RECONHECIMENTO FACIAL PARA IDENTIFICAÇÃO NO ACESSO AO DATA CENTER

Ilton do Nascimento Castro

Marcos Antônio Rodrigues da Silva Júnior

RESUMO

O artigo aborda o estudo e criação de um algoritmo de reconhecimento facial usando o método Fisherface, que tem como objetivo principal, analisar imagens faciais de uma base de dados, utilizando uma câmera (webcam) e dessa forma retornar os dados de identificação de pessoas, quando estas estiverem cadastradas na base. As etapas de criação do algoritmo consistem em: detectar faces, coletar as imagens, treinar e reconhecer. Em sua essência, este algoritmo fará extração de características essenciais e peculiares de cada uma das imagens coletadas, através de técnicas de reconhecimento facial, trazendo uma maior efetividade para identificação de faces. Devido ao nosso cenário atual de pandemia (COVID-19), esta forma de biometria irá ajudar a evitar o contato com equipamentos de acesso, que não estejam devidamente higienizados em um ambiente Data Center e consequentemente trazendo mais segurança para identificar intrusos em áreas que exigem autenticação.

Palavras-chave: 1. Reconhecimento Facial, 2. Acesso, 3. Biometria,4. Segurança Cibernética,5. Detecção facial,6. Centro de Dados, 6. COVID-19.

ABSTRACT

The article discusses the study and creation of a facial recognition algorithm using the Fisherface method, which has as main objective, to analyze facial images from a database, using a camera (webcam) and in this way return the identification data of people, when they are registered in the database. The steps to create the algorithm consist of: detecting faces, collecting images, training and recognizing. In essence, this algorithm will extract essential and peculiar characteristics from each of the collected images, through facial recognition techniques, bringing greater effectiveness to face identification. Due to our current pandemic scenario (COVID-19), this form of biometrics will help to avoid contact with access equipment, which is not properly sanitized in a Data Center environment and consequently bringing more security when identifying intruders in areas that require authentication.

Keywords: 1. Facial recognition, 2. Access, 3. Biometrics, 4. Cybersecurity, 5. Facial detection, 6. Data Center, 6. COVID-19.

Introdução

As buscas pela segurança de dados, principalmente em ambientes destinados ao armazenamento de recursos tecnológicos, trouxeram um crescimento contínuo, voltado as tecnologias que fazem identificação de pessoas através da face. Tecnologias que permitem associar imagens a pessoas, marcar regiões especiais do corpo e relacionar dados a um contexto específico em uma base dos dados, estão acessíveis a preços muito altos no mercado (KUROIWA, SILVIO, 2015, p.2).

O reconhecimento facial é uma técnica de biometria baseada em traços do rosto humano, este processo é realizado através de ligações algorítmicas de traços, tamanhos e formas, podendo ser citado como exemplo, uma distância exata entre partes do rosto, tamanho da arcada dentária, distância entre olho e boca, tamanho do crânio, entre outros detalhes (SILVIO, OKABE, 2014, p.2).

O reconhecimento facial é uma tecnologia que pode ser utilizada em um sistema de biometria, capaz de ser usada para fins de acesso, o que é essencial para as questões de segurança nos dias atuais. O fato desta tecnologia ser empregada em locais públicos e privados, possibilita a facilidade de minimizar limitações jurídicas e comprovar acessos de pessoas em horários distintos (SILVIO, OKABE, 2014, p.2).

O objetivo deste estudo é enfatizar e demostrar a importância do uso de um framework específicos com funcionalidades de detecção de pessoas nos sistemas de acesso por biometria de reconhecimento facial utilizando o método Fisherface, demonstrando que essa tecnologia pode ser aplicada para identificar acessos e evitar intrusões em um ambiente Data Center (KUROIWA, SILVIO, 2015, p.2).

A Figura 1 abaixo, representa o sistema de reconhecimento facial no Data Center.

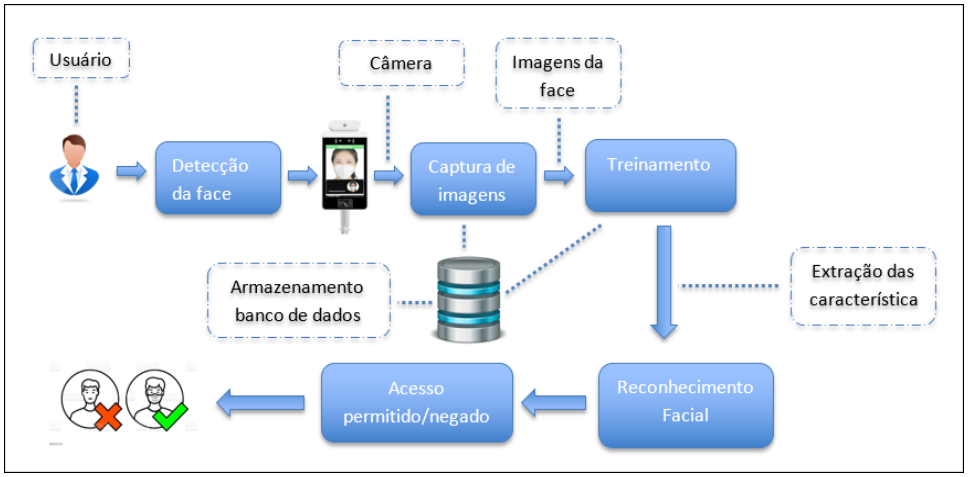


Figura 1 - Ilustração do sistema de reconhecimento facial no Data Center.

