar com o reconhecimento facial usado como uma ferramenta, de forma a poder ser maximizada para vários propósitos.

Como tal, serão abordadas quatro questões importantes que servirão de pontos de partida para esta reflexão:

- Qual é a técnica de reconhecimento facial para usar em ambientes com condições de iluminação variáveis e presença de obstáculos?
- Como é que as medidas de segurança, como autenticação múltipla, podem ser implementadas para proteger contra-ataques de roubo de identidade?
- Qual a aplicabilidade do algoritmo em diferentes dispositivos como Smartphones, câmaras de vigilância e microcomputadores?
- Qual a aplicabilidade do algoritmo noutras áreas como o reconhecimento de expressões faciais ou reconhecimento de indivíduos com diferentes características faciais?

Relativamente à técnica de reconhecimento facial para usar em ambientes com condições de iluminação variáveis e presença de obstáculos foi possível verificar que as diversas fontes divergem, quanto à forma dinâmica de abordar o projeto. Conforme o relatório 'An efficient method for face recognition under varying illumination', o reconhecimento eficiente de sistemas de reconhecimento facial requer imagens nítidas e confiáveis. No entanto, em circunstâncias quotidianas, a iluminação pode variar bastante e os objetos podem bloquear a perspetiva do sistema de reconhecimento facial, dificultando a captura de fotografias precisas e necessárias para a identificação facial (Xie & Lam, 2005).

Para lidar com estes problemas, vários métodos foram criados. O reconhecimento através da múltipla visualização de rostos é um método que utiliza várias fotografias do rosto de uma pessoa para aumentar a precisão da identificação. Para simplificar a identificação das características faciais, a padronização da iluminação é outro método diferente que envolve a alteração da tonalidade e da saturação de uma imagem (Liu et Al., 2021).

Com estes métodos, foram aplicados diferentes algoritmos para aumentar a precisão do reconhecimento facial quando há obstáculos e condições adversas de iluminação.

Convolutional Neural Network (CNN) é um algoritmo baseado em *Machine Learning* que tem sido utilizado para adquirir conhecimento e detetar características faciais em fotografias expostas a várias circunstâncias de iluminação ou diferentes tipos de obstáculos (Alzubaidi et Al., 2021).

O *Local Binary Pattern* (LBP), é descritor de características que demonstrou ter sucesso em identificar rostos mesmo com condições de iluminação fraca (Rathgeb et Al., 2023).

O método de reconhecimento visual *Histogram of Oriented Gradients* (HOG) é outro descritor de características que funciona através do cálculo do gradiente de uma imagem, utilizando diferentes direções para representar visualmente o gradiente. O algoritmo *Histogram of Oriented Gradients* (HOG) é frequentemente utilizado em sistemas que envolvem o reconhecimento de objetos, reconhecimento facial e a deteção de perdestes. A representação é eficaz na identificação de objetos em imagens com diferentes níveis de iluminação e é robusta na identificação de obstáculos parciais e totais (Julina & Sharmila, 2017).

Para enfatizar o referido anteriormente, de acordo com (Kapse et Al, 2022, p.3), "the HOG (Histogram of Oriented Gradient) is a feature descriptor used in machine vision for processing of digital images for the purpose of detecting objects. HOG is extensively known for their use

in the detection of moving objects.". O *Histogram of Oriented Gradients* analisa a porção localizada de uma imagem quantificando as ocorrências da orientação e magnitude do gradiente (Kapse et Al., 2022).

De acordo com (Patil & Shinde, 2020), esta técnica compartilha semelhanças com a *Edge Orientation Histograms* e *Scale Invariant Feature Transformation*. No entanto, o descritor *Histogram of Oriented Gradients* (HOG) enfatiza explicitamente a estrutura e a forma de um objeto. Este descritor supera os descritores de contorno através da incorporação da magnitude e do ângulo do gradiente para calcular as características de um rosto. Ao gerar histogramas com base na magnitude e nas orientações do gradiente para diferentes localizações da imagem, o *Histogram of Oriented Gradients* captura com eficiência as informações relevantes.

Verificou-se que o *Histogram of Oriented Gradients* (HOG) tem sido amplamente utilizado e eficaz na deteção de visão computacional que consiste na utilização do algoritmo para identificar e localizar objetos em vídeos ou imagens. Ele é utilizado regularmente em sistemas de deteção e reconhecimento facial porque captura e representa as características estruturais faciais e os seus pontos de referência. O propósito do *Histogram of Oriented Gradients* na deteção facial para controlar o acesso a um determinado local, é a extração de caraterísticas de imagens que são utilizadas para identificar e localizar rostos de forma assertiva.

Através do estudo 'Reconhecimento facial baseado em HOG e PCA: Uma comparação quanto à invariância à iluminação' os autores verificaram a eficácia de diferentes algoritmos, quando existe uma variação de iluminação. Neste estudo foram utilizados três diferentes algoritmos: *Principal Component Analysis* (PCA), *Histogram of Oriented Gradients* (HOG) e *Histogram of Oriented Gradients* (HOG) + *Principal Component Analysis* (PCA). Após serem efetuadas vários testes diferentes, verificou-se que o algoritmo que apresentava a maior taxa de acerto e que ao mesmo tempo apresentava a menor variação na percentagem de acertos era o HOG. "Notadamente, o Histograma de Orientação de Gradiente possibilitou uma extração de características mais focada nos contornos da face e, com os testes realizados, mostrou-se que o método é mais robusto quando comparado com o método Eigenface (PCA simples)" (Panceri et Al., 2015, p.59).

O algoritmo HOG é apenas uma das técnicas de visão computacional disponíveis e a escolha da utilização de qualquer técnica depende da aplicação específica e dos requisitos existentes.

De acordo com os autores consultados, todos estes algoritmos mostraram-se eficazes para aumentar a precisão do reconhecimento e identificação facial em ambientes com condições de iluminação variáveis, mas a vantagem critica do *Histogram of Oriented Gradients* na deteção de rostos é a capacidade de capturar e apresentar informações das formas e texturas da imagem. Através da análise da distribuição da orientação dos gradientes, o *Histogram of Oriented Gradients* distingue eficazmente rostos de outros objetos numa imagem, mesmo com condições de iluminação adversas, diferentes expressões faciais e posições. Outra grande vantagem do *Histogram of Oriented Gradients* é que o mesmo é altamente eficaz em sistemas de deteção e reconhecimento facial instalados em microcomputadores com um grande limite de processamento, como é o *Raspberry Pi 4* utilizado no projeto desenvolvido, ao contrário do *Convolutional Neural Network*, também conhecido como *CNN* que necessita de um grande poder de processamento para funcionar de forma eficaz.

A biblioteca *Dlib* em conjunto com a biblioteca *face_recognition* oferecem uma solução clàssica para a deteção e reconhecimento facial utilizando a técnica *Histogram of Oriented Gradients* (HOG).

Para verificar que medidas de segurança podem ser implementadas num sistema de deteção e reconhecimento facial para o proteger contra-ataques de roubo de identidade foi possível verificar, através das fontes, que existem várias medidas que podem ser utilizadas.

O uso do reconhecimento facial é suscetível a ataques de roubo de identidade digital, nos quais um indivíduo tenta entrar num dispositivo ou num determinado local utilizando uma fotografia, ou vídeo falso de outro indivíduo. É possível ter um sistema de reconhecimento facial protegido contra estes ataques, através da implementação de vários procedimentos de autenticação. De acordo com Paul e Aslan (2021) uma técnica específica é a deteção de vitalidade, que envolve um sistema certificar-se de que o individuo que está a ser reconhecido existe e não é apenas uma imagem estática ou um vídeo (Paul & Aslan, 2021). Várias técnicas podem ser utilizadas para determinar se existe vitalidade, incluindo a identificação do piscar de olhos, movimento da cabeça, solicitar ao utilizador que execute uma determinada atividade, entre outros.

Outra técnica de verificação é a utilização de vários fatores fisiológicos, como a fusão do reconhecimento de voz com a leitura de impressão digital ou reconhecimento de características faciais. O uso desta técnica melhora a segurança do sistema de reconhecimento facial e diminui a probabilidade de roubo ou ataques de identidade. O uso de criptografia e

protocolos de segurança para a interação com o sistema também pode ajudar a evitar violações de informações e a entrada indesejada no sistema.

O uso de algoritmos para o reconhecimento facial numa variedade de dispositivos, incluindo smartphones e câmaras de vigilância, tem crescido bastante. A capacidade de reconhecimento facial tem sido usada numa variedade de plataformas, incluindo dispositivos móveis, câmaras e máquinas, com graus variados de sucesso, como reportado por (Kumar et al., 2018), os smartphones podem usar o algoritmo para permitir que os utilizadores protejam os seus dispositivos utilizando rostos reconhecidos. Por outro lado, as imagens de vigilância podem identificar criminosos suspeitos ou pessoas ilegais em locais restritos usando tecnologia de reconhecimento facial. No entanto, fatores como qualidade da imagem, velocidade de processamento e iluminação ambiente afetam a precisão dos diferentes algoritmos em vários dispositivos. Por isso, ao utilizar tecnologias de reconhecimento facial, é fundamental considerar as especificações técnicas do dispositivo.

Os algoritmos de reconhecimento facial, podem adicionar um grau extra de proteção ao reconhecer pessoas instantaneamente, e os dispositivos de gravação, como as câmaras de vigilância, são frequentemente utilizados em operações de proteção e rastreamento. No entanto, as variáveis nos diferentes ambientes que afetam as câmaras de segurança, como a mudança de iluminação e a existência de obstáculos, podem afetar a exatidão e a confiabilidade do algoritmo. Portanto, é crucial avaliar o desempenho dos algoritmos de reconhecimento facial em vários modelos de câmaras de vigilância, considerando as condições e a qualidade geral da imagem.

De acordo com Shetty et Al (2013, p.1112) outra medida de segurança é a "Two-factor authentication is a security process in which the user provides two means of identification, one of which is a physical token or biometric identification, and the other is the one that can be easily memorized, such as a security code or password." O sistema *Two-Factor Authentication* 2FA ou *Multi Factor Authentication* (MFA), é um sistema de autenticação robusto e seguro, uma vez que o individuo tem de se autenticar duas vezes e de formas diferentes para conseguir ter acesso ao sistema. "This system can be used in the places where high degree of security is needed such as banks, lockers, colleges and government organizations.".

A autenticação após o reconhecimento bem-sucedido adiciona características essenciais que garantem que a pessoa possa confirmar se o sistema está correto. Conforme Vimal (2022), na área de segurança, a autenticação é uma camada adicional de segurança, enquanto no desenvolvimento de tecnologia, a autenticação é um método que promove o Machine Learning e também a oportunidade de criar sistemas mais sofisticados (Vimal, 2022).

Relativamente à aplicabilidade do algoritmo em diferentes dispositivos como Smartphones, câmaras de vigilância e microcomputadores foi possível verificar diferentes abordagens entre as diferentes fontes.

O relatório 'A comparative study of facial recognition techniques With focus on low computational power.' de (Schenkel et al., 2019), que tem como objetivo realizar um estudo comparativo de técnicas de reconhecimento facial mostra que os *smartphones*, câmaras de segurança, entre outros dispositivos são apenas alguns dos gadgets que incorporam tecnologia de reconhecimento facial. As características dos gadgets e a qualidade da imagem da câmara, podem ter um impacto sobre o sucesso dos diferentes métodos. A precisão e a rapidez do sistema de identificação e reconhecimento facial, por exemplo, podem ser afetadas por fatores como a resolução do sensor e o poder de computação. A precisão do método pode ser afetada pelos fracos recursos de certos telefones e de certas câmaras de segurança em comparação com dispositivos de reconhecimento facial especializados.

No geral, um sistema de reconhecimento facial tem múltiplas aplicações e está a crescer em termos de aceitação numa variedade de contextos. Para melhorar a sua confiabilidade e eficácia, especialmente em áreas com iluminação variável e obstáculos, várias barreiras científicas devem ser resolvidas. Investigações mais recentes têm vindo a concentrar-se na criação de sistemas mais complexos que possam corrigir este tipo de problemas. Por exemplo, alguns estudos analisaram a aplicação de métodos de *Machine Learning*, que podem aumentar a precisão e a confiabilidade em circunstâncias desafiadoras. Outras pesquisas concentraram-se no uso de inúmeras câmaras ou scanners para fotografar o rosto de várias perspetivas, o que pode ajudar a superar desafios e a aumentar a taxa de reconhecimento.

Os *Smartphones* são dispositivos práticos e amplamente utilizados que fazem agora parte da vida quotidiana de toda a população. Como resultado, existe uma necessidade de criar sistemas de reconhecimento facial que possam ser utilizados de diferentes formas nos smartphones. As capacidades de processamento e memória destes dispositivos são um dos maiores obstáculos para a implementação deste tipo de técnicas. Além disso, a câmara e as capacidades computacionais dos vários dispositivos existentes no mercado variam, o que faz com que exista a possibilidade da eficácia dos diferentes métodos seja afetada. Portanto, é crucial avaliar o comportamento dos algoritmos de reconhecimento facial em vários modelos de smartphone, tendo em conta os requisitos de software e hardware.

Com base no relatório 'Face Recognition in Low Quality Images: A Survey.' da Universidade de Notre Dame, os algoritmos de reconhecimento facial, podem adicionar um grau extra de proteção ao reconhecer instantaneamente as pessoas, e os dispositivos de

gravação, como as câmaras de vigilância, são frequentemente utilizados em operações de proteção e rastreamento (Flynn et Al., 2019).

No entanto, existem condições adversas que podem afetar as câmaras de vigilância, como a mudança de iluminação constante e a existência de obstáculos, que podem afetar a exatidão e a confiabilidade dos diferentes métodos. Portanto, é crucial avaliar o desempenho dos métodos de reconhecimento facial em vários modelos de câmaras de vigilância, considerando as condições existentes e a qualidade geral da imagem.

Relativamente à aplicabilidade do algoritmo noutras áreas como o reconhecimento de expressões faciais ou o reconhecimento de indivíduos com diferentes características foi possível verificar, através das fontes, que o *Histogram of Oriented Gradients* (HOG) seria uma boa opção para ser utilizada no sistema de deteção e reconhecimento facial.

A capacidade da tecnologia de reconhecimento facial para identificar pessoas e reconhecer os seus vários traços faciais e emoções tem se mostrado promissora, o que levou a que fossem criadas grande variedade de oportunidades para a sua utilização em vários setores, como a assistência médica, segurança, entre outros.

Na área da medicina, o reconhecimento facial tem sido utilizado para identificar expressões faciais e sentimentos em indivíduos que sofrem de doenças mentais como a depressão, a psicose e a ansiedade. Os profissionais de saúde podem detetar e tratar com mais precisão certas doenças observando como o comportamento das pessoas. Por exemplo, um estudo da Universidade de Pittsburgh indicou que a tecnologia de reconhecimento facial tinha uma taxa de precisão de 80% para identificar a melancolia entre os participantes com base nas suas expressões (Vemou & Horvath, 2020).

A tecnologia de reconhecimento facial tem sido utilizada na área da segurança para reconhecer pessoas com vários traços faciais, como pelos faciais, óculos e máscaras, este último com mais importância desde o início da pandemia de Covid-19, onde as máscaras para tapar o nariz e a boca proliferaram. Como tal, é possível um sistema de reconhecimento facial, reconhecer pessoas que utilizam máscaras através da análise a uma parte específica do rosto.

No geral, a tecnologia de reconhecimento facial tem uma ampla gama de possíveis aplicações na compreensão e identificação das emoções, bem como no reconhecimento de pessoas com vários traços faciais. É concebível que, à medida que a tecnologia se desenvolve, ela encontre utilizações novas numa variedade de indústrias. As ramificações éticas da sua utilização, como preocupações com a privacidade e possíveis prejuízos na sua utilização, devem ser consideradas. Sistemas de reconhecimento facial têm sido aplicados no setor do

entretenimento para produzir representações digitais e realistas de pessoas. Isto tem sido utilizado para gerar criaturas realistas, em filmes e vídeo jogos, com origens em pessoas reais (Adjabi et Al., 2020). Por exemplo, no filme *Avatar*, um sistema de reconhecimento facial foi utilizado para registar as reações dos atores e das atrizes e aplicá-las aos personagens produzidos via computador.

No estudo 'Facial Expression Recognition Based on Facial Components Detection and HOG Features' os autores investigaram a eficácia no reconhecimento de expressões faciais através do algoritmo *Histogram of Oriented Gradients* (HOG) que foi escolhido por ser bastante sensível a deformações de objetos. De acordo com (Chen et Al., 2014, p.65) "Facial expressions result from muscle movements and these movements could be regarded as a kind of deformation. For example, the muscle movements of the mouth cause the mouth open or close, and cause brows raiser or lower.". Neste estudo, o algoritmo *Histogram of Oriented Gradients* (HOG) foi aplicado em duas bases de dados de imagens diferentes, JAFFE e Cohn-Kanade, e a performance do mesmo foi bastante positiva com uma taxa de sucesso de 94.3% e 88.7%, respetivamente.

No sentido de esclarecer detalhadamente o modo como se operacionalizou a deteção facial no desenvolvimento da aplicação, foi efetuado o levantamento de requisitos e escolhidos os instrumentos de dados, referidos nos Materiais e Métodos de Desenvolvimento.

