Tecnologias de Autenticação

Licenciatura em Eng. Informática

Segurança Informática 2022-2023

UNIVERSIDADE DE ÉVORA
ESCOLA DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE INFORMÁTICA

Diogo Mestre nº48973, Rodrigo Alves nº 48681

Docente responsável pela cadeira: Professor Pedro Patinho

Trabalho desenvolvido no âmbito da disciplina de Segurança Informática da Licenciatura em Eng. Informática.

Évora, 19 de junho de 2023

Conteúdo

1 Introdução

O documento enquadra-se no âmbito da unidade curricular de Segurança Informática e tem por objetivo dar a conhecer o trabalho de pesquisa, bem como o trabalho prático que nos foi proposto. De entre todos os temas abordados desta unidade decidimos escolher as tecnologias de autenticação e o Reconhecimento Facial para o trabalho de pesquisa e para o trabalho prático respetivamente.

Como mencionado previamente, este documento vai começar por introduzir o que são as tecnologias de autenticação, ou seja, vai ser descrito ao detalhe tudo acerca deste tema, as vantagens e desvantagens. De seguida, vão ser apresentados vários exemplos desta tecnologia sendo que iremos dar um maior ênfase à tecnologia selecionada para a realização da parte prática, o Reconhecimento Facial.

Existe um vasto conjunto de opções de tecnologias de autenticação, sendo que optámos por concentrar a nossa análise e pesquisa no Reconhecimento Facial, uma vez que esta escolha foi motivada pelo crescente interesse e implementação desta tecnologia num amplo conjunto de setores, desde a segurança pessoal até à identificação em sistemas biométricos avançados. É importante salientar, que reconhecemos a importância do Reconhecimento Facial como uma solução promissora e, portanto, decidimos dedicar uma secção prática específica a esta tecnologia.

2 O que são Tecnologias de Autenticação

A autenticação surgiu por volta da década de 1960, com o surgimento das primeiras bases de dados com senhas, sendo que os utilizadores tinham que possuir a senha que correspondesse à do armazenamento. Embora o processo de autenticação tenha evoluído bastante desde as décadas de 1960 e 1970, principalmente com o surgimento da criptografia, as senhas são ainda a forma de autenticação mais utilizada.

Desta forma, a autenticação não é nada mais do que o processo tecnológico que permite que uma pessoa prove que tem as permissões necessárias para aceder a determinados ambientes. Este processo dispensa a necessidade de verificação humana e presencial, uma vez que a autenticação pode ser feita a partir de dispositivos e localidades diferentes.

Figura 1: Autenticação

As tecnologias de autenticação são métodos e sistemas utilizados para verificar a identidade de um utilizador ou dispositivo. Estas tecnologias são aplicadas de forma a garantir que apenas pessoas autorizadas consigam aceder aos sistemas, serviços ou informações específicas. Neste documento vão ser identificadas e descritas uma grande parte das tecnologias de autenticação na Secção 3.

Assim a autenticação desempenha um papel fundamental na segurança da informação e na proteção contra acessos não autorizados, ou seja, este processo serve para confirmar se os utilizadores de certos

sistemas são legítimos e autênticos, de modo a comprovar que quem reivindica algum tipo de acesso é a pessoa que afirma ser.

Esta camada de proteção é resultado da utilização de ferramentas tecnológicas avançadas, como autenticação biométrica e autenticação de dois fatores, que reforçam a segurança dos sistemas, protegendo-os contra acessos não autorizados, roubo de dados e ameaças cibernéticas.

Estas tecnologias podem variar em termos de segurança, usabilidade, implementação, requisitos e nos contextos onde são utilizadas. Contudo os seus objetivos mantém-se, sendo estes: melhorar a segurança, proteger os sistemas e informações e garantir a privacidade, confidencialidade e integridade dos dados.

Em suma, as tecnologias de autenticação são extremamente importantes para garantir a segurança e a proteção de informações. Ao longo dos anos, estas tecnologias têm vindo a evoluir, de forma a proporcionar uma análise precisa e confiável da identidade dos utilizadores. Para além disso, estas tecnologias oferecem uma maior proteção contra acessos não autorizados, garantindo a privacidade e integridade dos dados e uma maior tranquilidade ao utilizador.

3 Exemplos de Tecnologias

3.1 Certificado digital

O objetivo do certificado digital é verificar se um certo procedimento está de acordo com as normas de segurança. Em muitos casos, pode ser visto como uma espécie de identidade digital, uma vez que é utilizado de forma a validar a identidade do utilizador em certas plataformas e sistemas. Este mecanismo possui inúmeras funcionalidades como, a assinatura de documentos, a realização de transações, o acesso a sistemas públicos, entre outras.

São documentos eletrónicos utilizados para a autenticação de utilizadores, de organizações e de dispositivos ou serviços na internet, para estabelecer comunicações seguras e confiáveis, de forma a garantir a autenticidade, integridade e privacidade dos dados transmitidos.