Este trabalho foi organizado em 6 seções. Na primeira será descrito a história sobre a tecnologia de reconhecimento facial, como surgiu, quais são os benefícios e malefícios dos sistemas que usam essa tecnologia nos dias atuais, quais são as áreas de aplicação dessa tecnologia, na segunda será feito uma descrição sobre o método Fisherface e sobre as técnicas básicas empregadas no método, a Análise Discriminante Linear (LDA) e Principal Component Analysis (PCA), na terceira serão apresentadas as características dos componentes utilizados no estudo dessa tecnologia, quais são as funcionalidades de cada componente, na quarta seção será abordada a implementação do algoritmo de reconhecimento facial e todas as suas etapas de criação do início ao fim , na quinta será serão mostradas quais foram os resultados positivos e negativos após a execução do programa e por último na sexta secção apresentam-se as conclusões sobre o artigo.

1. Referencial teórico

O francês Alphonse Bertillon em meados do século XIX, propôs um método que se baseava em um conceito de que com o tempo, as medidas do corpo de um ser humano adulto não mudavam com o tempo. (BERTILLON, 1896, apud SILVA, 2015, p.20).

Na década de 1960, surgiu um sistema de reconhecimento facial semiautomático, onde, através de uma base de dados com imagens de 10 pessoas, era possível fazer uma análise de forma interativa, mostrando a foto de cada pessoa e caso o sistema respondesse de forma negativa, era possível receber um retorno com o nome da pessoa a ser identificada. O sistema conseguiu usar matriz de pesos e medidas

para melhorar sua precisão a cada apresentação de uma nova imagem. Através dessa interação era possível aplicar um treinamento assistido para fins de teste, após apresentação dessas imagens 250 vezes, o sistema conseguiu de forma assertiva a classificação de todas essas imagens. (TAYLOR, 1967, apud SILVA, 2015, p.20).

Na década seguinte, foi desenvolvido um sistema bem mais evoluído, este sistema começou a utilizar 22 duas características para melhoria do reconhecimento, tais como abertura do olho e largura da boca, sombra dos olhos. (GOLDSTEIN; HARMON; LESK, 1971, apud SILVA, 2015, p.20).

O intuito era tornar o resultado de reconhecimento aproximado ao feito por seres humanos, através da extração de características da imagem da base, através de uma ordem com características e limiares. A título de curiosidade, os experimentos feitos com 255 faces atingiram 70% de efetividade. (SILVA, 2015, p.20).

O método Fisherface, com o objetivo de redução de dimensionalidade de imagens, aplica uma técnica chamada LDA, este método teve uma efetividade considerável em bases de dados que, contém imagens com problemas de variações de luminosidade. (BELHUMEUR; HESPANHA; KRIEGMAN, 1997, apud SILVA, 2015, p.21).

> No âmbito da extração de características o método de PCA foi utilizado, por ter um sucesso em sistemas de reconhecimento facial, além de estar bem difundido no mercado, lembrando que também diminui a dimensionalidade e mantendo apenas as características de maior importância e descartando as de menor relevância. A técnica PCA gera um conjunto de imagens do domínio que é selecionado para treinamento, na etapa seguinte é criado um espaço de faces e posteriormente uma base de dados dos usuários é criada. (BISSI;2018, p.28).

1.1 Benefícios e malefícios dos sistemas que usam essa tecnologia

A procura pela segurança em ambientes onde são alocados recursos tecnológicos e dados em geral está em constante crescimento, por esse motivo surge a necessidade de gerenciamento de identidades. Uma tecnologia importante e em constante crescimento é a biometria, especificadamente o reconhecimento facial, que pode nos trazer vários benefícios, mas também se não forem tomados os devidos cuidados, podem trazer prejuízos enormes.

Outro risco iminente neste ano de 2020, é de contágio com a doença COVID-19. A disseminação desse vírus acontece principalmente do contato com superfícies infectadas que não foram devidamente higienizadas.

Uma das ações que contribuem para a infecção da doença COVID-19 é, tocar em olhos e nariz após o contato com alguma superfície infectada. (MCINTOSH, 2020,

p.3). Neste ponto, podemos dizer que o reconhecimento facial será de crucial importância, pois ao apresentar a face em sistemas de acesso, será evitado o contato físico com possíveis locais por onde circulam o vírus.

Nos dias atuais, estamos lidando com uma situação atípica que é a pandemia do COVID-19, um dos principais meios de contaminação está na má sanitização de equipamentos que possam ser contaminados, então nesse aspecto, o reconhecimento facial traz um grande benefício, pois não precisamos tocar em equipamentos que dependem de uma validação para identificar o acesso em alguns lugares, como por exemplos Data Centers.

Outro benefício, está no reconhecimento automático de pessoas que trabalham em um ambiente corporativo com muito fluxo de funcionários, pois pode facilitar de forma mais rápida a liberação, registro e gestão dos mesmos. Para fins segurança do ambiente esta tecnologia é essencial, pois o contato físico, pode ser substituído em alguns aspectos e afim de evitar possíveis ameaças.

O reconhecimento facial já é utilizado em dispositivos móveis, como por exemplo: em smartphones para desbloqueio de tela, assim como plataforma de aplicativos de motorista de carro que também já utilizam a tecnologia.

A tecnologia de reconhecimento facial, evita fraudes e traz facilidade nos processos de integração com outros sistemas, visto que os seres humanos possuem características peculiares e quando os dados são compartilhados de forma segura observando todos os quesitos legais, tornam-se fortes aliados no processo de integração com o ambiente tecnológico.

Assim com outras tecnologias, temos também problemas em relação ao reconhecimento facial. Hoje com a evolução de aplicativos e dispositivos de dados, podemos ter de uma forma não-autorizada e compartilhamento de informações, ou seja, roubo de dados por pessoas mal-intencionadas, que tem o objetivo de criar contas falsas, efetuar cadastros em sites de compras, denegrir a própria imagem de pessoas na rede mundial de computadores e também o uso impreciso e discriminatório, pode ser um malefício, pois oferece o risco de pessoas inocentes serem confundidas com criminosos em qualquer tipo de ambiente, causando um dano moral e psicológico.