Foi desenvolvido um sistema de deteção e reconhecimento facial para controlo de acesso a um determinado local em linguagem *Python* utilizando a técnica *Histogram of Oriented Gradients (HOG)* através da biblioteca *Dlib* que tem integrada uma outra biblioteca chamada *face_recognition* que contem funcionalidades relacionadas com a deteção e reconhecimento facial. Outras bibliotecas foram utilizadas durante o desenvolvimento deste projeto, como a *OpenCV* para o processamento de imagem e apresentação da mesma e também a biblioteca time para operações relacionadas com tempos.

3. Materiais e Métodos de Desenvolvimento

Este capítulo descreve a metodologia de investigação utilizada, os materiais necessários, os procedimentos envolvidos no sistema, o software e a tecnologia necessária e utilizada, assim como os procedimentos utilizados em todo o processo. Resumindo, este capítulo tem como objetivo descrever qual foi o método de pesquisa utilizado, como se

procedeu à recolha de dados e a posterior análise, interpretação e considerações éticas dos mesmos

O estudo utiliza uma abordagem de pesquisa qualitativa e descritiva através de um procedimento de Participante Investigação-Ação. Uma abordagem qualitativa permite ao pesquisador explorar os temas de uma forma fácil e ampla, que não necessita de referências estatísticas para extrair, analisar e reportar resultados. O tema em estudo é também um campo que pode ser explorado qualitativamente. A abordagem qualitativa captura tendências e desenvolvimento em sistemas de deteção e reconhecimento facial, flexibilidade, expectativas, qualidades e detalhes (Elliott & Timulak, 2021). Por outro lado, a abordagem descritiva identifica características, categorias e tendências. A abordagem descritiva permite a observação qualitativa. A maneira mais eficiente de fazer esta pesquisa é por observação, e os pesquisadores utilizam observações qualitativas. A monitorização dos resultados, em diferentes pessoas, num sistema de deteção e reconhecimento facial é necessário para a observação qualitativa, excluindo medições e números. Nesse caso, o pesquisador mantém distância do sistema operacional enquanto observa as suas configurações. As qualidades vistas são naturais e eficientes porque o sistema de deteção e identificação facial está num ambiente natural. Num projeto de pesquisa descritivo, o pesquisador pode optar por ser um participante pleno, um participante como observador, um observador como participante ou um observador pleno. Por exemplo, um pesquisador pode observar e acompanhar a atividade de um sistema de deteção e reconhecimento facial com o objetivo de controlar o acesso a um escritório que é concedido através da deteção e do reconhecimento facial, à distância.

De acordo com (Bogdan & Biklen, 1994, 293), "A investigação-acção é um tipo de investigação aplicada no qual o investigador se envolve activamente na causa da investigação", e como objetivo melhorar a qualidade da investigação que está a ser desenvolvida. Neste tipo de investigação, quem investiga deve inserir-se ao máximo no meio daqueles que pretende estudar, recolhendo, através de vários instrumentos, tudo aquilo o que considera relevante para o seu estudo.

A observação participante foi o método de recolha de dados mais utilizado durante a realização deste estudo e ao longo de todo o processo. Este método é referido por vários autores como sendo uma das abordagens para a recolha de dados mais utilizadas nas investigações que utilizam uma abordagem qualitativa e descritiva.

De acordo com (Queiroz et Al., 2007, p.278) a observação participante "consiste na inserção do pesquisador no interior do grupo observado, tornando-se parte dele, interagindo

por longos períodos com os sujeitos, buscando partilhar o seu quotidiano para sentir o que significa estar naquela situação".

Este método foi utilizado desde a fase inicial do desenvolvimento deste estudo até à fase final do mesmo, mas nunca da mesma forma. Numa fase inicial o método de observação participante foi utilizado para selecionar o local de instalação do sistema de deteção e reconhecimento facial e para estabelecer uma relação com os participantes, numa fase intermédia, o pesquisador teve uma observação participante que permitiu recolher dados e analisar o progresso do seu projeto e já numa fase final o pesquisador participou ativamente em toda a fase de testes do projeto desenvolvido, ou seja um sistema de deteção e reconhecimento facial para controlo de acesso a um determinado local. A recolha documental é outro método utilizado numa abordagem qualitativa, mas também diferente, devido ao próprio pesquisador não ter um papel principal e tão ativo.

De acordo com (Bell, 1993) existem dois possíveis documentos a serem recolhidos dependendo da sua natureza, existindo os documentos de fontes primária e os de fontes secundária. Segundo a autora, os documentos recolhidos são classificados como documentos de fontes secundárias, porque são documentos existentes e anteriores à realização deste estudo.

A entrevista foi outra técnica utilizada neste estudo e segundo (Natércio, 2005, p.97) "A realização de entrevistas constitui uma das técnicas de recolha mais frequentes na investigação naturalista, e consiste numa interação verbal entre o entrevistador e o respondente, em situação de face a face ou intermédio do telefone."

As entrevistas foram realizadas presencialmente ou online, através de uma plataforma digital com base num grupo de questões já preparadas previamente às entrevistas, o que ajudará durante a realização das mesmas. Este grupo de questões previamente elaborado são também referidos, por outros autores, como sendo "guiões de entrevista".

Segundo (Natércio, 2005, p.99) este tipo de guiões:

> deve ser constituído a partir das questões de pesquisa e eixos de análise do projeto de investigação. A sua estrutura típica tem um carácter matricial, em que a substância da entrevista é organizada por objetivos, questões e itens ou tópicos. A cada objetivo corresponde uma ou mais

questões. A cada questão correspondem vários itens ou tópicos que serão utilizados na gestão do discurso do entrevistado em relação a cada pergunta.

Todas as entrevistas foram anotadas e guardadas em formato digital. Uma vez que as entrevistas realizadas permitem que exista mais liberdade nas respostas dos entrevistados, as mesmas são definidas como sendo entrevistas exploratórias não-diretivas que têm como objetivo fazer com que, através das respostas dos entrevistados, o pesquisador possa ganhar uma perspetiva diferente em relação à qual tem na atualidade.

Numa fase inicial, a observação participante, foi utilizada para realizar o levantamento de requisitos e analisar o local de implementação do sistema de identificação e reconhecimento facial onde foi possível verificar que existem condições de iluminação adversas e que não existe, atualmente, qualquer sistema de controlo de acesso. Além disso o pesquisador teve o primeiro contacto com os participantes, que confirmaram que atualmente não existe nenhum sistema de controlo de acesso implementado. Numa segunda fase, o desenvolvimento do software já estava a decorrer e foi possível ao pesquisador montar o sistema de identificação e reconhecimento facial no local da implementação do mesmo e efetuar alguns testes de acordo com a variação de iluminação, com diferentes expressões faciais e com diferentes indivíduos.

A recolha documental teve como objetivo analisar os diferentes estudos existentes e dessa forma auxiliar o pesquisador na escolha do Software, Hardware, abordagem do projeto, metodologia do projeto, recolha e tratamento dos dados.

O Pesquisador realizou duas entrevistas, uma na fase inicial com o objetivo de realizar um levantamento de requerimentos e outra após a implementação do sistema de identificação e reconhecimento facial, com o objetivo de perceber junto dos elementos se responde à necessidade identificada durante a entrevista inicial.

A análise dos dados recolhidos ocorreu de diversas formas, em relação aos dados recolhidos através da observação participante, os mesmos foram reunidos e posteriormente identificados os pontos chave desta observação que teve como principal ponto comum a identificação da falta de segurança existente hoje em dia, devido ao facto do local não ter nenhum sistema de controlo de acesso, atualmente em vigor. A análise dos dados recolhidos através das entrevistas teve como principal objetivo, no início do projeto efetuar o levantamento de requerimentos e no final avaliar, junto dos utilizadores, se o sistema implementado respondia às necessidades existentes. Para tal, com base nas respostas de três

elementos, foi possível criar uma nuvem de palavras, através de uma aplicação externa MAXQDA, que ajudaram a identificar as necessidades:

Figura 1 - Nuvem de Palavras que identificou o tema (Garcia, 2023, p.1).

Foi então identificada a preocupação atual e a necessidade de implementar um sistema de deteção e reconhecimento facial para acesso a um determinado local, com verificação em dois passos para responder a questões relacionadas com segurança, como o roubo de identidade.

A privacidade e o consentimento foram garantidos na recolha e utilização dos dados faciais e foram observados os princípios éticos, ou seja, foi garantida a proteção dos dados faciais dos indivíduos e também assegurado que quaisquer dados pessoais, não foram utilizados de forma indevida. O pesquisador seguiu as leis de privacidade e obteve a aprovação necessária de todos os envolvidos de forma explicita, de forma a garantir que os envolvidos estavam corretamente informados e que concordavam, com a recolha de dados efetuada.

O local escolhido para a implementação do sistema de identificação e reconhecimento facial foi dentro de um edifício, na porta de acesso a um departamento de uma determinada empresa, localizado em Lisboa, Portugal. Foram escolhidos 3 participantes, entre os 15 elementos do departamento, de forma aleatória.

Na imagem abaixo, é possível visualizar o cronograma de todo o projeto académico em questão. O cronograma presente na Tabela 1 foi sendo adaptado ao longo da elaboração do projeto académico, proposto e aceite, uma vez que alguns fatores externos influenciaram a extensão do tempo de algumas das tarefas, como por exemplo a montagem do sistema no microcomputador *Raspberry Pi 4*:

Tarefas	**Meses**								
	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro
Elaboração do Pré-projeto									
Entrega do Pré-projeto									
Elaboração da Revisão de Literatura									
Recolha e análise dos dados									
Desenvolvimento do sistema de deteção e reconhecimento facial									
Montagem do sistema de deteção e reconhecimento facial no Raspberry Pi 4									
Testes e análise dos resultados									
Redação da versão final do projeto académico									
Entrega da versão final do Projeto académico									

Figura 2 - Cronograma da Investigação (Garcia, 2023, p.2)

No fluxograma abaixo, podemos verificar a arquitetura do código que corresponde ao design da investigação relativo ao registo de um utilizador no sistema de deteção e reconhecimento facial:

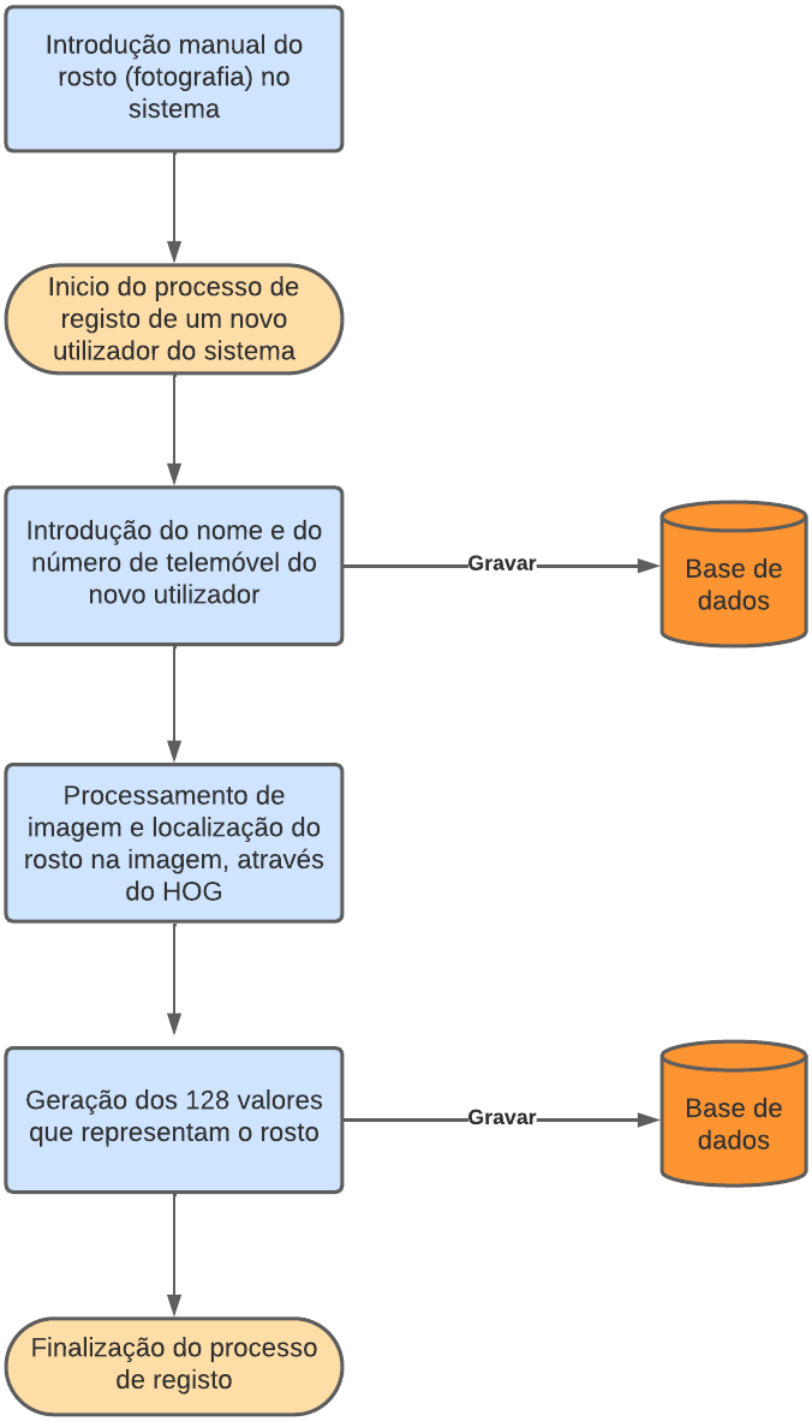


Figura 3 - Arquitetura de Código - Registo Utilizador (Garcia, 2023, p.4)

No fluxograma abaixo, podemos observar a arquitetura completa do sistema:

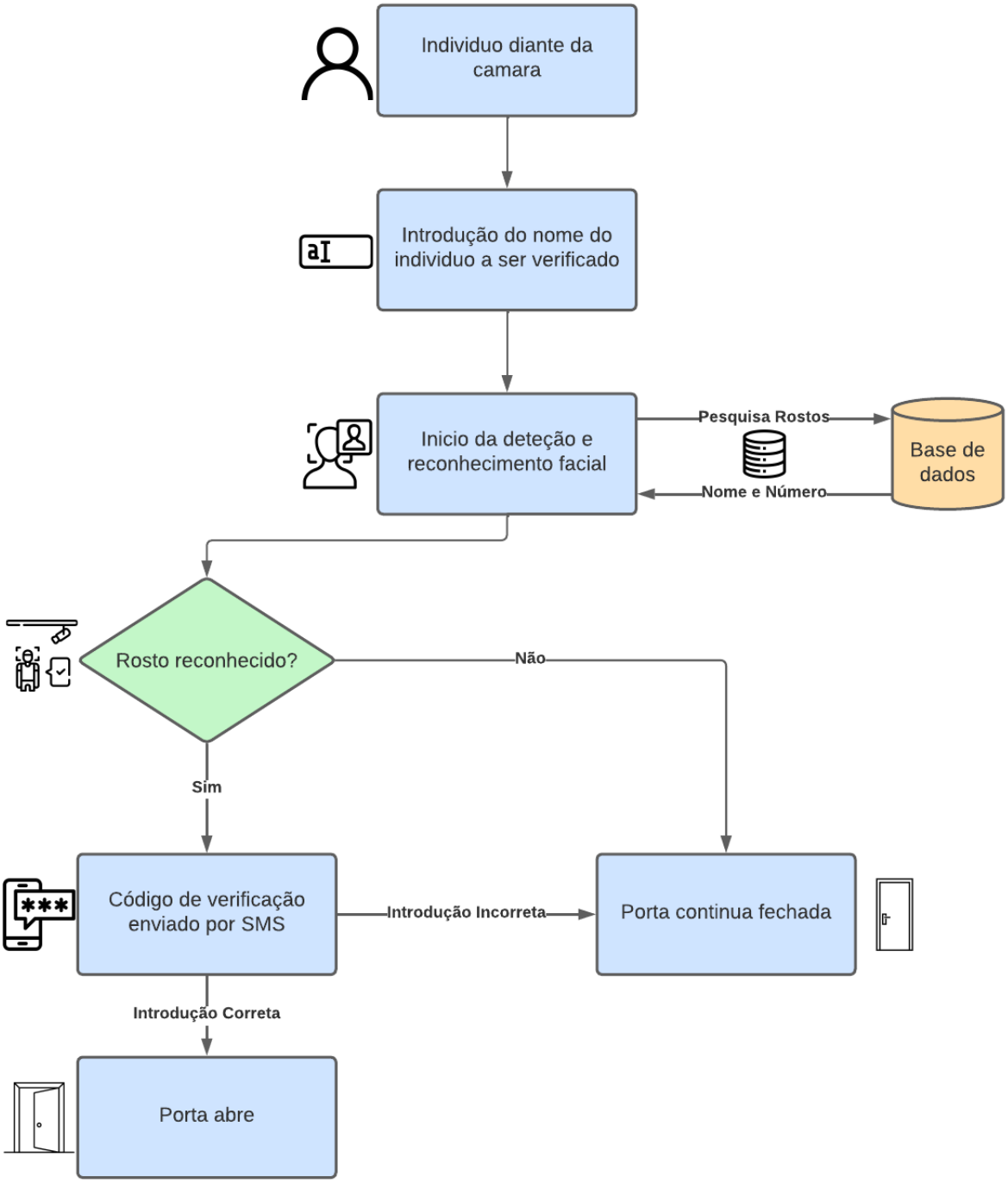


Figura 4 - Arquitetura Completa Do Sistema (Garcia, 2023, p.6)

4. Resultados e Discussão de Resultados

Neste capítulo, foi possível verificar os resultados obtidos durante e após o desenvolvimento do sistema de deteção e reconhecimento facial, de forma a ser possível verificar as diferentes fases de desenvolvimento, como foi desenvolvido e analisar a performance e a precisão do sistema.