O certificado digital é obrigatório em algumas empresas e pode ser usado em conjunto com a chave pública e a chave privada. Estes são emitidos por uma Autoridade Certificadora (AC) confiável, que é responsável por verificar a identidade do requerente antes de o emitir.

A assinatura digital é uma forma de criptografia que garante a autenticidade do certificado e que impede que o mesmo seja alterado ou falsificado, uma vez que tem a mesma validade legal que uma assinatura à mão, e é válida em qualquer software onde é permitido assinar digitalmente.

Esta tecnologia possui várias vantagens e desvantagens. De entre as vantagens podemos destacar:

- Possibilidade de empresas com várias unidades partilharem o mesmo certificado, de forma a diminuir os custos;
- Permite ter conexões seguras (como o protocolo *HTTPS*);
- Garantem: a autenticidade na identificação do titular, a integridade dos dados (assegurando que as informações não foram manipuladas) e a privacidade das informações transmitidos;
- Permite que os dados sejam armazenados e que ocorra um back-up das informações transmitidas.

Algumas das desvantagens desta tecnologia são:

- A complexidade da implementação e da gestão dos certificado, uma vez que exige conhecimentos técnicos e recursos adequados;
- A fiabilidade destes está diretamente dependente da credibilidade/confiabilidade da Autoridade Certificadora que os emite;
- Os custos envolventes às suas manutenções e renovações;
- Perda de credibilidade e risco de perda ou de danos, caso este não sejam atualizados.

3.2 Autenticação com chave pública e privada

A tecnologia de autenticação com chave pública e privada é utilizada na criptografia com chave assimétrica, que tende a ser mais lenta e necessita de um maior poder computacional, no entanto é um excelente método para garantir a segurança num canal público e inseguro.

Nesta, cada entidade (por exemplo, uma pessoa ou um dispositivo) possui um par de chaves: uma chave pública e uma chave privada, sendo que uma é para codificar e a outra para descodificar.

A chave pública pode ser compartilhada com outras entidades, desde que esteja no sistema ou servidor. Por sua vez a privada é mantida em segredo, não é divulgada e é apenas acessível ao autor da mesma, incumbindo-lhe a sua criptografia. Ambas as chaves estão matematicamente relacionadas, ou seja, o conteúdo que é encriptado com a chave pública só pode ser desencriptado pela chave privada correspondente e vice versa, assim qualquer entidade pode encriptar uma mensagem usando a chave pública do destinatário (que é partilhada entre emissor e recetor) e só a chave privada do recetor permite decifrar a informação. A geração das chaves públicas e privadas é computacionalmente económica, fácil de realizar e de utilizar.

A segurança de um sistema de criptografia de chave pública reside no esforço computacional necessário para encontrar a chave privada correspondente à chave pública. Portanto, a chave privada é o elemento essencial para garantir a segurança efetiva do sistema. Por outro lado, a chave pública pode ser livremente distribuída sem comprometer a segurança, uma vez que a sua divulgação não permite a dedução da chave privada correspondente. Assim a segurança depende apenas da capacidade de manter secreta a chave privada.

Esta apresenta algumas vantagens mas também algumas desvantagens. Nas vantagens destacam-se:

- Oferece um alto nível de segurança, uma vez que a chave privada permanece exclusiva ao proprietário e é quase impossível de ser descoberta através da pública;
- Não depende de passwords para a autenticação e não está vulnerável a ataques de força bruta;
- Permite a utilização de assinaturas digitais, que fornecem uma prova não repudiável da autoria da mensagem;
- Permite a partilha segura de informações.

As desvantagens desta tecnologia são:

- Esta necessita que as chaves sejam geridas adequadamente e a sua gestão apresenta uma certa complexidade, nomeadamente em certos ambientes com vários utilizadores;
- Requer uma infraestrutura confiável de certificados, de forma a garantir a autenticidade dos pares de chaves;
- A utilização das chaves pode ser mais difícil para utilizadores com menos conhecimentos;
- É necessário realizar backups para evitar a perda de chaves privadas e com estas a perda permanente de acesso a informações encriptadas e a perda na capacidade de se autenticar.

3.3 Token

Um token é uma tecnologia de autenticação usada em sistemas de segurança e acesso a recursos digitais. Serve para fazer a autenticação de sistemas web onde existe uma relação entre o utilizador e o servidor, ou seja, um token de autenticação transmite com segurança informações sobre identidades dos utilizadores entre aplicações e sites. Oferece ao utilizador um conjunto de códigos e chaves aleatórias, que podem ser substituídas num curto período de tempo, ou seja, tem um curto período de vida.

O token funciona da seguinte maneira: o utilizador realiza o login numa página, e é gerado um token (pode ser um código ou um valor único) que lhe dá permissão para entrar no site ou aplicação e utilizar os recursos num certo período de tempo, sem que necessite fazer o login novamente. Este também é compartilhado com aplicações/sites conectados para verificar a sua identidade.

Existem diferentes tipos de tokens usados para realizar a autenticação como:

- Tokens de hardware - São dispositivos físicos que permitem guardar chaves criptográficas.