O ambiente físico de uma organização que possui dados importantes, pode ser alvo de criminosos, que colocam em risco toda a infraestrutura de armazenamento desses dados. Outro problema que pode ser encontrado nessa tecnologia, são riscos

à privacidade, devido o envolvimento de dados pessoais utilizados para seu funcionamento, o direito fundamental de um cidadão pode ficar comprometido.

1.2 Áreas de aplicação dessa tecnologia

As áreas de aplicação desta tecnologia são diversas, o foco deste trabalho está na ideia de usar esta tecnologia para identificação de funcionários , em equipamentos de autorização de um Data Center, mas aplicação desta tecnologia está empregada há tempos em vários setores do nosso dia a dia, como por exemplo, empresas de valores que guardam bens valiosos de outras organizações, escritórios corporativos que devem guardar seus dados para que sejam acessados apenas por pessoas que realmente devem ter esse acesso, carteira nacional de habilitação do Distrito Federal para evitar fraudes, casas lotéricas, casas de câmbio, mercados, conveniências, eventos de grande magnitude, como exposições de tecnologia, são exemplos de áreas de aplicação.

A adesão da tecnologia de reconhecimento facial não está somente no ambiente onde estão os profissionais da área de tecnologia da informação e comunicações, ela expande-se em quaisquer áreas que exigem uma melhor identificação de pessoas, para melhoria de registros e prevenção de incidentes de segurança.

2 Método FisherFace

O método escolhido foi o Fisherface, pois a quantidade no acerto e confiança do algoritmo mostrou-se mais eficiente, conforme dados apresentados na Tabela 2.

Tabela 1 - Eigenface

Acertos	Confiança	Parâmetros
73	5388,98	Padrão
60	2976,57	40, 8000

Tabela 2 - Fisherface

Acertos	Confiança	Parâmetros
80	1645,89	Padrão
76	466,2	3, 2000

Tabela 3 – LBPH

Acertos	Confiança	Parâmetros
66	10,69	Padrão
63	0,77	2,2,7,7,50

Utiliza-se no processo de reconhecimento facial, um método chamado Fisherface, onde são extraídas imagens de características de cada indivíduo. Segundo Bissi (2018, p. 24), sobre as fisherfaces:

> Similar ao eigenfaces, as fisherfaces podem ser visualizadas como imagens de características onde, as características das fisherfaces são variações de aparência presentes nas Imagens de cada indivíduo, tais como variações de luminosidade, poses e expressões faciais. Assim como as imagens no espaço de dados possuem um valor para cada atributo, os vetores e características possuem um valor para cada fisherfaces (p.24).

A Figura 1.1 abaixo, representa a projeção de faces relativo ao *Fisherface.*

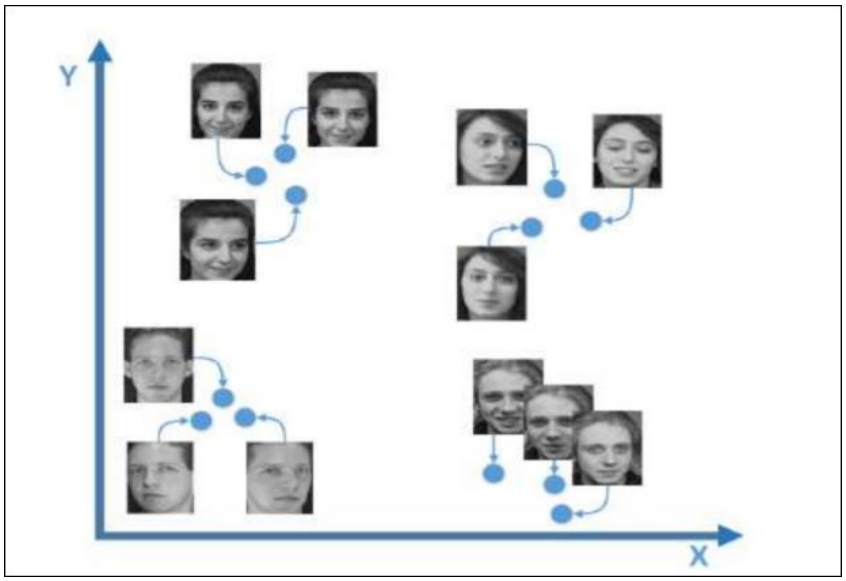


Figura 1.1 - Espaço de Faces Fisherfaces - (BISSI, 2018, apud SILVA, 2016, p.25)

A Figura 1.1 descreve perfeitamente o objetivo do Fisherface. De acordo com Bissi (2018, p. 25):

> Temos então que quanto mais diferente for uma pessoa da outra, mais distantes deverão estar suas projeções, e quanto mais parecidas forem as imagens de uma pessoa mais próximas deverão estar suas projeções (p.25).

Sobre o FisherFace, Bissi (2018, p.25), destaca que o algoritmo possui 8 etapas em sua combinação:

> Cálculo da face média por classe: Soma de todos os pixels de uma imagem pertencente a mesma classe, dividido pelo total de imagens dessa classe. Cálculo de face média geral: soma de todos os pixels de uma imagem, dividido pelo total de imagens independente da classe. Transformação das imagens em vetores: Concatenação de pixels linha a linha, formato um vetor de pixels Construção da matriz de dispersão intra-classe: Quanto as imagens de um indivíduo diferem uma das outras. Construção da matriz de dispersão inter-classe: Quanto as imagens de indivíduos distintos diferem umas das outras. Cálculo das fisherfaces: São as fisherfaces do LDA. Cálculo dos vetores de características: Vetores de imagens formados pelas características de média de cada fisherface. Cálculo da Similaridade: Uso de um classificador para pontuar a similaridade entre as imagens, exemplo utilizado, distâncias entre características de uma foto e outra (p.25).

2.1 Técnicas básicas empregadas no método Fisherface

Técnicas biométricas são empregadas na tecnologia de reconhecimento facial, as mesmas consistem na identificação de padrões faciais, tais como, formato da boca, rosto, distância entre olhos, boca, nariz, entre outros (*BISSI, 2018, apud* SILVA; CINTRA, 2015, p.11).