4.1. Hardware

Os sistemas de deteção e reconhecimento facial para controlo de acesso a um determinado local dependem fortemente de hardware. O desempenho e a qualidade de construção do hardware afetam diretamente a precisão e a performance do sistema. Câmaras, sensores de imagem e movimento, processadores, memória, redes, fontes de alimentação e motores de porta utilizados para simular o funcionamento de uma porta são exemplos de hardware. Peças de hardware adicionais são necessárias para um sistema de deteção e reconhecimento facial para acesso a um determinado local. As peças consistem num Servo Motor para a simulação de uma porta eletrónica e conectores que conectam fisicamente a tecnologia de reconhecimento facial ao motor de porta eletrónico utilizado para simular a abertura e fecho de uma porta. O hardware fez com que o controlo de acesso fosse efetuado com segurança com base nos rostos identificados e reconhecidos pelo sistema desenvolvido.

O *Raspberry Pi 4* é um pequeno computador que neste caso foi utilizado num sistema de controlo de acesso a um determinado local com deteção e reconhecimento facial. O *Raspberry Pi 4* serve como unidade central de processamento e oferece uma variedade de recursos para sistemas de deteção e reconhecimento facial (Syafeeza et al., 2020). Todo o código desenvolvido para o sistema de deteção e reconhecimento facial é executado no *Raspberry Pi 4* graças à sua capacidade de processamento. O *Display* e o motor de porta eletrónico foram utilizados devido ao *Raspberry Pi 4* ter portas *GPIO* disponíveis. Para a deteção e reconhecimento facial em tempo real foi utilizada uma *Webcam*. As imagens são processadas através do módulo responsável pela *Webcam* que está conectada ao *Raspberry Pi 4* através de uma ligação *USB*.

O sistema de deteção e reconhecimento facial para acesso a um determinado local é controlado centralmente pelo *Raspberry Pi 4* que permite uma correta integração e controlo do sistema. Para o controlo de acesso, é utilizado um *Servo Motor* que recebe sinais consoante o resultado da deteção e reconhecimento do rosto. O *Raspberry Pi 4* está também conectado a um *LCD* que permite ao utilizador visualizar resultados e interagir com o sistema através de um teclado virtual ou periféricos como um teclado ou um rato físico.

A conexão *Wi-Fi* no *Raspberry Pi 4* permite rede e comunicação que foi útil durante o desenvolvimento do projeto e posteriormente ao desenvolvimento do projeto estar concluído, para aceder remotamente ao mesmo. O *Raspberry Pi* foi escolhido por se tratar de um pequeno computador, ser facilmente utilizado, ser extensível e adaptável às necessidades existentes, pelo seu preço e também pelo suporte existente por parte da comunidade. Como resultado, o sistema de acesso por porta com proteção facial pode ser dimensionado e personalizado para atender a diferentes necessidades (Kapse et al., 2022).

Figura 5 - Raspberry Pi 4 (Farnell, n.d.)

Figura 6 - Lenovo Webcam 510 FHD (Lenovo 510 FHD, n.d.)

Para configurar a utilização da *Webcam USB* através do *Raspberry Pi 4* foi necessário habilitar a interface da camara através das opções de configurações do *Raspberry Pi 4*:

1. Abrir o terminal:

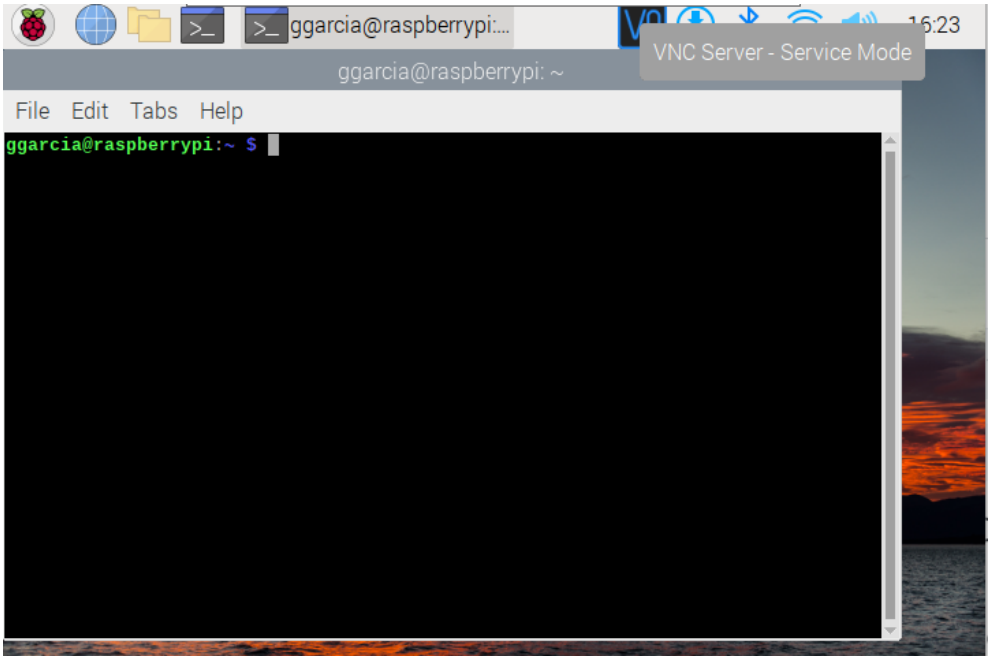


Figura 7 - Abrir o terminal (Garcia, 2023, p.16)

2. Execução do comando "*sudo raspi-config*":

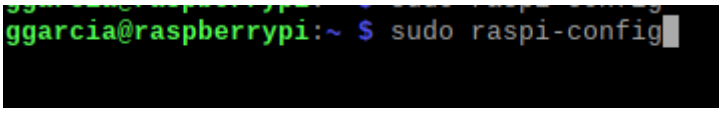


Figura 8 - Execução comando "sudo raspi-config" (Garcia, 2023, p.16)

3. Selecionar a opção “*Interface Options*”:

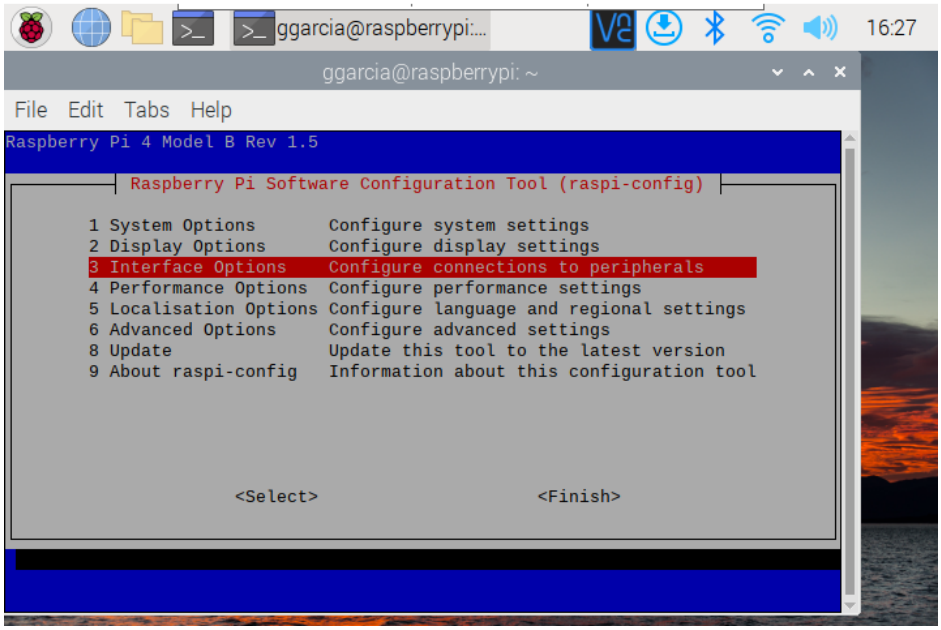


Figura 9 - Selecionar opção "Interface Options" (Garcia, 2023, p.16)

4. Selecionar a opção “*Legacy Camera*”:

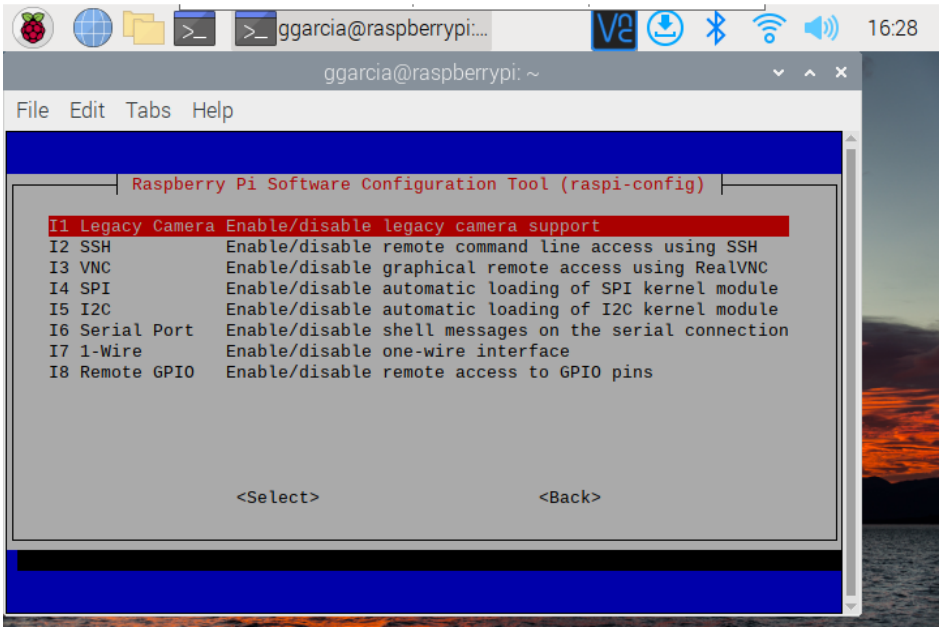


Figura 10 - Selecionar opção "Legacy Camera" (Garcia, 2023, p.17)

5. Habilitar através da seleção da opção “*Yes*”:

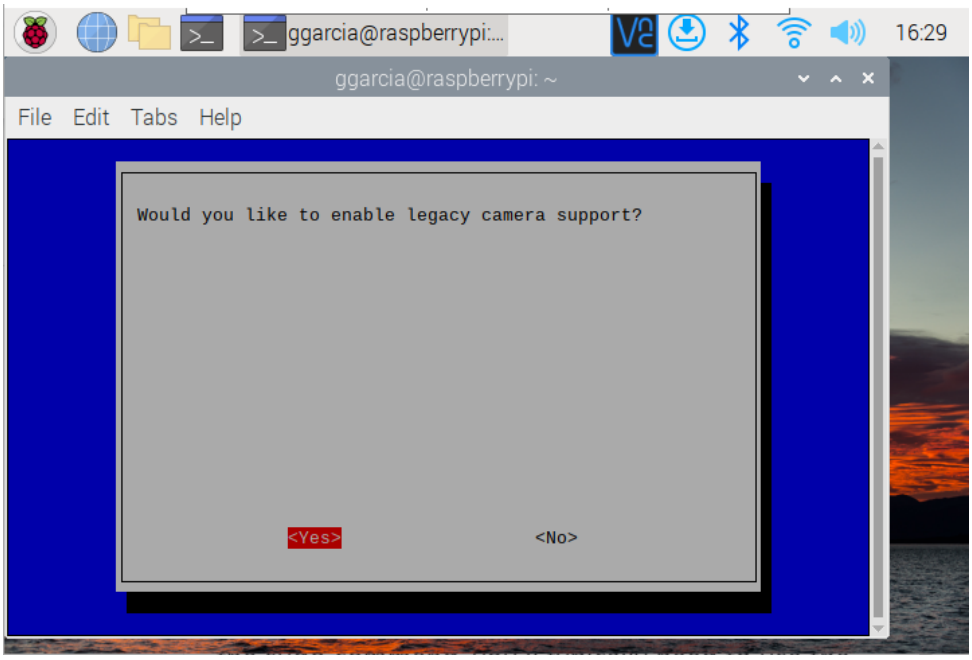


Figura 11 - Selecionar opção ”Yes” (Garcia, 2023, p.17)

Para garantir que a camara estava a funcionar, foi desenvolvido código para testar se a camara era corretamente iniciada:

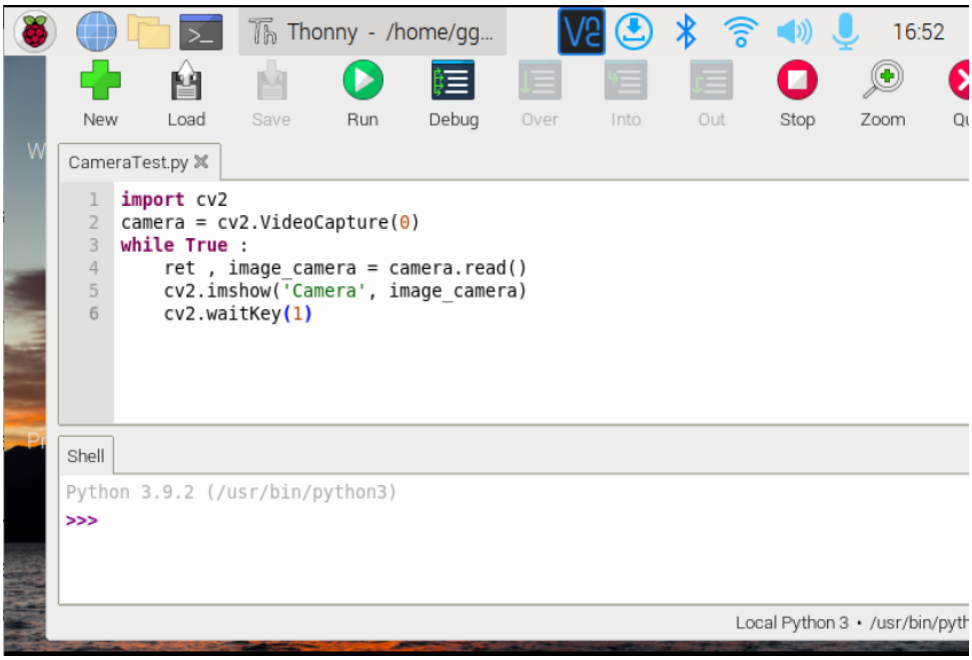


Figura 12 - Código de Verificação do funcionamento da camara no Raspberry Pi 4 (Garcia, 2023, p.18)

Este código, através da biblioteca *OpenCv* que em *Python* é designada como cv2 permite que a captura de vídeo através de uma *Webcam USB* seja capturada e apresentada numa janela, de forma continua:

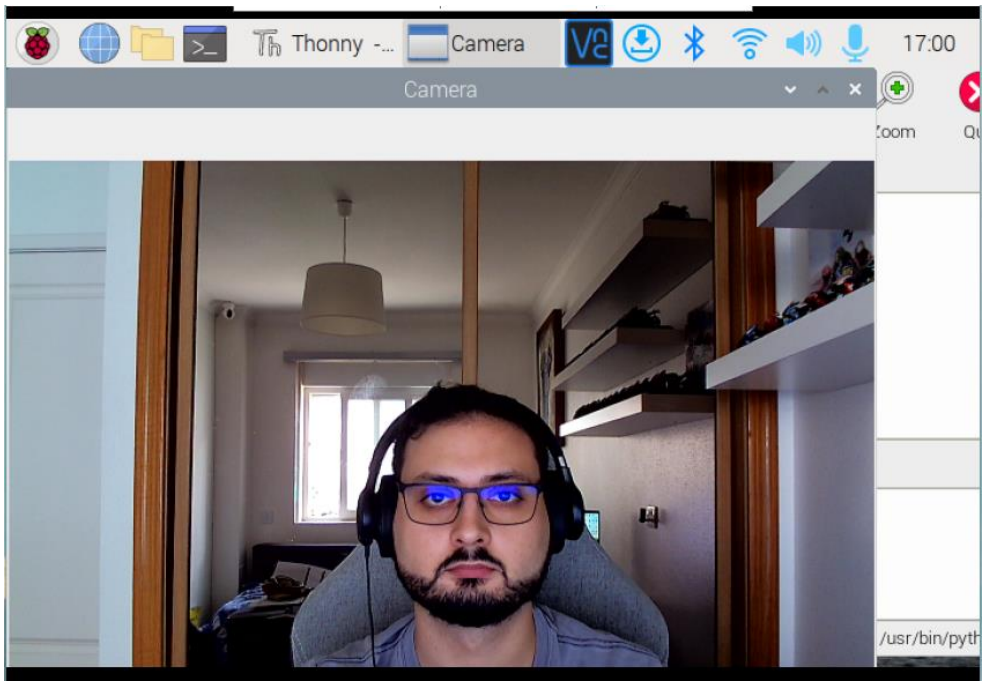


Figura 13 - Camara a funcionar no Raspberry Pi 4 (Garcia, 2023, p.18)

Pinos GPIO e Display

GPIO (*General Purpose Input/Output*) em microcontroladores ou microcomputadores, como o *Raspberry Pi 4*, são conectados a diferentes elementos de hardware e sensores. A deteção e reconhecimento de imagens em tempo real é iniciada através do *Display LCD* que utiliza pinos *GPIO*. Para iniciar o processo de deteção e reconhecimento de imagens o utilizador necessita de correr o código. A título de ilustração, ao correr o código através do *display GPIO*, a camara é acionada para começar a deteção e reconhecimento facial. No projeto desenvolvido o *Raspberry Pi 4* tem um *LCD* conectado através dos pinos *GPIO*, que fornecem feedback sobre o estado do sistema. Por exemplo, quando um rosto é detetado corretamente, o *LCD* retorna visualmente esta informação. Os pinos *GPIO* são usados para conectar dispositivos externos. No futuro os pinos podem conectar-se e interagir com hardware externo, como leitores *RFID* e leitores de impressão digital. O Display *LCD* é também utilizado para introduzir o código fornecido pelo sistema. Este código pode ser introduzido através de um teclado virtual ou físico.