- Tokens de software - São gerados pelas aplicações/sites para uso temporário. Estes são baseados em algorítmos criptográficos.

Como todas as tecnologias de autenticação esta possui tanto vantagens como desvantagens. As vantagens são:

- Fornece um nível adicional de segurança, uma vez que são mais difíceis de serem comprometidos por ataques de força bruta;
- Por serem compostos por códigos ou valores difíceis de serem decifrados torna esta tecnologia mais segura contra ataques de fishing;
- Possui uma maior flexibilidade e portabilidade, permitindo que os utilizadores se autentiquem de uma forma mais conveniente em diferentes dispositivos;
- Melhor experiência, pois permite aceder às contas em múltiplos dispositivos;
- Os tokens expiram, ou seja, estes são destruídos quando é terminada a sessão, garantindo uma maior proteção das contas.

As desvantagens são:

- Para tokens de hardware é necessário possuir o dispositivo físico para se autenticar;
- Pode exigir investimentos em infraestruturas;
- Um token físico pode ser roubado ou perdido, comprometendo a segurança da autenticação;
- Um token de software pode ser corrompido, o que também compromete a segurança.

3.4 Passwords e SMS

A password é uma tecnologia de autenticação que pode ser definida por uma senha ou por um pin. Enquanto que a senha pode ser composta por diferentes tipos de caracteres, o pin é formado por uma combinação numérica, a qual somente o utilizador deve conhecer.

A senha é um dos mecanismos mais conhecidos para autenticação digital e são utilizadas basicamente em todos os tipos de serviços, enquanto que os pin's vêm logo depois, sendo assim usados especialmente na autenticação de sistemas bancários.

A utilização de passwords oferece as seguintes vantagens:

- Possui um método de autenticação amplamente adotado devido à sua simplicidade de utilização e entendimento;
- A implementação e a manutenção destes sistemas tendem a ser relativamente baratas em comparação com outras formas de autenticação;
- Apresenta uma maior facilidade na sua alteração caso seja decifrada por um invasor.

Contudo existem as seguintes desvantagens:

- Esquecimento das passwords por motivos de fraqueza humana ou por exigência de complexidade neste tipo de acessos;
- Reutilização de uma password pode comprometer um serviço.

Outra tecnologia semelhante à anterior é o SMS, esta não é comum entre as empresas, pois é mais utilizada no âmbito pessoal. Esta é considerada um dos mecanismos mais versáteis, pois oferece a possibilidade de enviar lembretes para os utilizadores e a possibilidade de manter um canal próximo de comunicação. Além disso, o SMS é uma ferramenta que garante a segurança tanto dos utilizadores como das informações.

Este apresenta as seguintes vantagens:

- Capacidade de receber mensagens de texto o que a torna uma opção de autenticação amplamente acessível;
- Só um único número específico recebe a informação;

No entanto também apresenta desvantagens como:

- Possibilidade de interceção das mensagens durante o envio das mesmas;
- Dependência dos serviços de envio das mensagens (por exemplo, das operadoras);
- Nem todos possuem um número de telemóvel válido e existe ainda a possibilidade dos mesmos estarem situados numa região onde existem condições adversas à autenticação.

3.5 Geometria da mão

A geometria da mão é uma das tecnologias de autenticação que utiliza características físicas e espaciais da mão de um individuo com o objetivo de verificar a identidade. Esta tecnologia utiliza algoritmos e sensores infravermelhos para recolher e analisar dados relacionados com a geometria da mão, como: tamanho, forma, proporções e características únicas, como veias, linhas e rugas da pele. Estes dados vão ser posteriormente comparados com as informações que já se encontram armazenadas.

Esta tecnologia de autenticação oferece várias vantagens, tais como:

- Alta segurança uma vez que oferece um alto nível de precisão na identificação de uma pessoa com base nas características específicas da mão, únicas para cada indivíduo, ou seja, é extremamente difícil ser falsificada;
- É rápida e conveniente o que permiti aos utilizadores acederem a dispositivos ou a serviços com facilidade, sem a necessidade de senhas ou cartões de identificação.

Contudo, esta tecnologia possui algumas desvantagens:

- Pode comprometer a privacidade dos dados biométricos recolhidos das pessoas;
- Em certos casos esta pode não ser adequado a todos, pois se o sujeito possuir problemas de saúde como por exemplo deficiências físicas nas mãos, esta tecnologia torna-se quase impossível de utilizar.

3.6 Impressão digital

A impressão digital é uma das tecnologias de autenticação biométricas mais utilizadas para verificar a identidade de uma pessoa. Esta tecnologia utiliza sensores infravermelhos para recolher a imagem da impressão digital do utilizador.

Após a captura da impressão digital, os algoritmos de autenticação analisam os padrões e características presentes, como bifurcações, loops e pontos de terminação. Estes dados são comparados com as informações armazenadas previamente na base de dados para verificar a identidade do utilizador.