Apesar do Fisherface utilizar com maior amplitude a técnica LDA, também será comentado sobre a técnica PCA que também pode ser aplicada no algoritmo.

2.2 PCA - Principal Component Analysis

Técnica amplamente utilizada no tratamento de características, foi o primeiro método que teve êxito em sua aplicação no processo de reconhecimento facial. Ainda é utilizado amplamente nos dias atuais para comparação de novas propostas na área específica do estudo de reconhecimento facial (BISSI, 2018, apud PENTEADO, 2009, p.21).

Referente a PCA, Bissi (2018, apud Penharbel, 2005, p.21), destaca que:

> A PCA é uma técnica matemática que descreve um conjunto de dados usando as principais componentes que representam da melhor maneira o conjunto de dados, usados de maneira a reduzir a dimensionalidade dos dados ou então detecção de padrões (p.21).

A organização de um algoritmo de reconhecimento facial, precisa levar em consideração, técnicas de extração de dados principais da face, com o objetivo de aumentar a efetividade do sistema, evitando assim, falhas e possíveis problemas de administração da ferramenta que emprega essa tecnologia.

2.3 LDA - Linear Discriminant Analysis

A LDA é outra técnica utilizada no tratamento de dados de imagens no processo de reconhecimento facial, Bissi (2018, pag.22), destaca que:

> Com mesmo objetivo da técnica PCA, temos que o LDA consiste em reduzir a dimensionalidade dos dados visando a classificação. A partir de um conjunto de dados multidimensionais rotulados, o LDA gera um conjunto de dados de menor dimensionalidade que representa as classes dos dados originais (p.22).

Esta técnica é a mais utilizada no algoritmo do Fisherface, pois a preocupação com a melhoria na tradução de particularidades entre imagens, está amplamente difundida nesta técnica, que foi basicamente, uma melhoria do seu antecessor Eigenfaces.

O Fisherface utiliza a técnica LDA para aumentar de forma bastante significativa, a confiabilidade entre as imagens cadastradas na base de dados para o treinamento do algoritmo, justamente pelo foco em reduzir dimensionalidade dos dados, ou seja, quando maior for a similaridade entre fotos, maior a probabilidade de acerto nas características faciais.

3. Metodologia

O foco desse estudo é apresentar um algoritmo que utiliza o método Fisherface para chegar ao objetivo final que é reconhecer uma face e imprimir alguns dados de cadastro. Abaixo, estão descritos, os componentes e funcionalidades objetivas de cada um para melhor compreensão do estudo, são eles:

1. Pycharm: É uma IDE (ambiente de desenvolvimento) utilizado especificadamente para linguagem python, nele será desenvolvido a parte de código para o programa;
2. Linguagem Python: Está é uma linguagem de programação de alto nível, utilizada para escrita do código do programa de reconhecimento facial;
3. Biblioteca OpenCV: É uma biblioteca de programação com funções computacionais, que irá servir de auxílio para criar o algoritmo;
4. Fisherface: Este é o método já mencionado para facilitar a implementação do programa, que será utilizado junto com técnica LDA e scripts “.yml”, com o objetivo de treinar o algoritmo;

5. Base de dados de Imagens: Essa é uma base de dados local que, será preenchida com imagens dos dois integrantes do grupo, elas serão utilizadas para treinar o algoritmo para reconhecer as faces;

6. Laptop com uma webcam integrada e outra separada: Será utilizado um laptop para demonstração prática do algoritmo de reconhecimento facial em funcionamento.

4. Implementação do algoritmo

O trabalho inicia neste momento com a parte prática. As etapas de reconhecimento facial são divididas especificadamente em 4: detecção da face, coleta das imagens, treinamento do algoritmo e por fim reconhecimento. Cada uma dessas etapas são de extrema importância para que sejam alcançadas todas as expectativas deste estudo.

Abaixo, será feito a descrição de cada etapa de forma mais detalhada para facilitar o entendimento do processo, inclusive do código implementado com toda sua lógica.

4.1 Detecção da face

Conforme o algoritmo apresentando na Figura 2, o mesmo foi projetado apenas para identificação da face, ou seja, o sistema detectou o rosto com um quadrado vermelho assim que o localizou, de acordo com a demonstração na Figura 3.

```python
import cv2

classificador = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")
camera = cv2.VideoCapture(1)
amostra = 1
numeroAmostras = 50
id = input('Digite seu identificador:')
largura, altura = 220, 220
print("Capturando as faces...")

while (True):
    conectado, imagem = camera.read()
    imagemCinza = cv2.cvtColor(imagem, cv2.COLOR_BGR2GRAY)
    facesDetectadas = classificador.detectMultiScale(imagemCinza, scaleFactor=1.5, minSize=(150,150))

    for (x, y, l, a) in facesDetectadas:
        cv2.rectangle(imagem, (x, y), (x + l, y + a), (0, 0, 255), 2)
        if cv2.waitKey(1) & 0xFF == ord('q'):
            imagemFace = cv2.resize(imagemCinza[y:y + a, x:x + l], (largura, altura))
            cv2.imwrite("fotos/pessoa." + str(id) + "." + str(amostra) + ".jpg", imagemFace)
            print("[foto " + str(amostra) + "capturada com sucesso]")
            amostra += 1


    cv2.imshow("Face", imagem)
    #cv2.waitKey(1)
    if (amostra >= numeroAmostras + 1):
        break

print("Faces capturadas com sucesso")
camera.release()
cv2.destroyAllWindows()
```

Figura 2 - Algoritmo de detecção das imagens.