Nos sistemas de deteção e reconhecimento facial, os displays fornecem feedback e informações visuais aos utilizadores. O *Display* é utilizado para uma variedade de tarefas, incluindo a monitorização em tempo real. A deteção facial em tempo real e a monitorização do procedimento de reconhecimento são possíveis através de um *display* que exibe imagens e uma transmissão de vídeo em tempo real do rosto gravado. No futuro, através do *Display*, os utilizadores poderão visualizar avisos ou instruções que terão de ser seguidas durante o procedimento de deteção e reconhecimento facial.

Display utilizado no sistema desenvolvido:

Figura 14 - Display Joy-IT 3.5 (JOY-IT, n.d.)

Conetores:

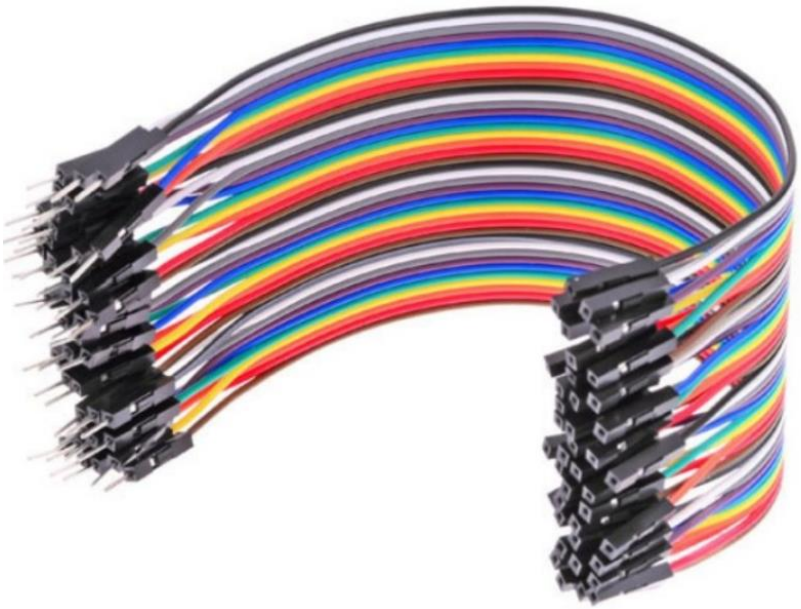


Figura 15 - Conetores GPIO (Ecocables, n.d.)

Para efetuar a ligação entre o *Raspberry Pi 4* e o *Display* foram utilizados conetores, que possibilitam a interface entre os dois componentes, mas também foi necessário investigar onde seria possível conectar cada conetor. A imagem abaixo descreve cada um dos Pinos *GPIO* do *Raspberry Pi 4*:

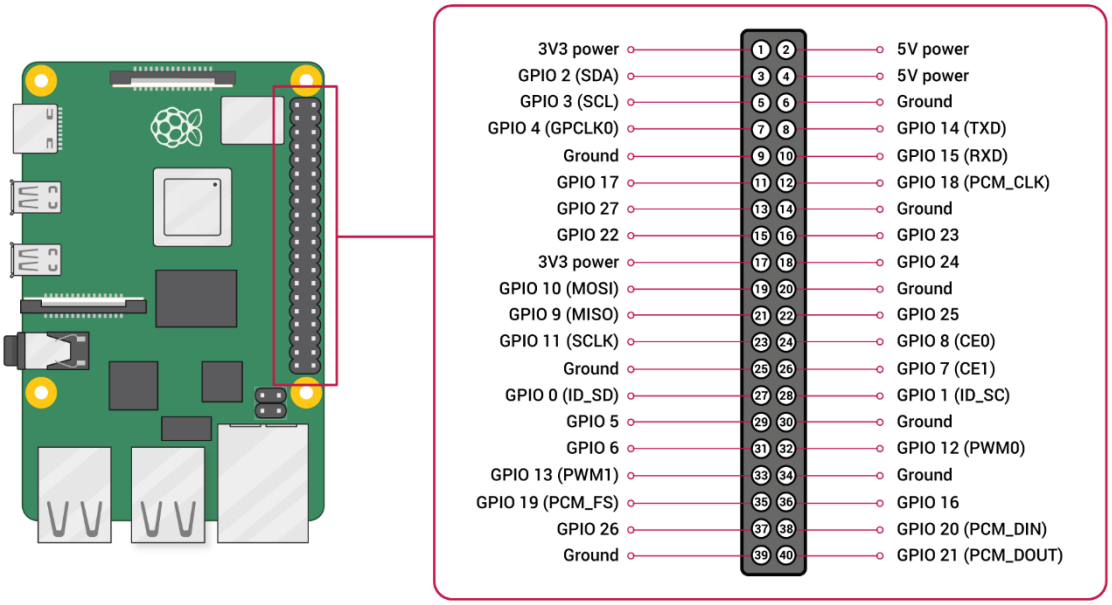


Figura 16 - Descrição dos Conetores GPIO do Raspberry Pi 4 (Raspberry, n.d.)

Foram conectados 25 Pinos dos 26 disponíveis, uma vez que o Pino representado com o número 2, na imagem acima, não é necessário para a alimentação do *Display*, porque o Pino número 4 tem exatamente a mesma função e além disso o Pino número 2, será utilizado para alimentar o *Servo Motor*.

Após terem sido realizadas as conexões, os dois componentes ficaram a comunicar entre si:

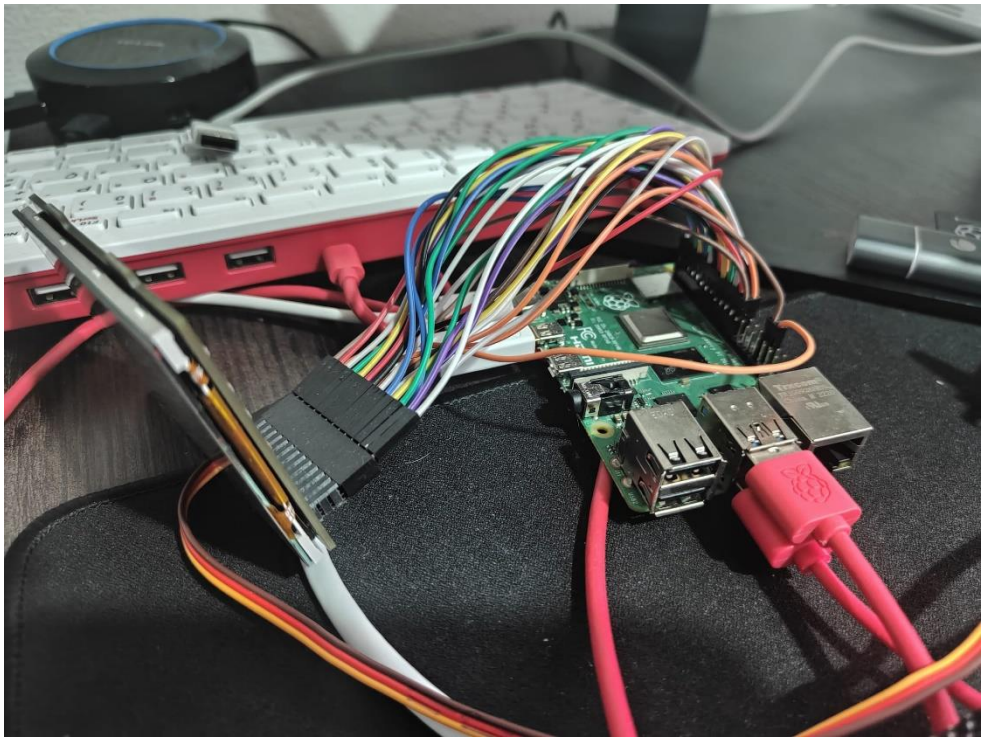


Figura 17 - Ligações entre o Display e o Raspberry Pi 4 (Garcia, 2023, p.19)

Figura 18 – Display (Garcia, 2023, p.19)

Servo Motor

Como já mencionado anteriormente o sistema utiliza um *Servo Motor* eletrónico para simular a abertura e fecho de uma porta eletrónica. Este Servo Motor está conectado ao *Raspberry Pi* através de conetores, que possibilitam a sua interface entre os dois componentes. O Sistema de deteção e reconhecimento facial foi responsável por enviar sinais digitais para o *Servo Motor*, sinais estes que foram enviados através do Pino 16 do *Raspberry Pi 4*. Estes sinais fizeram com que o *Servo Motor* rodasse até à sua máxima posição de abertura, simulando a abertura da porta e posteriormente após 3 segundos, rodasse até à sua mínima posição, simulando o fecho da porta.

O modelo escolhido, foi o *Servo Motor MG995*, por se tratar de um motor facilmente transportável e de integração rápida num sistema de deteção e reconhecimento facial, uma vez que é bastante utilizado nesta área, para simulação de uma fechadura de uma porta eletrónica:

Figura 19 - Servo Motor MG995 (Servo Motor MG995, n.d.)

Para efetuar a ligação entre o *Servo Motor* e o *Raspberry Pi 4*, foi necessário:

- Conetar o cabo vermelho do *Servo Motor* ao Pino do *Raspberry Pi 4* que correspondia à alimentação de 5V.
- Conetar o cabo castanho do *Servo Motor* ao Pino do *Raspberry Pi 4* que correspondia á Terra.
- Conetar o cabo laranja do *Servo Motor* ao Pino GPIO 16 do *Raspberry Pi 4*.

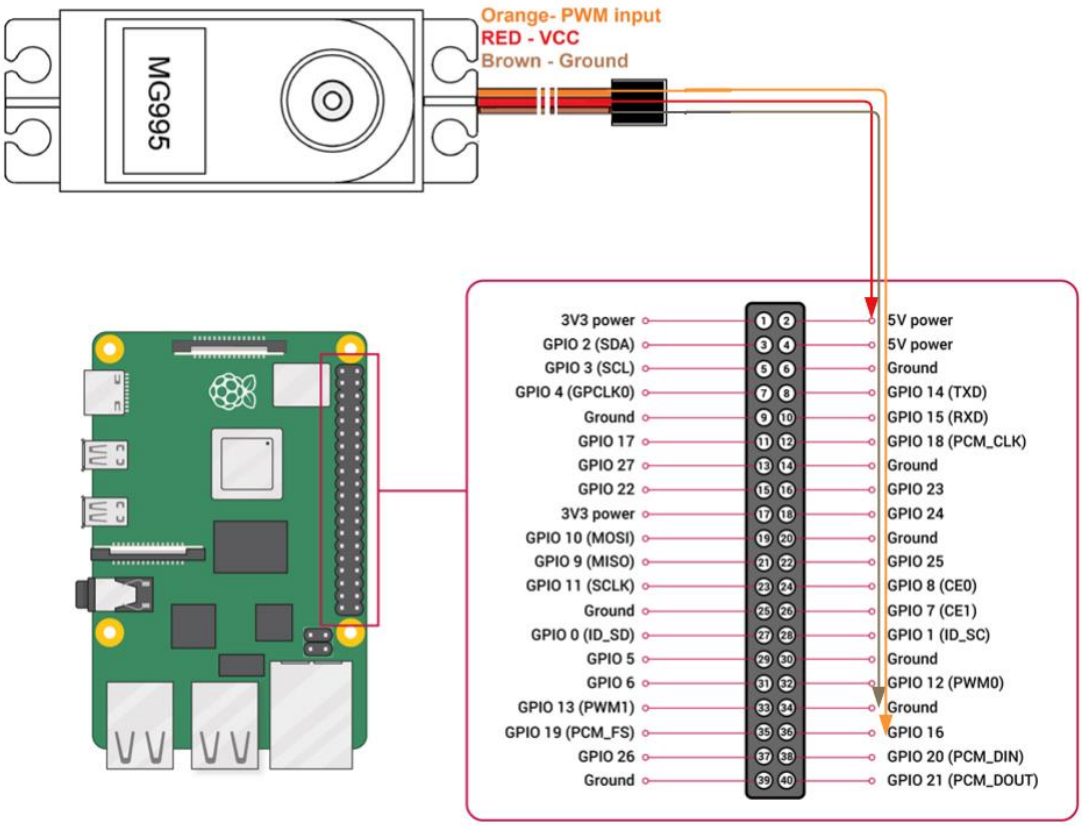


Figura 20 - Conexão Servo Motor com Raspberry Pi 4 (Garcia, 2023, p.20)

Na imagem abaixo, podemos observar a função *open_door* que foi definida durante o desenvolvimento do sistema de deteção e reconhecimento facial. Esta função foi responsável por enviar sinais digitais para o *Servo Motor* com o objetivo de simular a abertura de uma porta eletrónica, quando um utilizador é verificado com sucesso:

```
def open_door():
    print('Door is Opening...')
    servo.max() #comment for PC
    sleep(3) #waits for 3 sec and closes again
    print('Door is Closing...')
    servo.min() #comment for PC

servo = Servo(16) #declare the pin of GPIO of the motor / comment to test on PC
servo.min() #comment to test on PC
```

Figura 21 - Definição da função open_door (Garcia, 2023, p.19)

Um sistema de deteção e reconhecimento facial para controlar o acesso a um determinado local com *Multi-Factor Authentication (MFA)* efetua a gestão da deteção e reconhecimento facial, da comunicação com o servo motor, que simula uma porta elétrica, e a *Multi-Factor Authentication (MFA)* combinando componentes de hardware e software. O sistema desenvolvido consiste na deteção e reconhecimento facial com a gestão automática de controlo de acesso a um determinado local através de um microcomputador *Raspberry Pi 4* em que é efetuado o registo de um individuo no sistema, a captura de imagens, em tempo real, para deteção e reconhecimento facial, a notificação por *SMS* de um código de verificação que é introduzido num *display GPIO*, conectado ao *Raspberry Pi 4* onde caso a validação seja verificada com sucesso, é enviado um sinal para um servo motor, que simula um motor de uma porta elétrica, para que a porta seja aberta.

- O Registo de um novo utilizador é realizado manualmente através de uma imagem introduzida no sistema onde posteriormente, através do *Histogram Of Gradients* é localizado o rosto. De seguida através da biblioteca *Dlib* são detetadas 68 coordenadas (x, y) diferentes, que mapeiam os pontos faciais do rosto. Através destas 68 coordenadas diferentes, são gerados os 128 valores que representam o rosto e guardados na base de dados *faces_database*. O nome e o contacto telefónico do individuo, após serem introduzidos, são associados aos 128 valores que representam o rosto e gravados, respetivamente, na base de dados *names* e *numbers*.

Posteriormente, para a verificação de um rosto, o sistema de deteção e reconhecimento facial pergunta ao utilizador o nome, captura uma imagem do utilizador que está diante da porta, em tempo real, através de uma camara disponível e conectada ao sistema de deteção e reconhecimento facial. Caso exista mais do que um utilizador na imagem em tempo real, apenas o utilizador mais perto da camara será capturado. O sistema de deteção e reconhecimento facial processa então a imagem para detetar a presença de um rosto, extrair os 128 valores que representam o rosto e compará-los com os 128 valores que representam o rosto do utilizador presente na base de dados. Se o rosto for reconhecido como autorizado:

- o sistema envia um código de autenticação por SMS (*Short Message Service*) para o número associado ao individuo contendo um código de quatro dígitos;
- o individuo introduz o código no display conectado ao sistema e é retornado se o código está ou não correto.
- se o código estiver correto é enviado um sinal para o sistema de gestão automática do controlo de acesso para abrir a porta.