Esta tecnologia de autenticação oferece várias vantagens, tais como:

- Alta precisão na identificação do utilizador;
- Facilidade/Conveniência na utilização, uma vez que a impressão digital está sempre disponível e não requer o uso de senhas ou cartões adicionais;
- É considerada uma forma segura de autenticação, uma vez que é difícil ser replicada ou falsificada.

Contudo existem algumas desvantagens na sua utilização:

- Embora as impressões digitais sejam únicas para cada indivíduo, não são invioláveis;
- A autenticação requer a recolha de dados que posteriormente vão ser guardados, o que pode causar preocupações em relação à privacidade dos mesmos;
- Se a impressão digital for danificada ou alterada devido a ferimentos, queimaduras ou outros fatores, a autenticação através da mesma pode-se tornar problemática ou mesmo impossível;
- Algumas pessoas podem ter dificuldade em a utilizar por razões de saúde;

4 Reconhecimento Facial

4.1 O que é o Reconhecimento Facial?

Reconhecimento facial é uma forma de identificar ou verificar a identidade de uma pessoa com base nas características do seu rosto, sendo por isso que esta tecnologia faz parte da segurança biométrica. Os sistemas de reconhecimento facial podem ser usados para identificar pessoas em fotos, vídeos ou em tempo real.

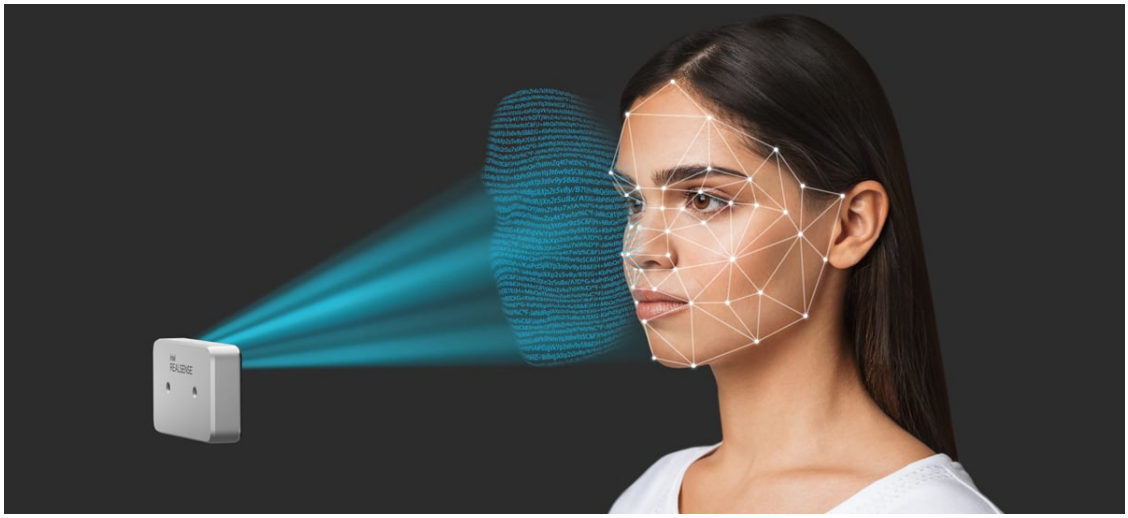

Figura 2: Reconhecimento Facial

4.2 Como funciona?

Esta tecnologia é muito conhecida hoje em dia graças ao Face ID, que é usado para desbloquear um smartphone. Normalmente, o reconhecimento facial não conta com uma base de dados vasta de fotos para determinar a identidade de uma pessoa; ele simplesmente a identifica e reconhece como sendo a proprietária única do dispositivo, limitando o acesso de outros.

Além disso, o reconhecimento facial funciona através da realização da correspondência entre os rostos de pessoas por meio de câmeras especiais e de imagens numa lista de observação. As listas de observação podem conter imagens de qualquer pessoa, incluindo pessoas que não são suspeitas de irregularidades e ainda de imagens provenientes de qualquer lugar, até mesmo das nossas contas nas redes sociais.

O funcionamento dos sistemas de tecnologia facial tendem a executar as seguintes operações por esta ordem:

1. Deteção do rosto

   Após a captura de um elemento visual é realizada a deteção e localização de um rosto.

2. Análise do rosto

   De seguida a imagem do rosto é capturada e analisada, sendo que a análise é executada pelo software que faz a leitura da geometria do rosto que foi encontrado. Os principais fatores que podem influenciar o resultado desta operação são a distância entre os seus olhos, a profundidade das suas órbitas oculares, a distância entre a testa e o queixo, o formato da maçã do rosto e o contorno dos lábios, das orelhas e do queixo. O objetivo desta etapa é identificar os pontos de referência faciais principais que distinguem o rosto e que vão ajudar a realizar o processo de identificação de uma pessoa.

3. Conversão da imagem em dados

   O processo de captura facial transforma as informações analógicas (um rosto) num conjunto de informações digitais (dados) com base nas características faciais da pessoa. A análise do rosto

é basicamente transformada numa fórmula matemática. O código numérico é chamado de impressão facial. Da mesma forma as impressões digitais são únicas, cada pessoa possui a sua própria impressão facial.