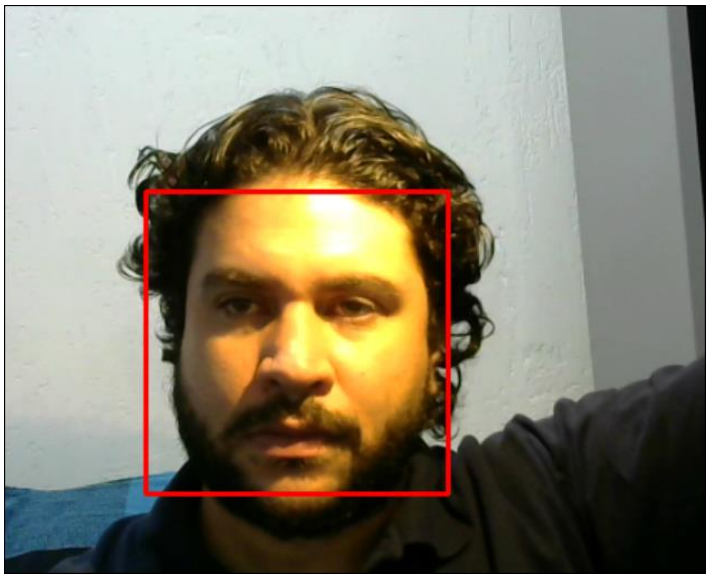


Figura 3 - Detecção de face.

4.2 Coleta das imagens

Nessa etapa é necessário digitar o identificador (ID), para que seja iniciada a captura das imagens pelo algoritmo (necessário apertar a letra “q” do teclado) e consequentemente, a imagem será salva na base de dados local.

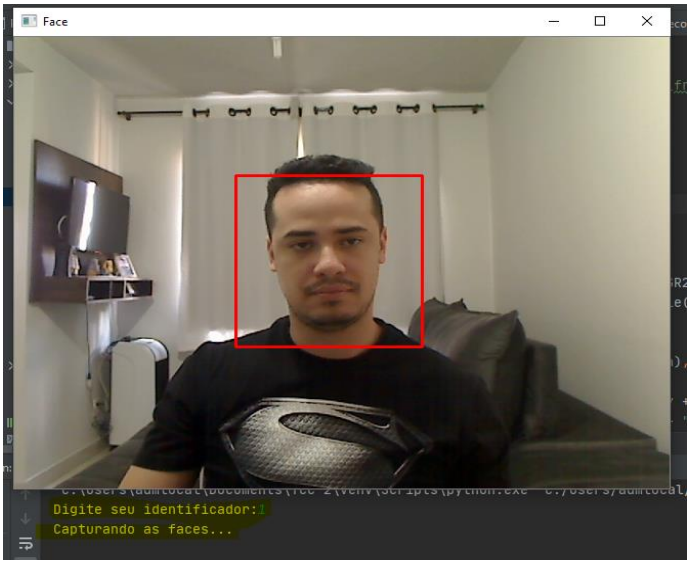


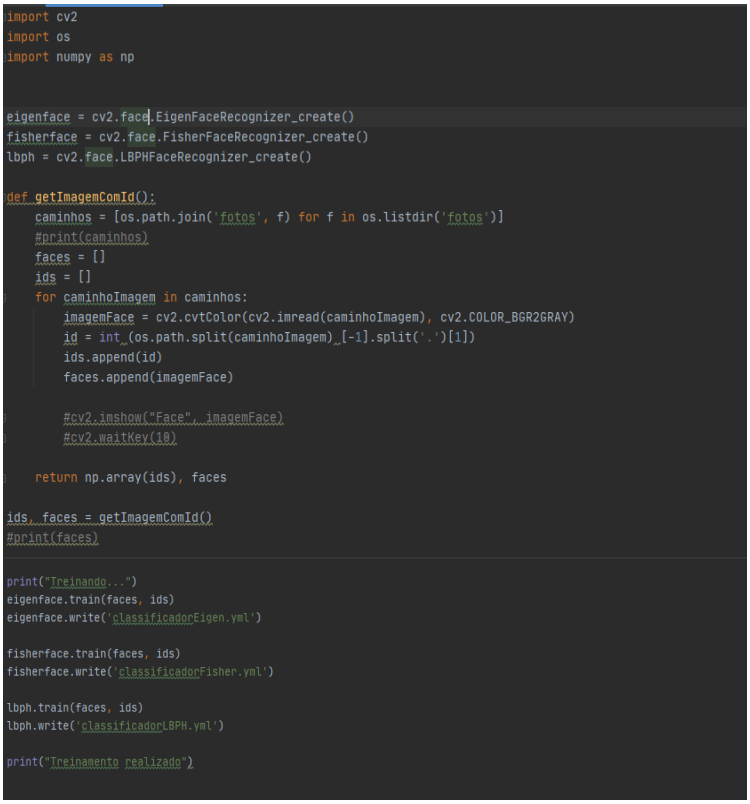
Figura 4 - Coleta de imagens.

4.3 Treinamento do algoritmo

O algoritmo descrito na figura 6, que realiza o treinamento com as imagens cadastradas na base de dados, cria o arquivo chamado classificadorFisher.yml, neste arquivo são escritos os parâmetros do treinamento conforme Figura 5. O código completo de forma pública, com todas as etapas, está disponível em: https://github.com/rdpinformacao/CodigoReconhecimentoFacial.git.

```
%YAML:1.0
---
opencv_fisherfaces:
   threshold: 1.7976931348623157e+308
   num_components: 1
   mean: !!opencv-matrix
      rows: 1
      cols: 48400
      dt: d
      data: [ 1.8072000000000000e+02, 1.7858000000000001e+02,
          1.7546000000000001e+02, 1.7308000000000001e+02,
          1.7186000000000001e+02, 1.7220000000000002e+02,
          1.7078000000000000e+02, 1.6886000000000001e+02,
          1.6644000000000000e+02, 1.6347999999999999e+02,
          1.6024000000000001e+02, 1.5852000000000001e+02,
          1.5775999999999999e+02, 1.5581999999999999e+02,
          1.5288000000000000e+02, 1.4992000000000002e+02,
          1.4675999999999999e+02, 1.4408000000000001e+02, 141.
```