No fluxograma que pode ser visualizado abaixo, podemos observar a arquitetura do código relativo à deteção e reconhecimento facial de um individuo que pretenda aceder a um determinado local:

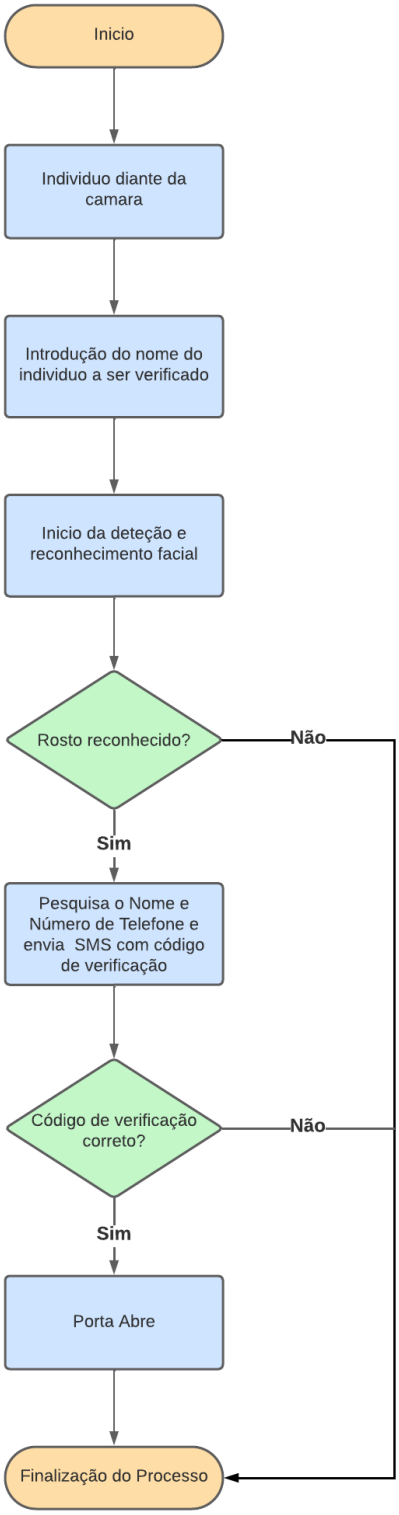


Figura 22 - Arquitetura De Código - Deteção e Reconhecimento Facial De Um Utilizador (Garcia, 2023, p.5)

4.2. AccessFace Sentinel

O sistema *Multi-Factor Authentication (MFA),* em português Autenticação de dois fatores (2FA) ou Verificação de dois fatores foi utilizado no âmbito do projeto académico, para prevenir o acesso não autorizado a um determinado local, uma vez que é adicionada uma camada extra de segurança ao sistema de deteção e reconhecimento facial desenvolvido. Este sistema requer que o utilizador confirme que é mesmo ele que está a tentar aceder a um determinado local. Este sistema pode utilizar várias formas de confirmação, por exemplo um código enviado *Short Message Service* (SMS) para o telemóvel do utilizador ou para o email ou através de uma aplicação externa instalada no telemóvel, responsável por gerar um código de verificação. Para este projeto académico, o utilizador recebeu os seus códigos de verificação, no telemóvel, através de um *SMS*, por se tratar de uma forma mais ágil e ser facilmente integrado no sistema desenvolvido. Através de uma aplicação externa *Twilio*, foi possível criar um telefone virtual que foi responsável pelo envio dos códigos de verificação. Para integrar o *Twilio* no sistema desenvolvido, foi necessária alguma investigação do funcionamento da interface do *Twilio*. O sistema desenvolvido comunica com a interface do *Twilio* através da validação da conta, utilizando o *SID* único. Posteriormente, através da biblioteca *random*, foi configurado o tipo de código que seria gerado e enviado, que consistia num código de quatro dígitos gerado aleatoriamente entre a combinação do número 0000 e o número 9999. Este código é enviado através do número virtual, atribuído pelo *Twilio* para o número do utilizador que está a ser verificado e que foi gravado na base de dados *numbers* durante o registo do mesmo. No fluxograma abaixo, é possível observar a interface entre o sistema de deteção e reconhecimento facial e o *Twilio*:

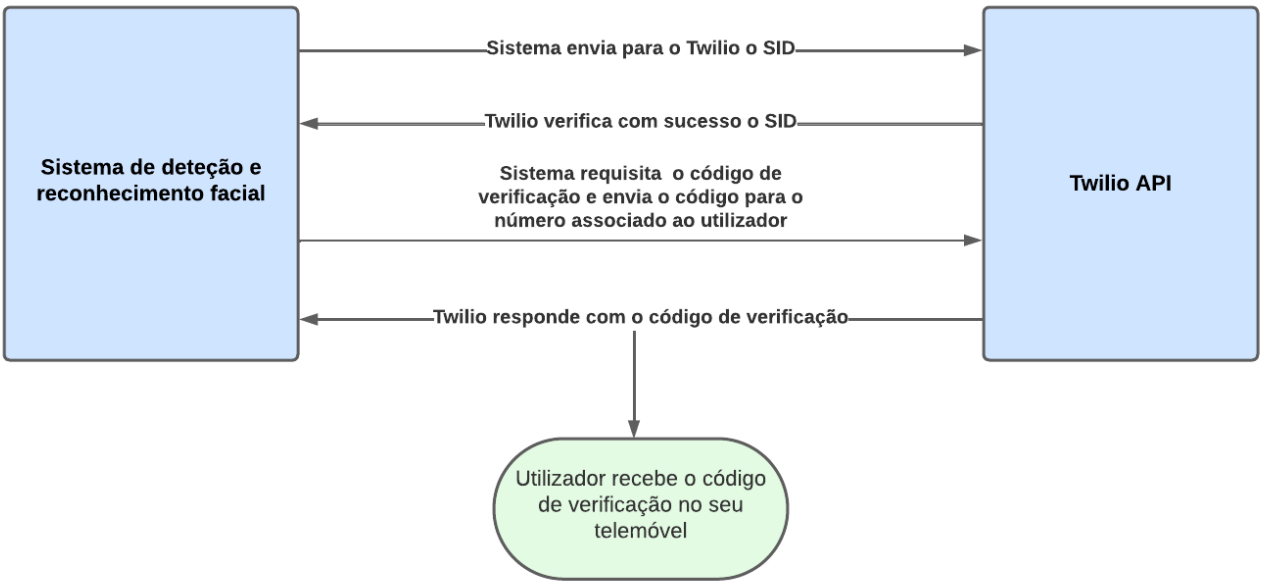


Figura 23 - Interface Sistema <> Twilio (Garcia, 2023, p.7)

Na imagem abaixo, é possível observar a função que executa este processo:

```
def SMS_verification_function(number): #sends sms
    SMS_verification = str(randint(0000,9999)) #randint is called and generates random number
    account_sid = 'AC12102875827be5d363407afd9d35a98e'
    auth_token = '4e43253ae8b97cdf1674006e22479210'

    client = Client(account_sid, auth_token)

    message = client.messages \
        .create(
             body=SMS_verification,
             from_='+12058833056',
             to = number #number based on DB
         )
    return SMS_verification
```

Figura 24 - Função SMS_verification_function (Garcia, 2023, p7)

Exemplo de código de verificação enviado:

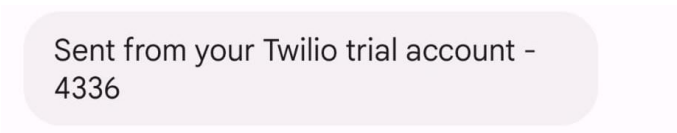


Figura 25 - Exemplo Código Verificação Enviado (Garcia, 2023, p.7)

4.3. Base de Dados

A base de dados foi criada através da função *database_cr*, que é utilizada para criar e também gerir a base de dados onde são guardadas três listas distintas em três ficheiros distintos:

Figura 26 - Ficheiros Base de Dados (Garcia, 2023, p.8)

- **Faces_database**
- **Names**
- **Numbers**

O objetivo desta função foi verificar se os ficheiros da base de dados existem e carrega-los se existirem, ou criar novas listas vazias se não existirem. A função desenvolvida utiliza o modulo Pickle que é responsável por serializar ou desserializar objetos para gravar e carregar dados.

Na imagem abaixo, é possível observar a função *database_cr*:

```python
# 1 - If the DB does not exist create the DB files with empty lists.
# 2 - If exists will read and add the new values.
2 usages
def database_cr():
    faces_databse_path = 'faces_database'
    #detects if the file exists or not.
    #database_exist is boolean (true or false)
    database_exist = os.path.exists(faces_databse_path)

    if database_exist :
        #open the 'faces_database' file in binary read mode ('rb').
        file_read = open('faces_database', 'rb')
        #reads the serialized data from the file and loads it into the faces_database variable.
        faces_database = pickle.load(file_read)

        file_read = open('names', 'rb')
        names = pickle.load(file_read)

        file_read = open('numbers', 'rb')
        numbers = pickle.load(file_read)

    else :
        #database files don't exist.
        #So the code initializes empty lists for faces_database, names, and numbers.
        faces_database = []
        names = []
        numbers = []

    #returns the loaded or initialized lists faces_database, names, and numbers.
    return faces_database,names,numbers
```

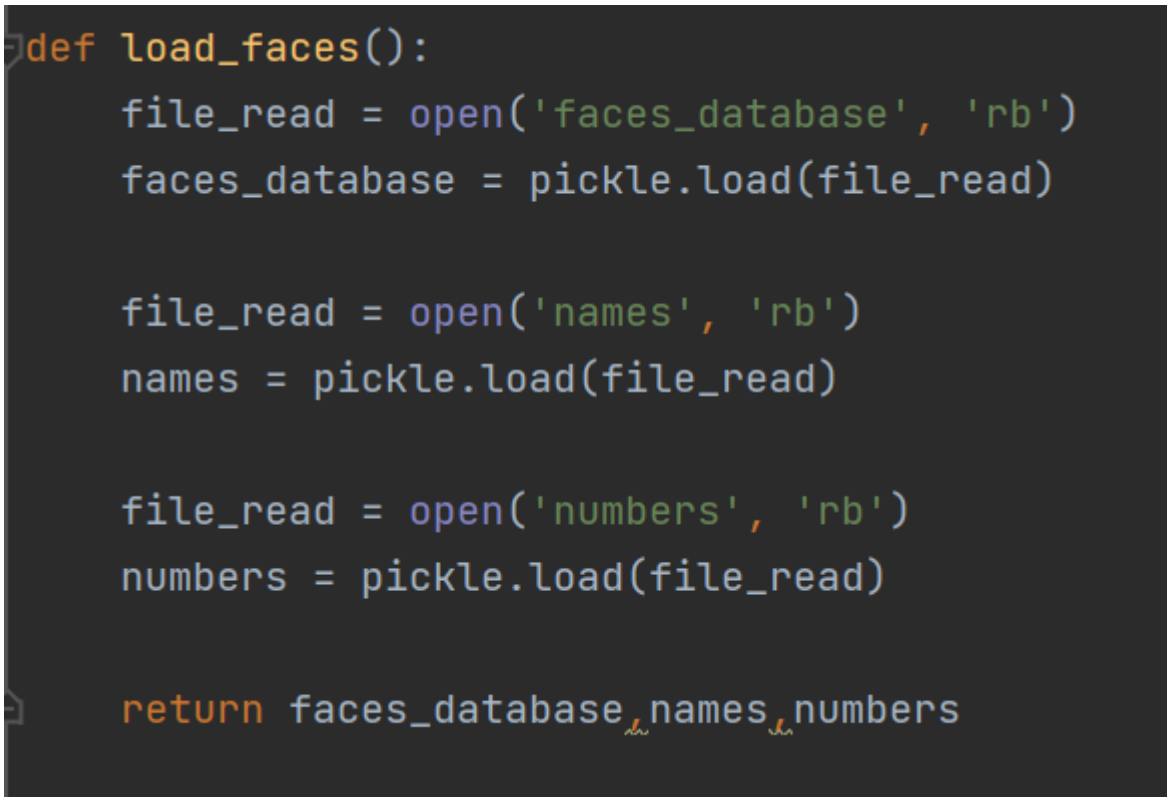
Figura 27 - Função database_cr (Garcia, 2023, p.8)

Durante o registo de um novo utilizador, é necessário gravar nos ficheiros da base de dados, os dados relativos a este novo utilizador. Para isso, foi criada a função *save_faces_database* responsável por gravar dados nas listas dos três ficheiros. Estas listas são gravadas em formato binário:

```
    #save the user face encondings, name and number to files DB
2 usages
def save_faces_database(faces_database,names,numbers):

    file_saving = open('faces_database', 'wb')
    pickle.dump(faces_database,file_saving)

    file_saving = open('names', 'wb')
    pickle.dump(names,file_saving)

    file_saving = open('numbers', 'wb')
    pickle.dump(numbers,file_saving)
```

Figura 28 - Função save_faces_database (Garcia, 2023, p.9)

Antes da verificação de um utilizador ser efetuada, foi necessário expor ao sistema a base de dados existente e foi criada a função *load_faces* que é responsável por carregar os dados que estão gravados na base de dados:



```
def load_faces():
    file_read = open('faces_database', 'rb')
    faces_database = pickle.load(file_read)

    file_read = open('names', 'rb')
    names = pickle.load(file_read)

    file_read = open('numbers', 'rb')
    numbers = pickle.load(file_read)

    return faces_database, names, numbers
```

Figura 29 - Função load_faces (Garcia, 2023, p.9)

OpenCV é uma biblioteca utilizada em *Python* criada para resolver problemas de visão computacional. *Python* é uma linguagem de programação utilizada em várias áreas, incluindo inteligência artificial, análise de dados e desenvolvimento *web* (Minichino & Howse, 2015). É uma linguagem interpretada simples de aprender e utilizar. Existem inúmeras bibliotecas de deteção e reconhecimento facial em *Python*. *OpenCV* é uma das bibliotecas de deteção e reconhecimento facial mais utilizadas. Uma biblioteca de visão computacional *open source* chamada *OpenCV* pode ser utilizada para várias tarefas, incluindo processamento de imagem e apresentação da mesma. Após a instalação da biblioteca, utiliza-se o módulo cv2 do *Python* para realizar quaisquer ações relacionadas com o processamento e apresentação de imagem (Minichino & Howse, 2015). A linguagem de programação e as bibliotecas, foram as fontes primárias de todos os serviços tecnológicos e de infraestruturas necessárias para alimentar o sistema.

A biblioteca *OpenCV* foi utilizada, durante o desenvolvimento deste projeto, para o processamento e apresentação da imagem, nos seguintes termos:

- Durante o registo de um utilizador, é utilizada para efetuar a leitura da imagem introduzida na base de dados e para alterar o modelo de cor utilizado para representar cores numa imagem digital.

```
image = cv2.imread('PicG.jpg') #read the image using cv2 librarie
#cv2 reads image as BGR but the librarie face_recognition>
#>expects the input has RGB so we convert here and swap R&B.
image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
image = cv2.resize(image,(int(image.shape[1]*0.5),int(image.shape[0]*0.5))) #Resize the image change the size to -50%
```

Figura 30 – Processamento de Imagem (Leitura & Cor) (Garcia, 2023, p.10)

- Durante o processo de verificação de um utilizador, é utilizada para iniciar a camara e capturar vídeo em tempo real, desenhar retângulos nos rostos identificados, colocar texto por cima dos retângulos e mensagens.

Câmara iniciada para captação de vídeo em tempo real:

```
camera = cv2.VideoCapture(0) #initiate the camara component
```

Figura 31 - Inicialização da Câmara (Garcia, 2023, p.10)

Invocação da função *draw_rec* utilizada para criar um desenho de um retângulo no rosto identificado:

```
    if len(face_det)==0: #If List is Empty there was No Face Detected
        print('Face Not Detected.')
        cv2.imwrite('Face_Not_Detected.png', image)
    else: #If not, a Face was Detected
        box, idx = face_det
        image = draw_rec(image, box)
        image_face = image
        face_encodings = face_recognition.face_encodings(image_face,[box])
        #Print((face_encodings)) #Print 128 measurements
```

Figura 32 - Função draw_rec invocada para desenhar um retângulo (Garcia, 2023, p.10)

```
def draw_rec(image,box): #visualization of the face

    (top, right, bottom, left) = box
    start_pt = (left, top)
    end_pt = (right, bottom)
    color = (255, 0, 0)
    thickness = 2
    image = cv2.rectangle(image, start_pt, end_pt, color, thickness)

    return image
```

Figura 33 - Definição da função draw_rec function (Garcia, 2023, p.11)

Invocação da função *visualize_identity* e *type_text_on_image* responsáveis por colocar texto em cima dos retângulos dos rostos identificados. É efetuada a colocação, respetivamente, do Nome do utilizador identificado e da mensagem de sucesso ou insucesso:

```
image = visulize_identity(image, user_name, box)
# image = cv2.cvtColor(image, cv2.COLOR_RGB2BGR)
image = type_text_on_image(image, 'User Verified ! ')
```

Figura 34 - Invocação da função visualize_identity e type_text_on_image (Garcia, 2023, p.11)

```
else:
    print('User NOT Verified.')
    image = visulize_identity(image, 'User NOT Verified.', box)
```

Figura 35 - Invocação da função visualize_identity (Garcia, 2023, p.11)

```
def type_text_on_image(image, text): #visualize the name in the image detected / input is image and text
    height,width,_ = image.shape
    start_x = 190
    start_y = 50
    start_pt = (start_x,start_y)

    font = cv2.FONT_HERSHEY_SIMPLEX
    fontScale = 1
    color = (255, 0, 0)
    thickness = 2

    image = cv2.putText(image, str(text),start_pt, font,
                        fontScale, color, thickness, cv2.LINE_AA)
    return image



5 usages
def visulize_identity(image, identity, box): #calculate the box and put it on top of the box

    (top, right, bottom, left) = box
    start_x = int(((right + left) / 2)-50)
    start_y = int(top - 10)
    start_pt = (start_x,start_y)

    font = cv2.FONT_HERSHEY_SIMPLEX
    fontScale = 1
    color = (255, 0, 0)
    thickness = 2

    image = cv2.putText(image, str(identity),start_pt, font,
                        fontScale, color, thickness, cv2.LINE_AA)
    return image
```

Figura 36 - Definições das funções type_text_on_image e visualize_identity (Garcia, 2023, p.12)

4.4. Biblioteca Dlib e face_recognition

A biblioteca *Dlib* é um kit de ferramentas C++ moderno que contém algoritmos de *Machine Learning* e ferramentas para criar software complexo em C++, para resolver problemas do mundo real, como sistemas de deteção e reconhecimento facial. A biblioteca *Dlib* integra-se com ferramentas e algoritmos baseados em *Python* usando *Application Programming Interfaces (APIs)* especificas (Fernández Villán, 2019).