4. Localização de uma correspondência

   A impressão facial é comparada com uma base de dados de outros rostos conhecidos. Caso a impressão facial corresponda a uma imagem da base de dados de reconhecimento facial, a sua validação será feita.

4.3 Como é usado?

De todas as medições biométricas, o reconhecimento facial é considerado o mais natural. Desta forma esta tecnologia é utilizada com vários propósitos, tais como:

- Desbloquear telefones

  Vários smartphones usam o reconhecimento facial para desbloquear o dispositivo. A tecnologia oferece um meio eficiente de proteger dados pessoais e garante que os dados confidenciais permaneçam inacessíveis caso o telefone seja roubado.

- Aplicação da lei

  Regularmente, o reconhecimento facial tem vindo a ser usado pelas autoridades, de forma a que a aplicação da lei seja cumprida de forma correta.

- Controlo de aeroportos

  O reconhecimento facial tornou-se uma sinalização conhecida em muitos aeroportos. Cada vez mais há um maior número de passageiros que utiliza passaportes biométricos, pois estes permitem "saltar"o controlo automatizado de passaportes eletrónicos. Assim este tipo de reconhecimento não apenas reduz o tempo gasto, como também permite que o aeroporto reforce a segurança.

- Encontrar pessoas desaparecidas

  O reconhecimento facial pode ser usado para encontrar pessoas desaparecidas e vítimas de tráfico humano. Suponhamos que pessoas desaparecidas tenham sido adicionadas a uma base de dados. Nesse caso, a polícia pode ser alertada assim que elas forem identificadas por reconhecimento facial, independentemente se for num aeroporto, estabelecimento comercial ou outro espaço público.

- Redução de crimes em estabelecimentos comerciais

  O reconhecimento facial é usado para identificar quando ladrões conhecidos, organizações criminosas ou pessoas com um histórico de fraude entram em lojas. As imagens dessas pessoas podem ser comparadas às de grandes bases de dados de imagens de criminosos para que os profissionais de prevenção de perdas e de segurança sejam notificados quando ladrões que potencialmente representam uma ameaça entrarem na loja.

- Operações bancárias

  A biometria em operações bancárias online é outro benefício do reconhecimento facial, pois em vez de usarmos senhas de uso único, os clientes podem autorizar as transações com um simples olhar para o smartphone ou computador. Desta forma, o facto de não serem utilizadas senhas de acesso, os hackers não vão conseguir roubar as informações dos clientes.

- Serviços de saúde

  Os hospitais usam o reconhecimento facial para ajudar no tratamento dos pacientes, quer seja no acesso aos registos dos mesmo, no registo de paciente e até na identificação de doenças geneticamente específicas.

4.4 Vantagens & Desvantagens

O reconhecimento facial oferece várias vantagens em diferentes áreas de aplicação:

- Reforço na segurança

  O reconhecimento facial facilita a deteção de assaltantes e de invasores, pois a nível pessoal, este pode ser usado como uma ferramenta de segurança que bloqueia dispositivos e câmeras de vigilância. Além disso, as empresas podem também usar esta tecnologia como substituta de senhas de acesso a dispositivos.

- Maior conveniência

  Com a generalização desta tecnologia, poderão ser feitas operações num curto espaço de tempo, como por exemplo os clientes poderão pagar as suas compras usando o reconhecimento facial, em vez de ter que tirar cartões de crédito ou dinheiro do bolso.

- Processamento mais rápido

  O processo de reconhecimento facial leva apenas um segundo, o que traz benefícios para as empresas que utilizam essa tecnologia. Numa era de ataques cibernéticos e ferramentas de hackeamento avançadas, as empresas precisam de tecnologias seguras e rápidas. O reconhecimento facial permite a verificação rápida e eficiente da identidade de uma pessoa.

- Integração com outras tecnologias

  A maioria das soluções de reconhecimento facial é compatível com a maioria dos softwares de segurança e é integrada de forma fácil sobre as mesmas.

Esta tecnologia apresenta algumas desvantagens, tais como:

- Vigilância

  Existe uma preocupação com o facto de que o uso de reconhecimento facial juntamente com câmeras de vídeo omnipresentes, inteligência artificial e análise de dados crie a possibilidade de vigilância em massa, o que poderá restringir a liberdade individual. Embora a tecnologia de reconhecimento facial possibilite que órgãos do governo rastreiem criminosos, ela também permite o rastreamento a qualquer momento de pessoas comuns e inocentes.

- Possibilidade de erros

  Os dados obtidos com o reconhecimento facial estão passíveis a erros, o que pode levar pessoas a serem culpadas por crimes que não cometeram. Por exemplo, uma leve mudança no ângulo da câmera ou mudança de aparência, como um novo estilo de cabelo, pode levar a um erro.

- Violação da privacidade

  A questão da ética e privacidade é a mais controversa. Sabe-se que órgãos do governo armazenam imagens de vários cidadãos sem o seu consentimento.