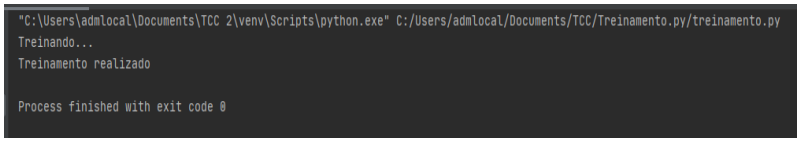
Figura 5 - Arquivo classificadorFisher.yml.



```python
import cv2
import os
import numpy as np


eigenface = cv2.face.EigenFaceRecognizer_create()
fisherface = cv2.face.FisherFaceRecognizer_create()
lbph = cv2.face.LBPHFaceRecognizer_create()

def getImagemComId():
    caminhos = [os.path.join('fotos', f) for f in os.listdir('fotos')]
    #print(caminhos)
    faces = []
    ids = []
    for caminhoImagem in caminhos:
        imagemFace = cv2.cvtColor(cv2.imread(caminhoImagem), cv2.COLOR_BGR2GRAY)
        id = int(os.path.split(caminhoImagem)[-1].split('.')[1])
        ids.append(id)
        faces.append(imagemFace)

        #cv2.imshow("Face", imagemFace)
        #cv2.waitKey(10)

    return np.array(ids), faces

ids, faces = getImagemComId()
#print(faces)

print("Treinando...")
eigenface.train(faces, ids)
eigenface.write('classificadorEigen.yml')

fisherface.train(faces, ids)
fisherface.write('classificadorFisher.yml')

lbph.train(faces, ids)
lbph.write('classificadorLBPH.yml')

print("Treinamento realizado")
```

Figura 6 – Código treinamento do algoritmo.

Após execução do código foi apresentado a seguinte mensagem “Treinamento realizado”.



```
"C:\Users\admlocal\Documents\TCC 2\venv\Scripts\python.exe" C:/Users/admlocal/Documents/TCC/Treinamento.py/treinamento.py
Treinando...
Treinamento realizado

Process finished with exit code 0
```

Figura 7 - Finalização do treinamento.

4.4 Reconhecimento

Nessa etapa é realizado o reconhecimento facial. Os dados de cadastros foram exibidos, após a validação positiva do reconhecimento facial. É possível realizar ajustes no código de modo que o algoritmo diferencie as pessoas que possuem cadastro ou não. Segue abaixo a Figura 8 com o reconhecimento do Marcos já cadastrado na base do sistema e a Figura 10, mostra uma pessoa que não tem o cadastro na base de dados.

Figura 8 - Reconhecimento facial pessoa 1 cadastrada.

Figura 9 - Reconhecimento facial pessoa 2 cadastrada.

Figura 10 - Reconhecimento facial pessoa 3 sem cadastro.

5. Resultados

Foram realizados testes durante o treinamento do código utilizando o Fisher-face e foi constado que dependendo do ângulo e da claridade, o algoritmo não é tão eficaz, pois podem haver variações na detecção das faces que estão na base.

Conforme mostrado no reconhecimento facial da Figura 11 e 12, houve uma variação na identificação devido à distância, câmera não ser a ideal para captura da foto com qualidade e a iluminação do ambiente não ser suficiente, esses recursos podem causar problemas na eficiência do algoritmo.

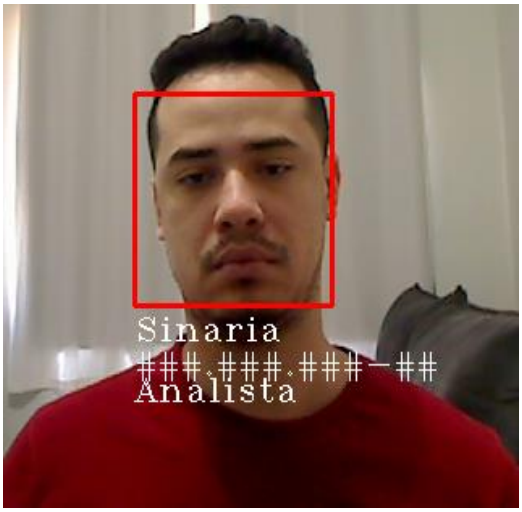


Figura 11 - Variação de precisão do reconhecimento.

Figura 12 - Pessoa não reconhecida na base.

De acordo com a Figura 12, mesmo o usuário cadastrado, o sistema não reconheceu a face do mesmo, pois a precisão do reconhecimento facial foi afetada, por conta da distância da câmera e baixa qualidade da webcam.

Na Figura 13, apresentada a seguir, foram realizados ajustes no código e nas capturas das imagens, as mesmas foram feitas através de uma webcam de maior qualidade, sendo possível obter o reconhecimento facial da pessoa já cadastrada na base de dados local, alcançando assim o resultado esperado.

Figura 13 - Ajustes realizados no código.

Executados os testes cobrindo parte da face identificou-se falhas, pois o sistema não foi capaz de reconhecer a pessoa que já era cadastrada, conforme a Figura 14.

Figura 14 – Cobrindo a boca.

No exemplo a seguir, na Figura 15, cobriu-se a metade da face, porém o sistema conseguiu realizar o reconhecimento com sucesso.

Figura 15 – Cobrindo a metade do rosto.

Na Figura 16 cobriu-se os olhos, o sistema apresentou falha e não conseguiu reconhecer a face.

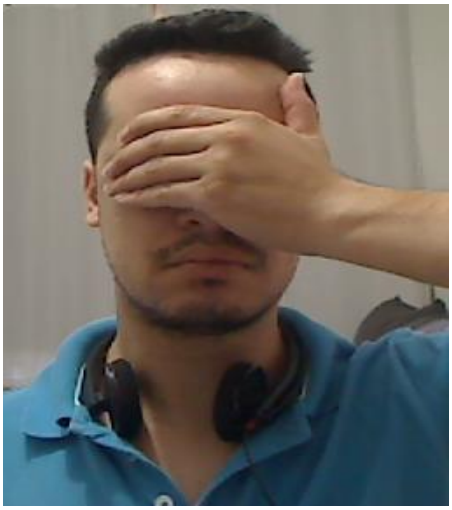


Figura 16 - Cobrindo os olhos.