No projeto desenvolvido, utilizámos o *Histogram of Oriented Gradients* através da interface *face_recognition.face_locations* presente na biblioteca *face_recognition* contruída com a biblioteca D*lib*, para localizar a área que corresponde ao rosto do individuo mais próximo da camara, tal como podemos observar através da seguinte imagem:

```
def face_detection(image):

    #face_location localizes the face in the image with HOG and get the location of the face in the image
    boxes = face_recognition.face_locations(image)
    print(len(boxes))
    if len(boxes)>0:
        idx = capture_nearest_person(boxes) #captures nearst person idx
        box = boxes[idx]

        #box contains a list of tuples of found face locations in css
        #(top, right, bottom, left) order / idx contains the index of the nearst person
        return box,idx
    else:
        return ()
```

Figura 37 - Definição da função face_detection (Garcia, 2023, p.13)

No código acima, é possível observar a função *face_detection*, criada no decorrer do desenvolvimento deste projeto que tem como finalidade aplicar o *Histogram of Oriented Gradients* e retornar os valores encontrados num rosto com a ordenação *CSS* (*top*, *right*, *bottom left*) e guardá-los na variável *box*.

Uma vez que todo este processo é efetuado automaticamente através da interface *face_recognition.face_locations* presente na biblioteca *face_recognition*, foi construído, para exemplificar, um pequeno código à parte deste projeto que retorna visualmente a aplicação do *Histogram of Oriented Gradients*:

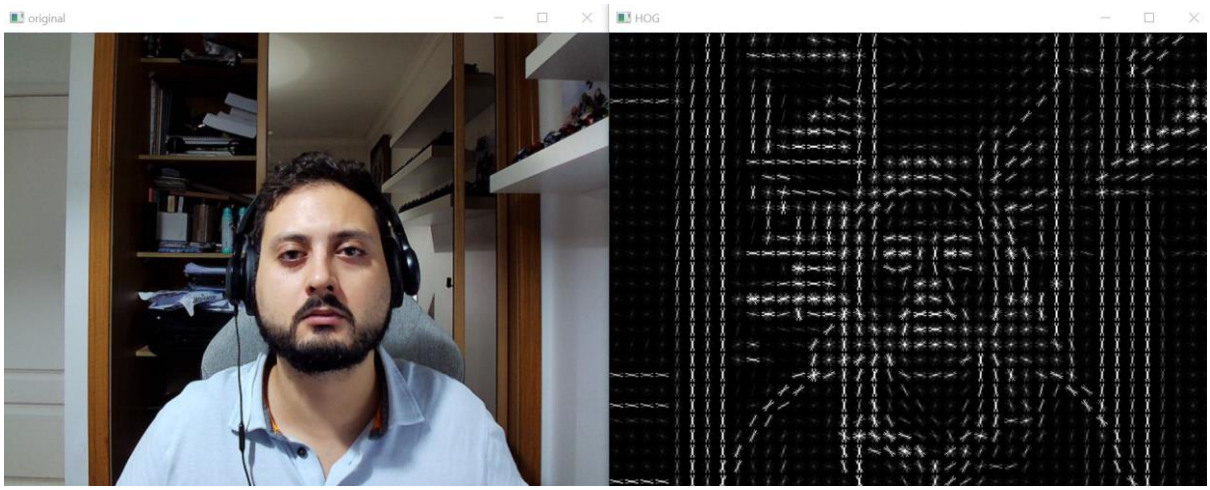


Figura 38 - Exemplo de uma comparação entre uma imagem original e a imagem calculada pelo HOG (Garcia, 2023, p.13)

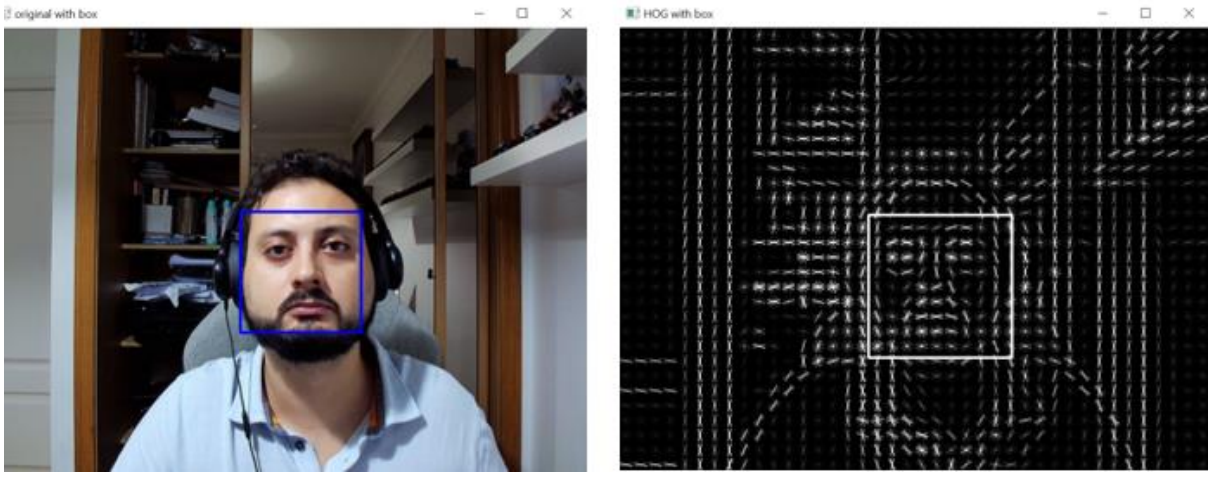


Figura 39 - Rosto detetado pelo HOG (Garcia, 2023, p.13)

Especificamente, para o projeto que foi desenvolvido, a biblioteca Dlib é utilizada como um detetor de coordenadas faciais de referência através do modelo pré-treinado *get_frontal_face_detector*. Posteriormente através do modelo pré-treinado *shape_predictor_68_face_landmarks.dat* presente na biblioteca Dlib foi utilizado para verificar a localização de 68 coordenadas (x, y) diferentes, que mapeiam os pontos faciais num rosto.

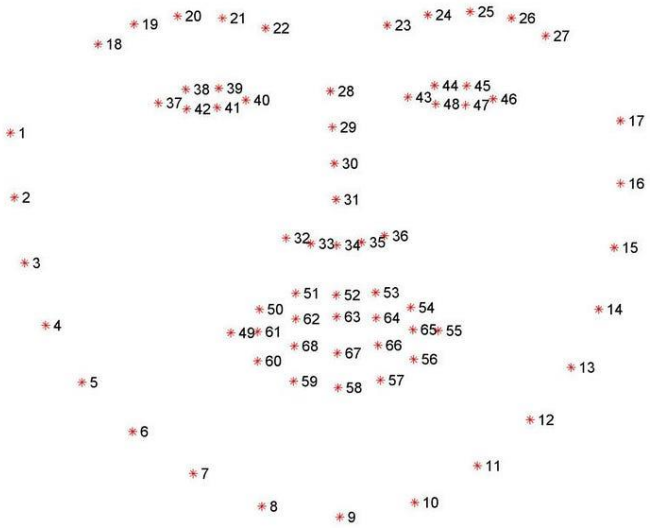


Figura 40 - 68 coordenadas (x, y) diferentes, que mapeiam os pontos faciais num rosto (Fernández Villán, 2019)

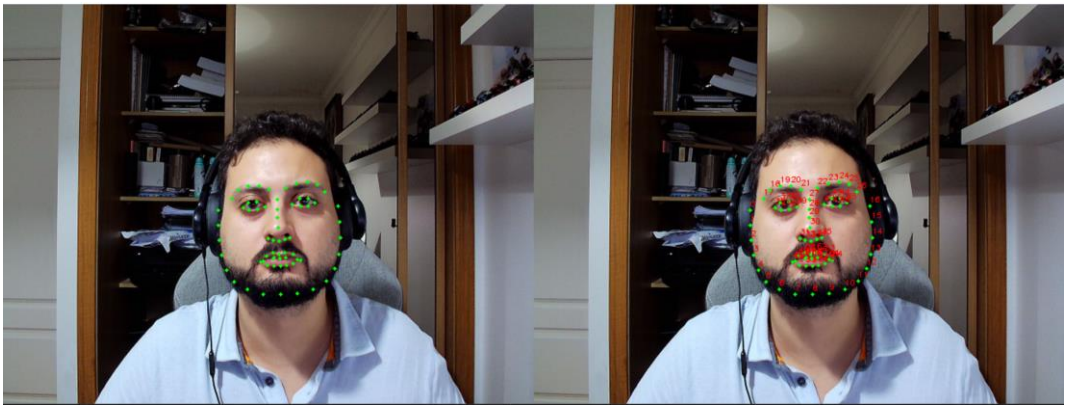


Figura 41 - Exemplo das 68 coordenadas identificadas num rosto (Garcia, 2023, p.13)

A biblioteca *Dlib* tem outras funcionalidades poderosas que ajudam a determinar a posição e orientação dos rostos, detetar rostos e reconhecer objetos. O sistema de deteção e reconhecimento facial desenvolvido é exposto aos rostos em formato de imagem que são necessários identificar. O sistema de deteção e reconhecimento facial não guarda imagens na sua base de dados, ele utiliza os 68 pontos de referências faciais do rosto para posteriormente gerar 128 valores que representam o rosto, estes que são guardados num ficheiro correspondente à base de dados.

A geração dos 128 valores que representam um rosto, foi realizada através de um modelo pré-treinado. Este modelo foi treinado através de milhares de imagens que permitiram, ao dia de hoje, ser um modelo de confiança. O pacote *face_recognition* fornece a interface *face_encondings* que gera automaticamente os 128 valores que representam o rosto da imagem exposta ao sistema de deteção e reconhecimento facial.

No código desenvolvido, podemos observar como se processa a geração dos 128 valores que representam o rosto:

```
while True:
    user_name = input('Please enter your name here: ') #Enters name
    print(user_name in names)
    while user_name not in names:
        print('The name you entered doesn\'t exist in the database')
        user_name = input('Please enter your name correctly: ')  #Enters name)
    if user_name in names:
        print('Name exists in the database')

    #Get user_name and look for his index in names DB / Goes to face_database DB
    #and access that index which contains the face linked to that user_name
    user_face = faces_database[names.index(user_name)]
    number = numbers[names.index(user_name)] #Index of user_name and get the number
    #sleep(5)
    _, image = camera.read() #Get the image from the camara and put it at image variable
    # image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
    face_det = face_detection(image) #Apply face_detetion function to find the face in the image of the camara
    if len(face_det)==0: #If List is Empty there was No Face Detected
        print('Face Not Detected.')
        cv2.imwrite('Face_Not_Detected.png', image)
    else: #If not, a Face was Detected
        box, idx = face_det
        image = draw_rec(image, box)
        image_face = image
        face_encodings = face_recognition.face_encodings(image_face,[box])
        #Print((face_encodings)) #Print 128 measurements
```

Figura 42 - Geração 128 valores que representam o rosto (Garcia, 2023, p.14)

Como podemos observar na imagem abaixo, os 128 valores são colocados num *Array*:

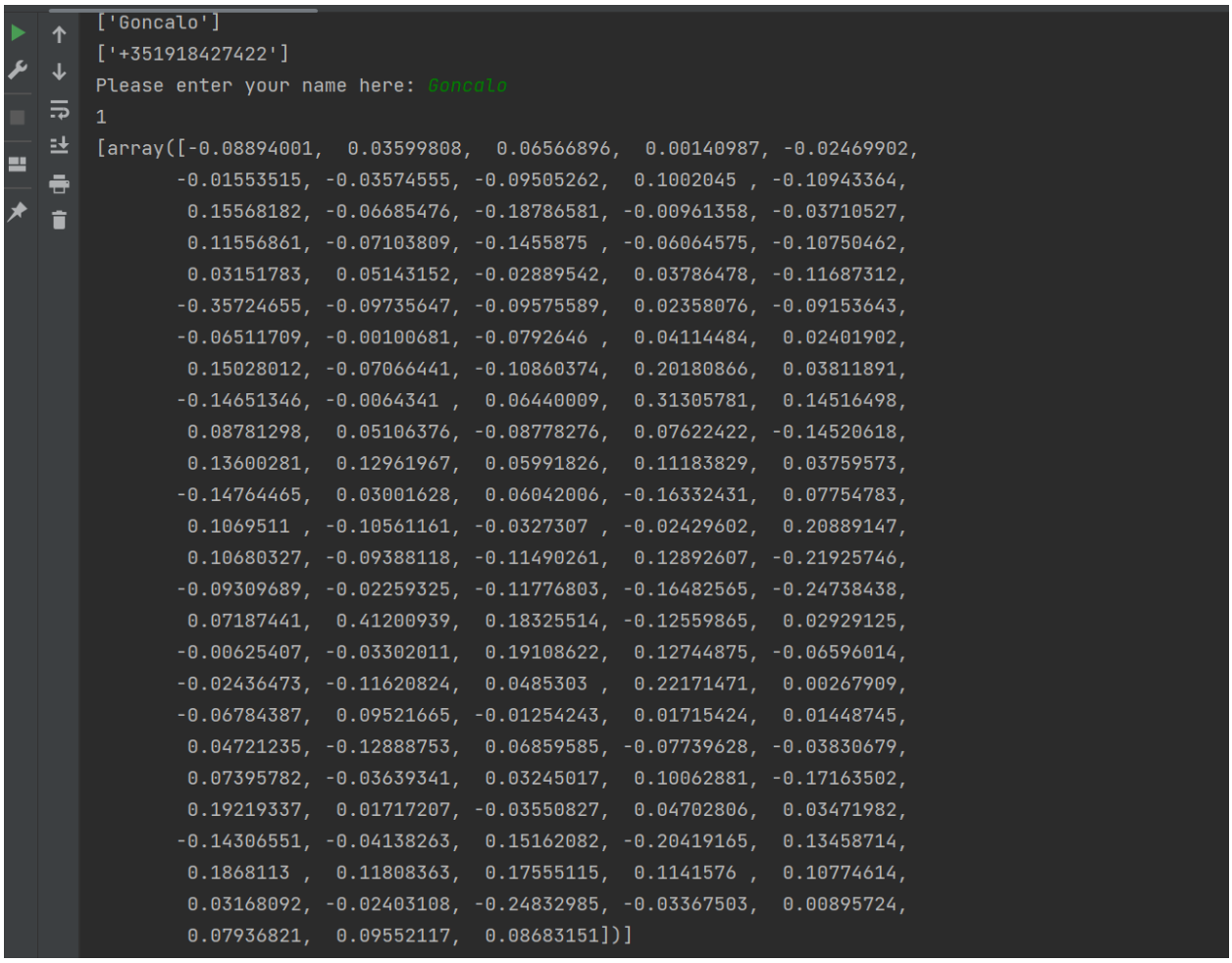


Figura 43 - Visualização dos 128 valores num Array (Garcia, 2023, p.14)

Posteriormente é necessário efetuar a comparação entre os 128 valores que representam o rosto que está presente na base de dados e os 128 valores que representam o rosto capturado através da webcam e calcular a distância euclidiana entre os dois conjuntos.

Posteriormente foi efetuada uma comparação com a distância euclidiana do rosto presente na base de dados, através da interface *face_recognition.compare_faces*, com um *threshold* de 0.6:

```
#Give the face encondings of the new face and compare it to the user_face from the DB
#Compare_faces return true or false and save in the verified variable.
verified = face_recognition.compare_faces(face_encodings,user_face)[0]
print("Verified:", verified)
```

Figura 44 - Comparação da Distância através da interface face_recognition.compare_faces (Garcia, 2023, p.15)

Que retorna se a comparação foi ou não efetuada com sucesso, que respetivamente faz com que seja ou não enviada uma mensagem para o número associado ao utilizador com um código de verificação, que será posteriormente introduzido pelo utilizador para que seja concedido o acesso ao local, caso o código seja correto.

Para verificar e validar, o resultado do cálculo da distancia entre os dois rostos durante a fase de testes, foi utilizada a interface *face_recognition.face_distance:*

```
distance = face_recognition.face_distance(face_encodings, user_face) #Measuring the distance beetween the 2 faces
print('Euclidean distance:', distance)
```

Figura 45 - Cálculo distância entre os dois rostos com a interface face_recognition.face_distance (Garcia, 2023, p.15)

Se o resultado fosse inferior a 0.6 então o reconhecimento facial era bem-sucedido, caso fosse superior a 0.6 o reconhecimento não era bem-sucedido.

De forma a poder analisar a performance a precisão, foram efetuados testes ao sistema de deteção e reconhecimento facial desenvolvido. O pesquisador analisou os dados obtidos através do método de observação participante nas diferentes fases do projeto desenvolvido assim como o resultado obtido da entrevista aos elementos participativos após a implementação do sistema.

Durante a primeira etapa do desenvolvimento do sistema de deteção e reconhecimento facial, foram efetuadas algumas anotações com base na observação efetuada em campo. Foram utilizados três indivíduos diferentes, em que apenas um existia na base de dados.

Os resultados foram positivos:

	Existe na base de dados	Identificação
Gonçalo	Sim	Sim
Andreia	Não	Não
Luís	Não	Não

Figura 46 - Resultados da observação e participação no comportamento do sistema em relação à deteção e reconhecimento facial (Garcia, 2023, p.20)

Através da figura acima o pesquisador verificou que dos três elementos participantes, apenas um foi corretamente identificado pelo sistema de identificação e reconhecimento facial, o qual os seus valores faciais se encontravam na base de dados. Os restantes dois elementos não foram identificados, uma vez que os seus valores faciais não constavam na base de dados. É importante referir que nesta fase, apenas se encontrava desenvolvido a deteção e o reconhecimento facial.