- Armazenamento de dados em massa

  O software de reconhecimento facial conta com a tecnologia de *machine learning*, que requer conjuntos de dados em massa para "aprender"e oferecer resultados precisos. Estes conjuntos volumosos de dados requerem armazenamento eficiente. Empresas de pequeno e médio porte podem não ter recursos suficientes para armazenar os dados necessários.

5 Parte Prática - FaceRecognation

```
print("#########################################################################################")

print(" _____                  ____                                  _  _    _                 ")
print("|  ___|__ _   ___  ___ |  _ \   ___   ___  ___    __ _  _ __  (_)| |_ (_)  ___   _ __  ")
print("| |_  / _` | / __|/ _ \| |_) | / _ \ / __|/ _ \  / _` || '_ \ | || __|| | / _ \ | '_ \ ")
print("|  _|| (_| || (__|  __/|  _ < |  __/| (__| (_) || (_| || | | || || |_ | || (_) || | | |")
print("|_|   \__,_| \___|\___||_| \_\ \___| \___|\___/  \__, ||_| |_||_| \__||_| \___/ |_| |_|")
print("                                                   |___/                                 ")
print("")
print("#########################################################################################")
```

Nesta secção serão apresentados todos os detalhes acerca do programa **FaceRecognation** que foi desenvolvido, com o objetivo de demonstrar a segurança de autenticação através do reconhecimento facial. O programa que foi implementado utiliza técnicas avançadas de visão computacional para garantir a segurança na autenticação dos utilizadores.

Estas técnicas combinam algoritmos sofisticados que analisam e reconhecem os traços faciais dos utilizadores, garantindo uma autenticação confiável e precisa. Desta forma, o programa é capaz de verificar e confirmar a identidade dos utilizadores com segurança, evitando acessos não autorizados. Deste modo, iremos apresentar as conclusões retiradas durante a experimentação das diferentes operações disponíveis(imagens, câmara) no programa.

5.1 Bibliotecas Utilizadas

De forma a conseguir utilizar as técnicas avançadas da visão computacional, foi necessário para o desenvolvimento deste projeto a introdução de bibliotecas. Estas são fundamentais para alcançar o objetivo deste trabalho. De seguida vão ser apresentadas todas as bibliotecas utilizadas bem como as suas características.

```
import cv2
import numpy as np
import face_recognition as fr
import time
from rich.console import Console
from data import recognize, get_users
from PIL import Image
```

5.1.1 Biblioteca cv2

A biblioteca cv2 é uma das bibliotecas mais populares e amplamente utilizadas para processamento de imagens e visão computacional em *Python*. Esta biblioteca fornece uma interface para a biblioteca OpenCV (Open Source Computer Vision Library), que contém um conjunto abrangente de funções e algoritmos para manipulação e análise de imagens e vídeos.

A cv2 é amplamente utilizada em aplicações da visão computacional, desde tarefas simples de processamento de imagens até projetos mais complexos que envolvem análise de vídeo em tempo real e interação com câmeras, sendo esta biblioteca conhecida pela sua eficiência e usabilidade.

Para a introdução desta biblioteca no trabalho foi necessário utilizar o seguinte comando:

```
pip install opencv-python
```

5.1.2 Biblioteca numpy

A biblioteca numpy é uma poderosa biblioteca para computação científica em Python. Esta biblioteca fornece um suporte para manipulação eficiente de arrays multidimensionais, juntamente com um grande conjunto de funções matemáticas de alto desempenho para a realização de operações com um grande número de dados.

A principal estrutura de dados fornecida pelo numpy é o objeto ndarray (N-dimensional array), que é uma matriz multidimensional homogênea de elementos do mesmo tipo. Estes arrays permitem armazenar e manipular grandes conjuntos de dados de forma eficiente, além de fornecer um grande conjunto de operações matemáticas e lógicas. A numpy é frequentemente usada em conjunto com outras bibliotecas científicas em Python, como pandas, matplotlib e scikit-learn, para realizar análise de dados, visualização e modelagem estatística.

Para a introdução desta biblioteca no trabalho foi necessário utilizar o seguinte comando:

```
pip install numpy
```

5.1.3 Biblioteca face_recognition

A biblioteca face_recognition é uma biblioteca de reconhecimento facial em Python que simplifica o processo de deteção, análise e reconhecimento de rostos em imagens e vídeos. A principal funcionalidade desta biblioteca é o reconhecimento facial, que permite identificar e comparar rostos em imagens.

A face_recognition é capaz de localizar automaticamente os rostos numa imagem, extrair características distintivas dos rostos detetados e compará-los com outros rostos numa base de dados para realizar reconhecimento facial. Esta biblioteca é construída a partir de outras bibliotecas populares, como dlib e numpy, e possui uma interface de alto nível que simplifica a implementação de recursos de reconhecimento facial em projetos Python.

A biblioteca face_recognition possui uma API simples e intuitiva, permitindo a realização de tarefas complexas de reconhecimento facial em poucas linhas de código. Além disso, a face_recognition é conhecida pela sua precisão e desempenho, tornando-a numa escolha popular em projetos de visão computacional que envolvam o reconhecimento facial.