Figura 17 - Cobrindo o nariz.

Foram realizados testes com pessoas já cadastradas na base do sistema e constatou-se que, mesmo elas utilizando máscaras, o algoritmo desenvolvido foi capaz de identificar a face, conforme demostrado nas Figuras 18 e 19.

Figura 18 – Com máscara

Figura 19 - Com máscara

Tabela 4 - Webcam utilizada.

Nome do componente	Fabricante	Modelo	Resolução máxima câmera
webcam 1	Logitech Europe S.A.	Logitech HD Webcam C270	720p/30qps (1 MP)
webcam 2	Logitech Europe S.A.	Webcam Pro 9000	1600 x 1200 (2 MP)
webcam 3 (integrada)	AsusTek Computer Inc.	Asus Vivobook S400CA	1.3 MP
webcam 4 (integrada)	Dell Technologies	Dell Latitude 7390	1280 x 720 (0,92 MP)

5.1 Resultados positivos

Agilidade e segurança para realizar o acesso ao Data Center, pois não será necessário fazer o reconhecimento da digital, sendo apenas necessário apresentar a face na câmera onde será realizado o reconhecimento facial, no caso de cadastro positivo, o acesso será liberado ao ambiente, caso contrário, o mesmo será notificado que não tem permissão para acessar e o registro será efetivado como tentativa de intrusão, para que seja analisado posteriormente, objetivando tomadas de decisões.

5.2 Resultados negativos

Ambiente com a iluminação ruim dificulta no reconhecimento da face, foto mal capturada, pode ser um futuro problema para o reconhecimento, outro fator importante que deve ser levado em consideração é a qualidade de resolução da câmera, quanto maior a resolução, mais são as chances de efetividade no reconhecimento facial, quanto menor a resolução, provavelmente as chances de efetividade serão piores, pois nos testes, foram identificados que, fotos capturadas da webcam do laptop com a resolução inferior, impossibilitaram a identificação de algumas faces.

Observou-se que o sistema apresenta algumas falhas em determinados pontos, um exemplo a ser citado é que ao apresentar para a câmera a foto de uma pessoa já cadastrada na base de dados, existe a possibilidade do sistema realizar a leitura dessa foto e liberar o acesso.

6. Considerações finais

Esse trabalho foi desenvolvido com base na LGPD, evitando compartilhamento de dados sensíveis de terceiros, com o objetivo de assegurar a proteção de dados.

A LGPD Lei Geral de Proteção de Dados, atualmente em vigor no brasil, cita em seu Art. 4°, alguns casos em que não se aplica o tratamento de dados pessoais:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (p.2).

A tecnologia de reconhecimento facial, tem seu respaldo pela LGPD, em casos específicos, conforme citado acima, ou seja, não podemos de forma aleatória, realizar testes com dados faciais de pessoas, visto que essas ações, em casos particulares sem o consentimento dos usuários, podem gerar sérios problemas com a justiça.

A LGPD Lei Geral de Proteção de Dados, cita também em seu Art. 11°, Seção II,do tratamento de dados pessoais sensíveis, sobre a:

> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (p.6).

O cenário relatado acima, nos informa claramente, que mesmo nos sistemas eletrônicos utilizados para autenticação, que é o caso do reconhecimento facial, por lei, estão garantidos, a prevenção contra fraude e reforça que esses sistemas de autenticação, devem ser seguros, permitindo a privacidade dos dados de pessoas cadastradas.

A importância dos sistemas de reconhecimento facial na segurança, é essencial para os dias atuais, onde precisamos ser ágeis na identificação de pessoas, para melhoria nos processos de segurança de informação, mais precisamente autenticidade. Garantir o registro de dados e horários de acesso, são formas de avaliação de possíveis comportamentos fora do padrão, para que sejam feitas tomadas de decisões importantes em cada ambiente.

O estudo realizado sobre os métodos de reconhecimento facial, foram suficientes para diagnosticar possíveis falhas que, podem ser exploradas por pessoas mal-intencionadas, com o propósito de acessar espaços físicos de empresas e roubarem dados importantes e assim utilizar como meio de extorsão ou como exposição da imagem da empresa, fazendo com que os danos, sejam imensuráveis.

Foram identificados durante o treinamento dos algoritmos Fisherface, que o seu poder de acerto e a sua confiabilidade é bem superior do que outros métodos utilizados nesta mesma tecnologia. O Fisherface é um algoritmo que utiliza as questões de dimensionalidade de imagens para gerar sempre uma precisão melhor.

Neste trabalho, a criação do algoritmo foi feita com sucesso, em todas as suas etapas do início ao fim, lembrando que é de extrema importância realizar todos os

passos desde a detecção de faces, coleta das imagens, treinamento do algoritmo e para finalizar obtendo o reconhecimento das faces.

As principais vulnerabilidades encontradas foram variação de precisão do reconhecimento, pessoa cadastrada na base, porém o sistema não reconhece e foi realizado teste aonde cobriu-se parte da face para verificar a precisão do sistema aonde é ilustrada na Figura 14 a 17 aonde ficou claro que o sistema é falho em alguns pontos.