O pesquisador concluiu nesta fase que o sistema de deteção e reconhecimento facial estava a funcionar corretamente, quando sujeito a variações de iluminação e com três indivíduos diferentes.

Na segunda fase do desenvolvimento, o sistema de deteção e reconhecimento facial já se encontrava concluído, o que possibilitou testar a ação do movimento de abertura de porta com base na deteção e reconhecimento facial. Nesta fase, participaram os mesmos três indivíduos, em que continuava a existir apenas um na base de dados.

Os resultados foram positivos:

	Existe na base de dados	Identificação	Abertura de Porta
Gonçalo	Sim	Sim	Sim
Andreia	Não	Não	Não
Luís	Não	Não	Não

Figura 47 - Resultados da observação e participação no comportamento do sistema em relação à deteção e reconhecimento facial e a ação de abertura de porta (Garcia, 2023, p.21)

Através da figura acima o pesquisador pode verificar que dos três participantes, apenas um foi corretamente detetado e reconhecido pelo sistema, o qual os seus valores faciais se encontravam na base de dados, que fez com que fosse enviado um sinal digital que despoletou a ação de movimento de abertura, sobre o motor da porta. Os restantes dois participantes não foram identificados, uma vez que os seus valores faciais não constavam na base de dados, o que fez com que não fosse enviado qualquer sinal digital para que existisse qualquer ação de movimento despoletada sobre o motor da porta.

O pesquisador concluiu nesta fase que o sistema de identificação e reconhecimento facial estava a funcionar corretamente.

4.5. Testes e validação

Na fase de testes, a utilização de cenários do mundo real torna-se essencial. O pesquisador avaliou o sistema de deteção e reconhecimento facial em circunstâncias do mundo real, considerando variáveis como condições de iluminação, obstáculos, mudanças de posição e expressões faciais. De seguida, o pesquisador examina o desempenho do sistema nessas circunstâncias, de modo a verificar e validar o mesmo.

A fase de testes ocorreu ao utilizar medidas apropriadas, como é o caso da *F-Measure*. Através desta medida foi possível testar a eficácia e a qualidade do sistema de identificação e reconhecimento facial. Esta medida analisou com precisão o quão bem o sistema desenvolvido deteta e reconhece rostos em tempo real.

A medida *F-Measure* como já referido, avalia a eficácia e a qualidade do sistema através da relação entre o número de resultados positivos e resultados negativos, sendo este último por o sistema recusar a abertura de porta a um utilizador presente na base de dados ou então pela identificação errada do utilizador.

A utilização da medida *F-Measure* para testar o sistema é utilizada através da definição de critérios de verdadeiro ou falso, positivo ou negativo.

Os critérios para que a análise da eficácia e qualidade de um sistema de deteção e reconhecimento facial seja efetuado com sucesso, segue as seguintes definições:

- Verdadeiro Positivo – O resultado do reconhecimento facial é correto e a imagem de entrada não é rejeitada.
- Falso Positivo – O resultado do reconhecimento facial é incorreto e a imagem de entrada não é rejeitada.
- Verdadeiro Negativo – A imagem de entrada é rejeitada devido ao individuo não estar presenta na base de dados.
- Falso Negativo – A imagem de entrada é rejeitada, mas o individuo está presente na base de dados.

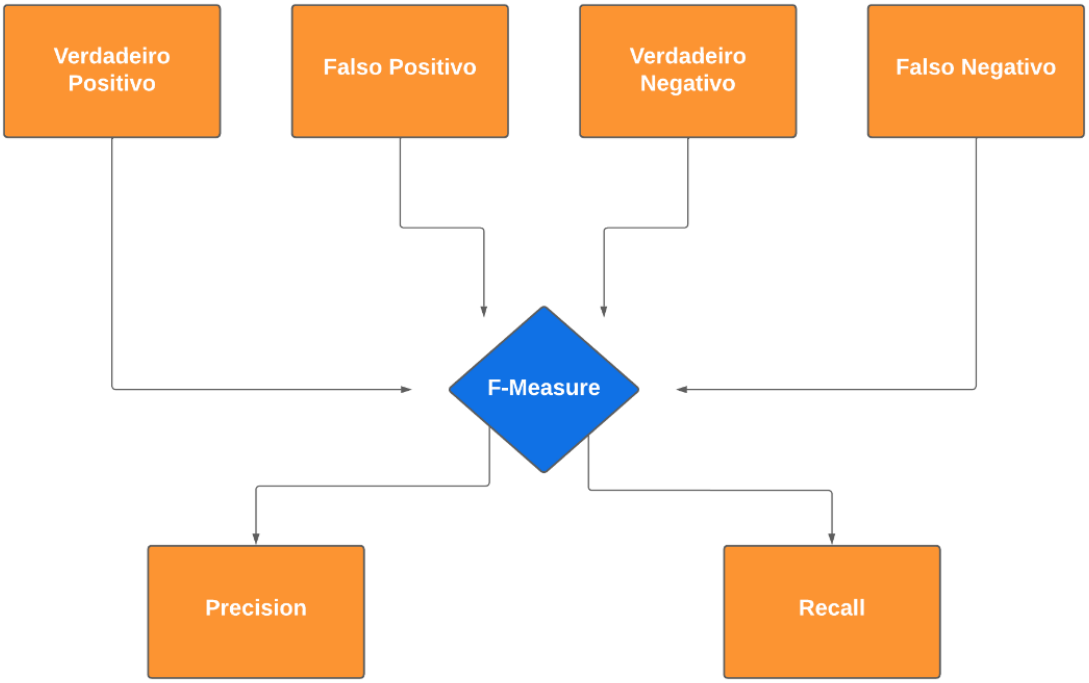


Figura 48 - Critérios para análise da eficácia e qualidade do sistema (Garcia, 2023, p.21)

Os dados necessários para que esta análise seja conduzida com sucesso, estão presentes na base de dados, ou seja, os indivíduos existentes na base de dados foram utilizados como parâmetros de entrada do sistema.

Mantendo sempre o sistema configurado da mesma forma, a cada execução da validação, foi efetuada uma média dos parâmetros do *F-Measure* obtidos em 15 execuções com o sistema configurado da mesma forma.

$$\textbf{Precision} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Positivo}}$$

$$\textbf{Recall} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Negativo}}$$

$$F - Measure = \frac{2 * Precision * Recall}{Precision + Recall}$$

Com os dados obtidos em cada uma das execuções é possível realizar os cálculos dos critérios *Precision* e *Recall*, como vamos poder observar. Para o projeto desenvolvido, o critério Precision demonstra a capacidade do sistema de deteção e reconhecimento facial em relação ao reconhecimento em si, em que é avaliada a quantidade de verdadeiros positivos sobre a soma de todos os valores positivos enquanto o critério *Recall* demonstra a capacidade do sistema de deteção e reconhecimento facial, de detetar com sucesso resultados classificados como positivos.

A análise de erros é um passo essencial na interpretação de dados e verifica se existem erros num sistema de deteção e reconhecimento facial, como falsos positivos (o resultado do reconhecimento facial é incorreto e a imagem de entrada não é rejeitada) ou falsos negativos (a imagem de entrada é rejeitada, mas o individuo está presente na base de dados). A capacidade de analisar resultados com base em resultados corretos ou resultados errados seria possibilitada pela identificação de padrões ou outras características dos erros que forneceram informações mais detalhadas acerca das origens dos mesmos. Estas informações mais detalhadas acerca dos erros ou das dificuldades do sistema, podem ter sido uteis para ajudar o pesquisador a identificar quais os pontos que vão necessitar de ser melhorados no futuro. Esta abordagem, também ajudou a identificar o que estava a funcionar corretamente e o que não estava a funcionar corretamente. A performance e os resultados dos testes sobre o sistema desenvolvido de deteção e reconhecimento facial foram representados graficamente através de uma matriz de confusão e calculados através de alguns critérios como a *precision, recall e F-Measure*.

No final do desenvolvimento e implementação do sistema de deteção e reconhecimento facial foi conduzida uma entrevista para avaliar se o mesmo correspondeu às necessidades identificadas pelos elementos participativos. Os resultados desta entrevista foram positivos e todos os elementos participativos viram as suas necessidades e preocupações respondidas pelo sistema implementado.

Todos os testes realizados, tiveram como objetivo analisar se os seus resultados respondiam ou não, às questões de investigação colocadas no início deste projeto. Através dos resultados obtidos, foi possível analisar e concluir que todos os testes foram realizados com sucesso e que todas as questões de investigação, foram apoiadas pelos resultados obtidos. Foi também possível verificar que o uso de alguns acessórios, como os óculos, utilizados no rosto dos utilizadores quando existe uma fraca iluminação, possa tornar mais difícil a deteção do rosto por parte do sistema desenvolvido, uma vez que as lentes vão emitir um reflexo da luz existente no *Display GPIO* instalado no microcomputador *Raspberry Pi 4*. Em contrapartida, o pesquisador verifica que o sistema é robusto no que toca à segurança contra roubos de identidade, quando os utilizadores se expõem ao sistema com diferentes expressões faciais e com o ambiente com fracas condições de iluminação.

Teste 1

Neste cenário de teste, o pesquisador tem como objetivo analisar os resultados quando a envolvência do espaço possui uma fraca iluminação.

Na imagem abaixo podemos observar o pesquisador, que é um dos participantes no teste, exposto à fraca iluminação:

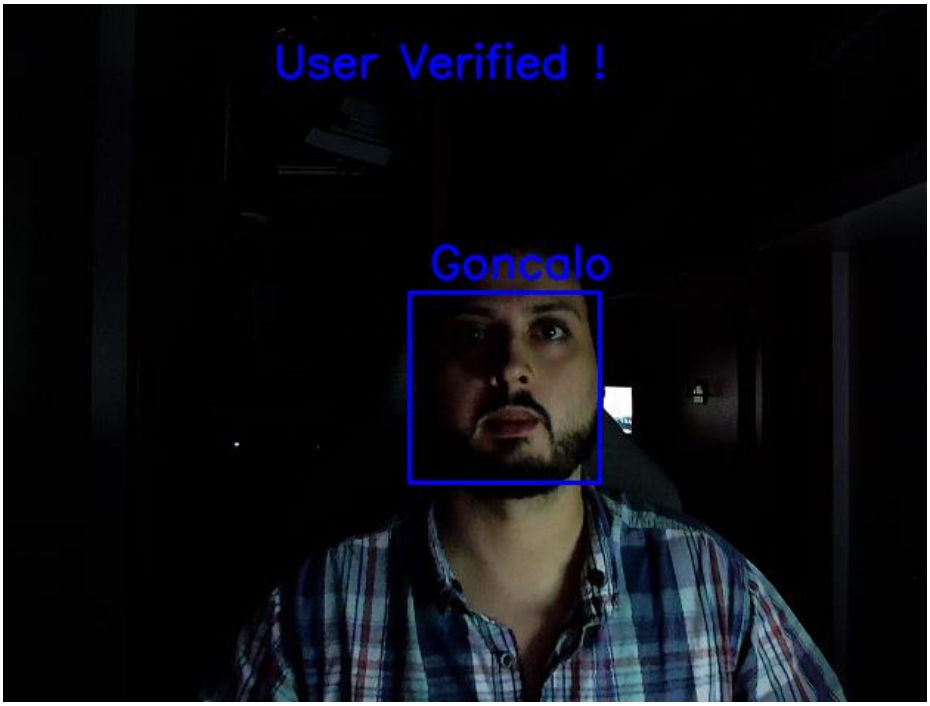


Figura 49 - Utilizador Gonçalo verificado com sucesso no Teste 1 (Garcia, 2023, p.22)

Através de uma matriz de confusão, o pesquisador verificou que nas 15 execuções os resultados foram sempre:

Tabela 1 - Resultados Teste 1 (Garcia, 2023, p.22)

Matriz de confusão		O que foi retornado pelo sistema:	
		Porta Abriu	Porta não Abriu
O que aconteceu na realidade:	Porta Abriu	45	0
	Porta não Abriu	0	0

- Verdadeiros Positivos (VP) = 45
- Falsos Positivos (FP) = 0
- Falsos Negativos (FN) = 0

Dado os resultados, os cálculos foram os seguintes:

$$\textbf{\textit{Precision}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Positivo}} = \frac{45}{45 + 0} = 1.0$$

$$\textbf{\textit{Recall}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Negativo}} = \frac{45}{45 + 0} = 1.0$$

$$\textbf{\textit{F – Measure}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision + Recall}} = \frac{2 * 1.0 * 1.0}{1.0 + 1.0} = 1.0$$

O resultado dos testes foi consistente durante as 15 execuções efetuadas, que levou a que o cálculo final da *F-Measure* fosse 1.0, o que indica que o sistema de deteção e reconhecimento facial teve uma performance perfeita, quando o sistema é exposto a condições de fraca iluminação.

Teste 2

Neste cenário de teste, o pesquisador tem como objetivo analisar os resultados quando os indivíduos utilizam acessórios no seu rosto. Neste caso os participantes colocaram óculos e uns auscultadores.

Na imagem abaixo podemos observar o pesquisador, que é um dos participantes neste teste, exposto à fraca iluminação, com os óculos e auscultadores:

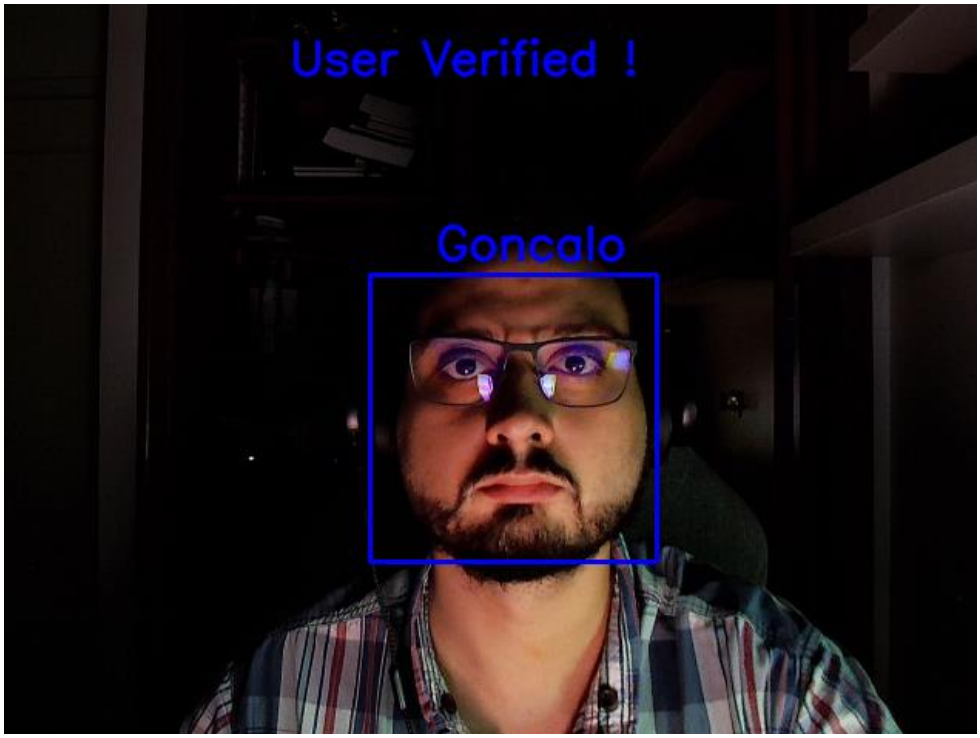


Figura 50 - Utilizador Gonçalo verificado com sucesso no Teste 2 (Garcia, 2023, p.23)

Através de uma matriz de confusão, o pesquisador verificou que nas 15 execuções os resultados foram:

Tabela 2 - Resultados Teste 2 (Garcia, 2023, p.23)

Matriz de confusão		O que foi retornado pelo sistema:	
		Porta Abriu	Porta não Abriu
O que aconteceu na realidade:	Porta Abriu	39	0
	Porta não Abriu	0	6

- Verdadeiros Positivos (VP) = 39
- Falsos Positivos (FP) = 6
- Falsos Negativos (FN) = 0

Dado os resultados, os cálculos foram os seguintes:

$$\textbf{\textit{Precision}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Positivo}} = \frac{39}{39 + 0} = 1.0$$

$$\textbf{\textit{Recall}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Negativo}} = \frac{39}{39 + 6} = 0.86$$

$$\textbf{\textit{F - Measure}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision + Recall}} = \frac{2 * 1.0 * 0.6}{1.0 + 0.6} = 0.92$$

O resultado não foi consistente durante as 15 execuções efetuadas, que levou a que o cálculo final da *F-Measure* fosse 0.92, o que indica que o sistema de deteção e reconhecimento facial teve uma performance suficientemente boa, para que o sistema seja considerado funcional quando os utilizadores utilizam diferentes acessórios nos seus rostos. Uma das dificuldades verificadas pelo pesquisador durante os testes, é que quando são utilizados óculos, existe um reflexo de luminosidade nas lentes, que dificulta a deteção do rosto por parte do sistema.

Teste 3

Neste cenário de teste, o pesquisador tem como objetivo analisar os resultados quando os indivíduos têm expressões faciais, no momento de deteção, diferentes da imagem utilizada inicialmente durante o registo.