Para a introdução desta biblioteca no trabalho foi necessário utilizar o seguinte comando:

```
pip install face_recognition
```

5.1.4 Biblioteca time

A biblioteca time é uma biblioteca padrão do Python que fornece funções relacionadas ao tempo e à medição de intervalos de tempo. Esta biblioteca permite trabalhar com informações de data, hora e realizar operações relacionadas com a medição de tempo. Como a biblioteca time faz parte da biblioteca padrão do Python, não é necessário instalá-la separadamente.

Para utilizar a biblioteca time, é apenas necessário importá-la a partir do seguinte código Python:

```
import time
```

5.1.5 Biblioteca rich.console

A biblioteca rich.console é uma biblioteca Python que oferece recursos avançados de formatação e exibição de texto no terminal. A principal funcionalidade da biblioteca rich.console é melhorar a experiência de visualização de texto no terminal. Esta biblioteca oferece uma série de recursos que permitem formatar e realçar o texto, tornando-o mais legível e atraente.

Para a introdução desta biblioteca no trabalho foi necessário utilizar o seguinte comando:

```
pip install rich
```

5.1.6 Biblioteca PIL

A biblioteca PIL (Python Imaging Library) é uma biblioteca popular em Python para manipulação e processamento de imagens, fornecendo uma ampla gama de funcionalidades para as suas edições em diferentes formatos a partir de uma API intuitiva e fácil de usar.

A principal funcionalidade da biblioteca PIL é a capacidade de carregar, criar e salvar imagens em vários formatos, como JPEG, PNG, BMP, TIFF e muitos outros. Além disso esta biblioteca permite abrir imagens existentes a partir de arquivos ou URLs, bem como criar novas imagens em branco para posterior edição.

Para a introdução desta biblioteca no trabalho foi necessário utilizar o seguinte comando:

```
pip install Pillow
```

5.2 Funcionalidades

Ao iniciar o programa com o seguinte comando no terminal:

```
python3 main.py
```

Vai ser apresentado um menu onde o utilizador poderá escolher uma das seguintes opções:

```
print("     __  __                              ")
print("    |  \/  | ___ _ __  _   _             ")
print("    | |\/| |/ _ \ '_ \| | | |            ")
print("    | |  | |  __/ | | | |_| |            ")
print("----|_|  |_|\___|_| |_|\__,_|------------")
print("|                                       |")
print("|   [1] Autentication                   |")
print("|   [2] Registration                    |")
print("|   [3] Testing                         |")
print("|   [4] Exit                            |")
print("|                                       |")
print("-----------------------------------------")
```

```
print("                                         ")
print("-----------------------------------------")
print("|                                       |")
print("|   [1] Images                          |")
print("|   [2] Camera                          |")
print("|                                       |")
print("-----------------------------------------")
```

Ao selecionar a opção "Autenticação"esta irá verificar a autenticidade do utilizador que está situado em frente à câmara. É realizada uma pesquisa na base de dados a partir do capturado pela câmara através das bibliotecas que foram descritas nos pontos 5.1.1, 5.1.2 e 5.1.3.

O programa começa por inicializar a câmara e processar cada frame da captura que recebe, convertendo-a para um formato RGB para realizar o reconhecimento facial. De seguida o código identifica a localização do rosto e codifica as suas características que são comparadas com as presentes na base de dados.

A escolha da melhor correspondência é feita através do cálculo das distâncias entre as codificações faciais. Quando existe uma correspondência, será apresentado uma mensagem de autenticação bem sucedida.

No caso de selecionar a opção "Registo"será pedido ao utilizador para inserir o nome e o caminho de uma imagem que o identifique. Depois a imagem é-lhe exibida de forma a verificar se o utilizador pretende registar-se com a mesma. Caso a resposta seja sim o programa realiza uma chamada à função *recognize* de forma a processá-la e a validá-la. Após a aprovação a imagem e o nome do utilizador são incorporados na base de dados.

Após a seleção da opção "Testagem"é mostrado ao utilizador duas opções. Se for escolhida a primeira opção é solicitado ao utilizador o caminho de uma imagem para que o programa seja capaz de reconhecer o rosto da mesma de forma a testá-lo. Caso seja escolhida a segunda o programa irá utilizar a câmara para reconhecer os rostos em tempo real. Os rostos detetados serão então comparados com os valores presentes na base de dados e se houver correspondência o nome do utilizador é exibido no ecrã.

5.3 Experiência Realizada

De forma a verificar a segurança do nosso programa, foram realizados vários testes com diversas imagens e através do auxílio da câmara. Na fase de experimentação foram encontrados vários problemas com o programa, tais como:

- Com imagens com baixa luminosidade e com elevado número de sombras, o programa não as reconhece e também apresenta falhas no seu funcionamento;
- Com imagens com dimensões reduzidas, ou seja, de perfil ou com uma parte do rosto omitido, o programa falha no reconhecimento;
- A câmara possui uma falha de segurança uma vez que permite o reconhecimento através de quadros/imagens de rostos;
- Outro erro foi a deteção incorreta quando eram usados quadros/imagens com algumas semelhanças aos rostos presentes na base de dados.