Algumas vulnerabilidades encontradas no estudo, podem ser evitadas com algumas boas práticas citadas abaixo:

1. Utilizar o algoritmo de reconhecimento facial com outros recursos, para melhoria da efetividade, por exemplo, reconhecimento por voz, reconhecimento por íris, dentre outros;
2. Criar mecanismos que detectem a presença real de uma face, para evitar exposição de fotos pelos celulares ou tablets;
3. Para captura de imagens, utilizar câmeras com boa resolução no mínimo acima de 1 MP;
4. Manter uma distância mínima de 50 cm, entre a face e o equipamento;
5. Exigir o consentimento digital, das pessoas que serão cadastradas para utilizarem esta tecnologia;
6. Efetuar testes de precisão do algoritmo, afim de evitar falsos positivos;
7. Melhoria contínua no código, utilizando as melhores práticas disponíveis no mercado de I.A.

O reconhecimento facial criado através de um algoritmo mostrou-se bastante eficaz, reconhecendo as faces colocadas a prova, imprimindo dados de cadastros, que podem ser diversos, como, cpf, rg, cargo. Algumas questões que foram mostradas, devem ser analisadas com mais critério, como por exemplo, devem ser capturadas fotos com qualidade, boa luminosidade, distância da câmera, expressões faciais devem ser registradas, falhas que podem ser exploradas utilizando imagens de pessoas que já estejam cadastradas na base de dados e assim comprometendo a segurança do ambiente.

Foram executados diversos testes e encontrado vulnerabilidade no sistema, pois é possível burlar o sistema, utilizando uma foto de uma pessoa já cadastrada na base, sendo ela impressa ou na tela de celular.

Durante o estudo também foi realizado teste cobrindo parte da face aonde foi possível identificar que se cobrir parte do rosto o sistema ainda continua reconhecendo, porém, ao cobrir qualquer parte como boca, nariz ou olhos o sistema não consegue identificar a face. Durante o teste foi possível identificar que tem uma pequena variação na identificação, isso acontece por conta de fotos tiradas com baixa qualidade, iluminação do ambiente entre outros fatores como a quantidade de fotos para realizar o treinamento sendo que foi testado na primeira vez com 25 fotos e posterior mente com 50 fotos aonde foi visível uma melhora na detecção das faces e diminuindo as variações e erros.

7. Referências

Ana,Leda. Algoritmos e Lógica de Programação, **Slideshare Rodfernandes**. 2009. Disponível em:<https://pt.slideshare.net/rodfernandes/material-de-apoio-de-algoritmo-e-lgica-de-programao>. Acesso em: 13/06/2020.

Bissi, Thelry David. Reconhecimento Facial com os algoritmos Eigenfaces e Fisherfaces, **Bitstream**. 2018. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/22158/3/ReconhecimentoFacialAlgotimos.pdf>. Acesso em:25/10/2020.

Brasil, Lei Nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 02/09/2020.

Celso,Kitamura. Compilador (compiler), **Celsokitamura**. 2017. Disponível em: <https://celsokitamura.com.br/compilador/>. Acesso em: 18/06/2020.

Da Ivson Soares Jose, Silva. Reconhecimento facial em imagens de baixa resolução, **Bitstream**. 2015. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/16367/1/disserta%c3%a7%c3%a3o_jiss_ci%c3%aanciadacomputa%c3%a7%c3%a3o.pdf>. Acesso em: 20/06/2020.

David Thelry ,Bissi. Reconhecimento Facial com os algoritmos Eigenfaces e Fisherfaces, **Bitstream**. 2018. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/22158/3/ReconhecimentoFacialAlgotimos.pdf>. Acesso em: 10/09/2020.

Dell. Manual do proprietário do Dell Latitude 7390, **Dell**. 2020. Disponível em:<https://www.dell.com/support/manuals/br/pt/brbsdt1/latitude-13-7390-laptop/latitude_7390-om/camera-specifications?guid=guid-71e89bdf-d54c-478c-bb0e-0cee4bceace2&lang=en-us>. Acesso em: 03/10/2020.

Icecat. Logitech QuickCam Pro 9000 webcam 1600 x 1200 pixels USB Preto Prateado, **Icecat**. 2019. Disponível em: <https://icecat.biz/br/p/logitech/960-000053/webcams-quickcam+pro+9000-896740.html>. Acesso em: 02/10/2020.

Kazuhiro Rogerio, Okabe; Carro Antonio, Silvio. Reconhecimento facial em imagens capturadas por câmeras digitais de rede, **Revistas Unoeste**. 2014. Disponível em: <http://revistas.unoeste.br/index.php/ce/article/view/1307/1425>. Acesso em: 11/06/2020.

Logitech. Hd-webcam-c270, **Logitech**. 2020. Disponível em: <https://www.logitech.com/pt-br/product/hd-webcam-c270>. Acesso em: 03/10/2020.

Mcintosh, Kenneth. Doença de Coronavírus 2019 (COVID-19), **Ebserh**. 2020. Disponível em: <http://www2.ebserh.gov.br/documents/1688403/5111980/4.pdf/49227786-d768-470e-9ea2-7e021aa96cc9>. Acesso em: 09/09/2020.

Paula Ana, Pereira. O que é algoritmo, **Tecmundo**. 2009. Disponível em: <https://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm>. Acesso em: 15/06/2020.

Tsutsumi Bruno, Kuroiwa; Carro Antonio, Silvio. Detecção de intrusão com reconhecimento facial em imagens geradas por câmeras de segurança, **Revistas Unoeste**. 2015. Disponível em: <http://revistas.unoeste.br/index.php/ce/article/view/1424/1459>. Acesso em: 09/06/2020.

Zambarda,Pedro. Ultrabook-asus-vivobook-s400ca, **Techtudo**. 2013. Disponível em: <https://www.techtudo.com.br/review/ultrabook-asus-vivobook-s400ca.html>. Acesso em: 02/10/2020.

Zenicola Filipe Luiz, Braga. Sistemas de Reconhecimento Facial, **Micti**. 2013. Disponível em: <http://eventos.ifc.edu.br/micti/wp-content/uploads/sites/5/2014/08/ESTUDO-SOBRE-METODOS-DE-RECONHECIMENTO-FACIAL-EM-FOTOGRAFIAS-DIGITAIS.pdf>. Acesso em: 10/08/2020.