Nas imagens abaixo podemos observar o pesquisador, que é um dos participantes neste teste, com expressões faciais diferentes:

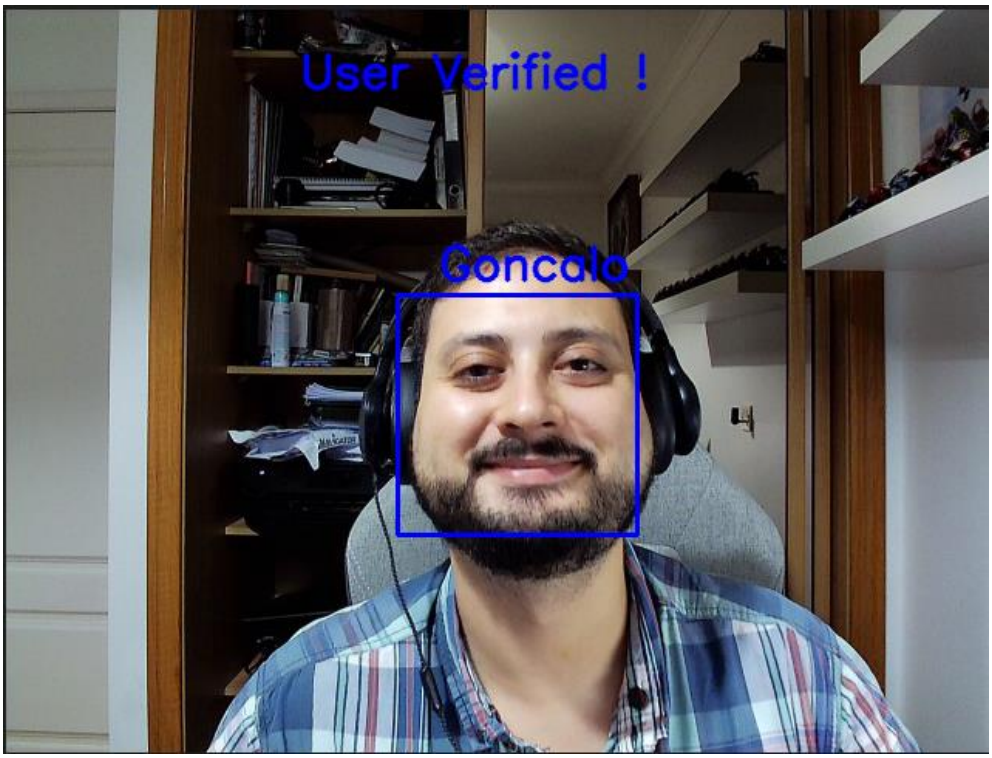


Figura 51 - Utilizador Gonçalo com a expressão facial de felicidade verificado com sucesso no Teste 3 (Garcia, 202, p.24)

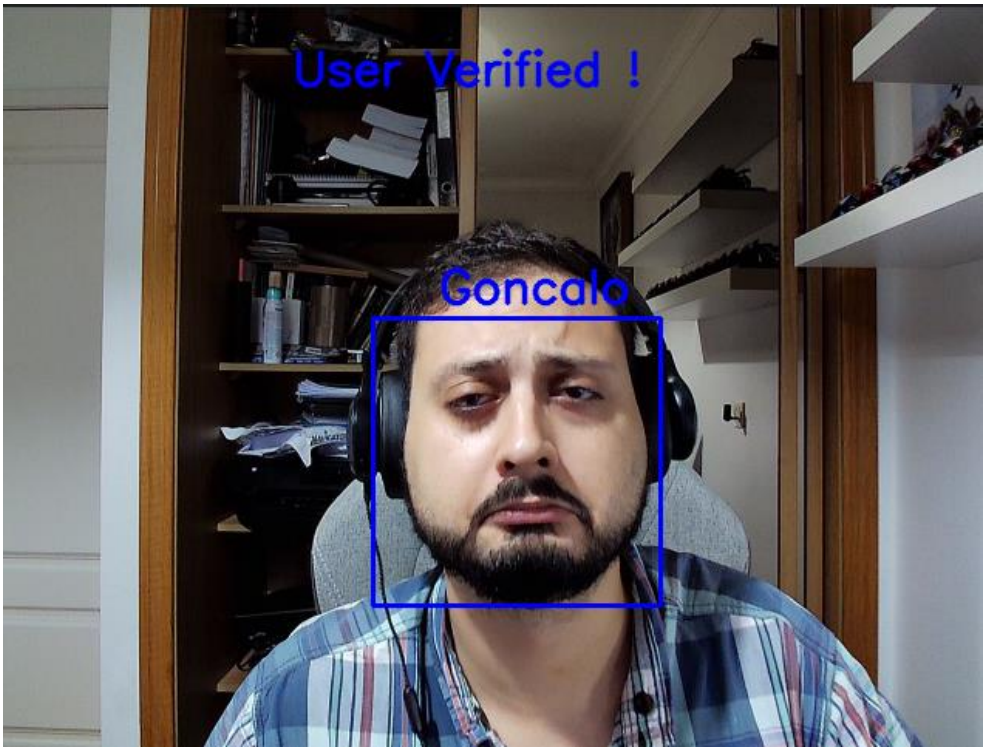


Figura 52 - Utilizador Gonçalo com a expressão facial de infelicidade verificado com sucesso no Teste 3 (Garcia, 2023, p.24)

Através de uma matriz de confusão, o pesquisador verificou que nas 15 execuções os resultados foram sempre:

Expressão facial de felicidade:

Tabela 3 - Resultados do Teste 3 com expressão de felicidade (Garcia, 2023, p.25)

Matriz de confusão		O que foi retornado pelo sistema:	
		Porta Abriu	Porta não Abriu
O que aconteceu na realidade:	Porta Abriu	45	0
	Porta não Abriu	0	0

Expressão facial de infelicidade:

Tabela 4 - Resultados do Teste 3 com expressão de infelicidade (Garcia, 2023, p.25)

Matriz de confusão		O que foi retornado pelo sistema:	
		Porta Abriu	Porta não Abriu
O que aconteceu na realidade:	Porta Abriu	45	0
	Porta não Abriu	0	0

- Verdadeiros Positivos (VP) = 45
- Falsos Positivos (FP) = 0
- Falsos Negativos (FN) = 0

Dado os resultados, os cálculos foram os seguintes:

$$\textbf{\textit{Precision}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Positivo}} = \frac{45}{3 + 0} = 1.0$$

$$\textbf{\textit{Recall}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Negativo}} = \frac{45}{45 + 0} = 1.0$$

$$\textbf{\textit{F - Measure}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision + Recall}} = \frac{2 * 1.0 * 1.0}{1.0 + 1.0} = 1.0$$

O resultado dos testes foi consistente durante as 15 execuções efetuadas, que levou a que o cálculo final da *F-Measure* fosse 1.0, o que indica que o sistema de deteção e reconhecimento facial teve uma performance perfeita, quando os utilizadores têm expressões faciais diferentes em relação à fotografia utilizada durante o registo do utilizador.

Teste 4

Neste cenário de teste, o pesquisador tem como objetivo analisar os resultados quanto à segurança do sistema implementado. Neste cenário, será verificado se o código de verificação está a ser enviado e posteriormente validado no sistema.

Através de uma matriz de confusão, o pesquisador verificou que nas 15 execuções os resultados foram:

Tabela 5 - Resultados do Teste 4 (Garcia, 2023, p.26)

Matriz de confusão		O que foi retornado pelo sistema:			
		Porta Abriu	Porta não Abriu	Código Enviado	Código Validado
O que aconteceu na realidade:	Porta Abriu	45	0	45	45
	Porta não Abriu	0	0	0	0
	Código Enviado	0	0	45	
	Código Validado	45	0	0	45

- Verdadeiros Positivos (VP) = 45
- Falsos Positivos (FP) = 0
- Falsos Negativos (FN) = 0

Dado os resultados, os cálculos foram os seguintes:

$$\textbf{\textit{Precision}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Positivo}} = \frac{45}{45 + 0} = 1.0$$

$$\textbf{\textit{Recall}} = \frac{\text{Verdadeiro Positivo}}{\text{Verdadeiro Positivo + Falso Negativo}} = \frac{45}{45 + 0} = 1.0$$

$$\textbf{\textit{F} - \textit{Measure}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision + Recall}} = \frac{2 * 1.0 * 1.0}{1.0 + 1.0} = 1.0$$

O resultado dos testes foi consistente durante as 15 execuções efetuadas, que levou a que o cálculo final da *F-Measure* fosse 1.0, o que indica que o sistema de deteção e reconhecimento facial teve uma performance perfeita relativamente à segurança do sistema contra o roubo de identidade.

5. Conclusão

A tecnologia de reconhecimento facial tem avançado de forma significativa nas últimas décadas com bastantes potencialidades nos mais diferentes setores. Para que um sistema de reconhecimento facial seja utilizado de forma eficaz, o tipo de iluminação e obstáculos que possam estar presentes no meio ambiente onde a tecnologia de reconhecimento facial será utilizada têm de ser considerados. Abordagens baseadas em *machine learning*, descritores de características e métodos híbridos, que misturam diferentes técnicas na tentativa de a precisão e performance ser melhorada, são os métodos de reconhecimento facial mais eficazes para este tipo de ambientes. No entanto, como a tecnologia de reconhecimento facial tem sido mais utilizada, têm sido discutidas várias preocupações relativamente à segurança e à confidencialidade. Para defesa contra a tentativa de roubos de identidade e garantir acesso a dados privados aos que têm autorização para aceder aos mesmos, vários mecanismos de identificação, como a necessidade de introdução de um código de verificação em conjunto com o sistema de reconhecimento facial, podem ser implementados.

Smartphones, câmaras de videovigilância e microcomputadores são apenas dois exemplos de vários *gadgets* que podem beneficiar de um sistema de deteção e reconhecimento facial. Como resultado de uma grande difusão destas ferramentas, o reconhecimento facial pode ser utilizado para objetivos de segurança, como o reconhecimento de criminosos ou a proibição de acesso a determinadas ferramentas, ou estruturas. Ao escolher uma técnica de reconhecimento facial, é crucial ter em consideração as diversas restrições, como a velocidade de tratamento de imagens e a qualidade das imagens.

A tecnologia de reconhecimento facial também pode ser utilizada para identificar pessoas ou distinguir pessoas com diferentes características faciais, ou expressões distintas. A área da medicina, bem como os setores de marketing e entretenimento, podem ser afetados pelo mencionado anteriormente. A privacidade e os direitos das pessoas não podem ser violados, mas é crucial garantir que estes sistemas sejam legalmente sólidos. Como resultado, um sistema de deteção e reconhecimento facial é uma ferramenta potente com uma ampla gama de aplicações. No entanto, ao escolher e executar um método de reconhecimento facial, é crucial considerar variáveis como a iluminação, segurança e restrições de dispositivos. É crucial garantir que a tecnologia seja utilizada de forma ética e legal à medida que se desenvolve.

Em pesquisas futuras, o grande objetivo é apostar mais nas técnicas e funcionalidades das tecnologias de deteção de rostos, para que o sistema consiga fracionar as diferentes áreas do rosto, como a zona da boca e a zona dos olhos. Desta forma, quando o sistema não conseguisse detetar o rosto devido, por exemplo, devido à utilização de óculos, tentaria que fosse suficientemente 'inteligente' para verificar apenas a zona da boca e comparar estes valores com os valores da zona da boca, existentes na base de dados.

Outra melhoria futura será a criação de um *front-end* para o *AccessFace Sentinel* com o objetivo de elevar a experiência do utilizador para outro nível.

Bibliografia

Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. In *Electronics (Switzerland)* (Vol. 9, Issue 8, pp. 1–53). MDPI AG. https://doi.org/10.3390/electronics9081188

Albahli, S., Alturki, R., Alharbi, M., & AlAnzi, F. (2020). *Deep learning techniques for detecting and recognizing face masks: A survey*.

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00444-8

Bell, J. (1993). *Doing your research project : a guide for first-time researchers in education, health and social science*. McGraw-Hill Open University Press.

Bogdan, R., & Biklen, S. (1994). *Investigacao Qualitativa em Educacao*.

Datta, A. K., Datta, M., & Banerjee, P. K. (2015). *Face Detection and Recognition: Theory and Practice* (1st ed.).

Ecocables. (n.d.). *40 Pin GPIO Raspberry Pi 3 Ribbon Cable*.

Elliott, R., & Timulak, L. (2021). *Descriptive and interpretive approaches to qualitative research: A generic approach*.

EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex. (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)., (2016). https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02016R0679-20160504&qid=1695122789213

Farnell. (n.d.). *RPI4-MODBP-4GB*. Retrieved September 15, 2023, from https://pt.farnell.com/raspberry-pi/rpi4-modbp-4gb/raspberry-pi-4-model-b-4gb/dp/3051887

Fernández Villán, A. (2019). *Mastering OpenCV 4 with Python: A practical guide covering topics from image processing, augmented reality to deep learning with OpenCV 4 and Python 3.7*.

Flynn, P., Prietro, L., & Mery, D. (2019). *Face Recognition in Low Quality Images: A Survey*. *2022-March*. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Garcia, G. (2023). *DIÁRIO DE INVESTIGAÇÃO - OBSERVAÇÃO DE CAMPO (NÃO IMPRESSO)*.

JOY-IT. (n.d.). *RB-TFT-Manual_04082020*.

Julina, J., & Sharmila, S. (2017, June 7). Facial recognition using histogram of gradients and support vector machines. *International Conference on Computer, Communication, and Signal Processing: Special Focus on IoT, ICCCSP 2017*. https://doi.org/10.1109/ICCCSP.2017.7944082

Kapse, A., Kamble, T., Lohar, A., Chaudhari, S., & Puri, D. (2022). Face recognition Attendance system using HOG and CNN algorithm. *ITM Web of Conferences*, *44*, 03028. https://doi.org/10.1051/itmconf/20224403028

Kumar, V. D. A., Kumar, V. D. A., Malathi, S., Vengatesan, K., & Ramakrishnan, M. (2018). Facial Recognition System for Suspect Identification Using a Surveillance Camera. *Pattern Recognition and Image Analysis*, *28*(3), 410–420. https://doi.org/10.1134/S1054661818030136

Lenovo 510 FHD. (n.d.). *Webcam Lenovo 510 FHD 1080p*.

Li, S. Z., & Jain, A. K. (2009). *Handbook of Face Recognition (The Second Edition) Springer-Verlag*.

Liu, T., Yang, B., Geng, Y., & Du, S. (2021). Research on Face Recognition and Privacy. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.809736

Minichino, Joe., & Howse, Joseph. (2015). *Learning OpenCV 3 computer vision with Python : unleash the power of computer vision with Python using OpenCV*. Packt Publishing.

Natércio, A. (2005). *INVESTIGAÇÃO NATURALISTA EM EDUCAÇÃO Um guia prático e crítico*.

Panceri, J. A. C., Pinto, L. A., Pereira, F. G., Cavalieri, D. C., & Komati, K. S. (2015). RECONHECIMENTO FACIAL BASEADO EM HOG E PCA: UMA COMPARAÇÃO QUANTO À INVARIÂNCIA À ILUMINAÇÃO. *Revista Ifes Ciência*, *V1*.

Patil, P., & Shinde, S. (2020). *Comparative analysis of facial recognition models using video for real time attendance monitoring system*. 850–855. https://doi.org/10.1109/ICECA49313.2020.9297374

Paul, K. C., & Aslan, S. (2021). An Improved Real-Time Face Recognition System at Low Resolution Based on Local Binary Pattern Histogram Algorithm and CLAHE. *Optics and Photonics Journal*, *11*(04), 63–78. https://doi.org/10.4236/opj.2021.114005

Queiroz, D. T., Vall, J., Souza, Â. M. A., & Vieira, N. F. C. (2007). *OBSERVAÇÃO PARTICIPANTE NA PESQUISA QUALITATIVA: CONCEITOS E APLICAÇÕES NA ÁREA DA SAÚDE PARTICIPANT OBSERVATION IN QUALITATIVE RESEARCH: CONCEPTS AND APPLICATIONS IN HEALTH* (Vol. 15, Issue 2).

Raspberry. (n.d.). *Raspberry Pi hardware: GPIO and the 40-pin Header*. Retrieved September 15, 2023, from https://www.raspberrypi.com/documentation/computers/raspberry-pi.html

Rathgeb, C., Kolberg, J., Uhl, A., & Busch, C. (2023). *Deep Learning in the Field of Biometric Template Protection: An Overview*. http://arxiv.org/abs/2303.02715

Ryan, P. (2019). *Facial Recognition — a visual step by step*. https://medium.com/swlh/facial-recognition-a-visual-step-by-step-d679289bab11

Schenkel, T., Ringhage, O., Márki, A., & Bae, J. (2019). *A COMPARATIVE STUDY OF FACIAL RECOGNITION TECHNIQUES With focus on low computational power Bachelor Degree Project in Information Technology Basic level 30 ECTS Spring term 2019*.

Servo Motor MG995. (n.d.). *Servo Motor MG995 180 Graus Tower Pro*. Retrieved September 15, 2023, from https://www.electrofun.pt/servo-motores/servo-motor-mg995-180-graus-tower-pro

Syafeeza, A. R., Alif, M. K. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, *11*(1), 417–424. https://doi.org/10.11591/ijpeds.v11.i1.pp417-424

Vemou, K., & Horvath, A. (2020, April 21). Facial Emotion Recognition. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376680

Vimal, C. (2022). Face Detection's Various Techniques and Approaches: A Review. *International Journal for Research in Applied Science and Engineering Technology*, *10*(1), 839–843. https://doi.org/10.22214/ijraset.2022.39890

Xie, X., & Lam, K.-M. (2005). *An efficient method for face recognition under varying illumination*. 3841-3844 Vol. 4. https://doi.org/10.1109/ISCAS.2005.1465468