Durante o desenvolvimento deste trabalho, foram encontrados alguns obstáculos que requerem uma maior atenção. Um dos desafios enfrentados foi a compreensão e utilização eficiente das bibliotecas necessárias para a realização do programa, uma vez que trabalhar com determinadas bibliotecas pode por vezes um processo complexo, especialmente quando se trata de entender a sintaxe, funcionalidades e recursos.

Na fase de testes, houve dificuldades em identificar o erro para cada uma das imagens problemáticas. Após a conclusão desta fase, conseguimos perceber os fatores que contribuíram para o resultado incorreto.

6 Conclusão

Com base na realização destes trabalhos foi possível verificar que todas as tecnologias de autenticação possuem tanto vantagens como desvantagens sendo que nenhuma é completamente segura. As tecnologias de autenticação são bastante utilizadas nas nossas atividades do quotidiano por meio dos dispositivos digitais, o que nos expõe a ataques, uma vez que todas estas tecnologias apresentam falhas e vulnerabilidades.

O reconhecimento facial destaca-se como uma das tecnologias de autenticação mais utilizadas atualmente, por isso decidimos implementar um pequeno programa que utiliza esta tecnologia, com o objetivo de avaliar a segurança da mesma em diferentes situações.

Durante a sua realização adquirimos novos conhecimento sobre as várias bibliotecas utilizadas e ainda foi possível verificar que a tecnologia em questão apresenta várias falhas de segurança, pelo menos no nosso programa. Constatámos que o nosso programa pode em certos casos ser facilmente "enganado", quando as imagens são semelhantes ou foram previamente manipuladas.

Estas conclusões permitiram verificar o quão importante é analisar cuidadosamente as tecnologias de autenticação e as suas implementações. Embora o reconhecimento facial possua muitas aplicações e benefícios, este também apresenta várias vulnerabilidades, das quais temos que estar conscientes e preparados. A segurança na autenticação é um desafio que tem vindo a ser desenvolvido e melhorado, de forma a garantir uma autenticação mais robusta e confiável.

Referências

[1] Compugraf contributors. O poder das tecnologias de autenticação. https://www.compugraf.com.br/tecnologias-de-autenticacao/, 2021. [Online; accessed 18-June-2023].

[2] TS2 contributors. Principais tecnologias de autenticação biométrica: um guia abrangente. https://ts2.space/pt/principais-tecnologias-de-autenticacao-biometrica-um-guia-abrangente/, 2023. [Online; accessed 18-June-2023].

[3] ClearSale contributors. Autenticação digital: conheça os principais métodos e sua importância. https://blogbr.clear.sale/metodos-de-autenticacao-conheca-os-principais, 2023. [Online; accessed 18-June-2023].

[4] Konica Minolta contributors. Tecnologias de autenticaÇÃo. https://www.konicaminolta.pt/pt-pt/software/seguranca/tecnologias-de-autenticacao, 2023. [Online; accessed 18-June-2023].

[5] Paulo Sérgio Magalhães & Henrique Dinis Santos. Biometria e autenticação. https://repositorium.sdum.uminho.pt/bitstream/1822/2184/1/capsi.pdf, 2003. [Online; accessed 18-June-2023].

[6] kaspersky contributors. O que é reconhecimento facial – definição e explicação. https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition, 2023. [Online; accessed 18-June-2023].

[7] Lastpass contributors. A importância da autenticação multifator para pmes. https://blog.lastpass.com/pt-br/2022/10/a-importancia-da-autenticacao-multifator-para-pmes/, 2023. [Online; accessed 18-June-2023].

[8] Unico contributors. Com a autenticação digital pode-se resguardar empresas e clientes? https://unico.io/institucional/autenticacao-digital/, 2023. [Online; accessed 18-June-2023].

[9] Autenticação.gov. Assinatura digital autenticação.gov. https://www.autenticacao.gov.pt/assinatura-digital/assinatura-digital-qualificada, 2023. [Online; accessed 18-June-2023].

[10] RNC Digital contributors. Quais as vantagens e desvantagens do certificado digital. https://rncdigital.com/quais-as-vantagens-e-desvantagens-do-certificado-digital/, 2023. [Online; accessed 18-June-2023].

[11] IEEE XPLORE contributors. True2f: Backdoor-resistant authentication tokens. https://ieeexplore.ieee.org/document/8835225, 2019. [Online; accessed 18-June-2023].

[12] FORTINET contributors. What is an authentication token? https://www.fortinet.com/resources/cyberglossary/authentication-token, 2023. [Online; accessed 18-June-2023].

[13] TOTVS contributors. Token de autenticação: o que é, como funciona e tipos. https://www.totvs.com/blog/gestao-logistica/token-de-autenticacao/, 2023. [Online; accessed 18-June-2023].