UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Eliabe Vinicius Costa e Silva

# Avaliação de Algoritmos de Reconhecimento Facial para Autenticação de Usuários

**Uberlândia, Brasil**

**2023**

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Eliabe Vinicius Costa e Silva

# Avaliação de Algoritmos de Reconhecimento Facial para Autenticação de Usuários

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Orientador: Thiago Pirola Ribeiro

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Ciência da Computação

Uberlândia, Brasil

2023

*Este trabalho é dedicado a Helia Rejane Costa e Silva e Daniel Costa e Silva*

# Agradecimentos

Agradeço primeiramente a Deus, aos meus pais e minha família, tudo que sou e conquistei é graças a eles. Além disso, agradeço a minha namorada, que me deu apoio incondicional durante esse ultimo ano de graduação e transformou a minha vida.

Agradeço também a todas as minhas amizades, principalmente ao grupo Paragons, que foram minha família nessa cidade e meu porto seguro durante toda a faculdade e principalmente durante a pandemia.

Agradeço também a Ufuteria e a Computaria, por terem trago o samba para a minha vida e por terem me ensinado o verdadeiro significado de trabalho em equipe, eles me proporcionaram os momentos de descontração e emoção que me deram forças para concluir a graduação.

Agradeço também, ao meu orientador Thiago Pirola por toda a ajuda e paciência que teve comigo durante todo esse projeto, obrigado por me guiar e me explicar todo o processo de pesquisa.

# Resumo

A segurança digital tem uma grande importância no cenário de rápida evolução tecnológica. Assim, a biometria de reconhecimento facial se torna uma promissora ferramenta para a aprimorar a segurança de dados. O objetivo dessa pesquisa é aprofundar o entendimento sobre o uso do reconhecimento facial e identificar os métodos que são amplamente usados no cenário atual. O projeto se divide em duas partes principais, a primeira sendo a pesquisa teórica para fazer um investigação de estudos atuais e selecionar os métodos que se mostram importantes para esse cenário. Após isso, a segunda parte da pesquisa faz experimentos com esses algoritmos para determinar a precisão do identificação facial. A partir de referenciais teóricos, os algoritmos de Eigenface, Fisherface, *Local Binary Patterns Histograms* (LBPH) e Facenet foram escolhidos para fazerem parte do estudo, isto sendo baseado nos melhores resultados de estudos mais recentes. Portanto, os métodos foram testados com dois datasets de imagens faciais, O *Labelled Faces in the Wild* e o *Celebrity Face Image Dataset*. Após os experimentos, foi apresentado uma superioridade do Modelo Facenet usando *Transfer Learning* com uma acurácia de média 99%, além disso o modelo LBPH se mostra superior aos outros dois tendo um de media entre 64% e 78%. Porém, os algoritmos de Eigenface e fisherface apresentam resultados inferiores ao esperado, trazendo acurácias no intervalo de 17% até 51% e 11% até 63% de acurácia, sucessivamente.

**Palavras-chave**: Reconhecimento Facial, Facenet, Eigenface, Fisherface, LBPH, Labelled Faces in the Wild.

# Lista de ilustrações

# Lista de tabelas

# Lista de abreviaturas e siglas

**CNN** Redes Neurais Convolucionais - *Convolutional Neural Network*

**FAR** Taxa de Falsa Aceitação - *False Acceptance Rate*

**FN** Falso Negativo - *False Negative*

**FP** Falso Positivo - *False Positive*

**FRR** Taxa de Falsa Rejeição - *False Rejection Rate*

**HOG** *Histogram Oriented Gradients*

**LBP** *Local Binary Pattern*

**LBPH** *Local Binary Patterns Histograms*

**LDA** *Linear Discriminant Analysis*

**LFW** *Labelled Faces in the Wild*

**MTCNN** *Multi-Task Cascaded Convolutional Neural Network*

**PCA** Análise de Componentes Principais - *Principal Component Analysis*

**ResNet** Rede Neural Residual - *Residual Network*

**RNA** Redes Neurais Artificiais

**TN** Verdadeiro Negativo - *True Negative*

**TP** Verdadeiro Positivo - *True Positive*

**VG-RAM** *Virtual Generalizing Random Access Memory*

# Sumário

# 1 Introdução

No cenário atual de rápida evolução tecnológica, o conceito de segurança digital está em constante redefinição. Sistemas que, outrora, eram tidos como impenetráveis, hoje enfrentam desafios sem precedentes, exigindo uma adaptação contínua para manter a integridade e confidencialidade das informações no mundo moderno (ROSS; JAIN, 2007).

Diante dessa conjuntura, é imperativo reavaliar as práticas de segurança da informação, especialmente no que concerne à autenticação de usuários. O advento do reconhecimento facial se destaca como uma promissora solução, capaz de transformar a forma como interagimos com sistemas digitais (ROSS; JAIN, 2007). Este trabalho se propõe a ser uma pesquisa científica que aprofundará o entendimento sobre a eficácia dessa tecnologia.

A investigação se concentrará na análise minuciosa dos métodos de reconhecimento facial e suas diferentes abordagens. Dessa maneira, a pesquisa irá explorar quais métodos são importantes no cenário atual e o quão preciso esses algoritmos são.

Para embasar este estudo, será realizada uma revisão da literatura especializada. Serão identificadas e avaliadas as tecnologias mais adequadas ao escopo do projeto, levando em consideração principalmente dados de precisão nesse contexto. Além disso, serão analisados casos de estudo e experiências anteriores, permitindo uma compreensão mais holística das práticas de reconhecimento facial.

## 1.1 Motivação

Como apontado anteriormente, a necessidade de um desenvolvimento constante na segurança da informação é muito importante. A pesquisa conduzida por Moraes (2010) ressalta o impacto da biometria na autenticação do usuário, transformando o paradigma de “o que eu sei” ou “o que eu tenho” para o mais robusto e pessoal “quem sou eu”.

Dessa forma, a implementação de uma autenticação biométrica confiável representa um significativo avanço na segurança digital. Ao adotar esta abordagem, fica impedido o acesso de pessoas mal intencionadas às informações de outros usuários, uma vez que não é mais possível obter êxito simplesmente ao descobrir informações confidenciais, como senhas e nomes de usuário, ou ao obter objetos de autenticação, como cartões de acesso ou crachás.

Essa nova abordagem acrescenta uma camada adicional de segurança para os usuários, criando uma barreira substancial contra acessos não autorizados. A autenticação biométrica eleva o nível de proteção, pois se baseia em características únicas e intransferíveis do próprio usuário, como impressões digitais ou características faciais, tornando

praticamente impossível a usurpação da identidade de um indivíduo, mesmo com a posse de informações convencionais de autenticação. Assim, os sistemas que adotam essa tecnologia proporcionam uma salvaguarda mais robusta e confiável para os dados e informações dos usuários.

Ao se inserir esta inovação no campo da segurança da informação, abre-se um horizonte promissor para a construção de sistemas mais resilientes e eficazes, capazes de enfrentar os desafios impostos pelo cenário tecnológico contemporâneo. Portanto, a pesquisa aqui proposta busca não apenas compreender e avaliar as práticas de autenticação por reconhecimento facial, mas também contribuir para o avanço e aprimoramento contínuo da segurança digital no mundo atual.

## 1.2 Metodologia

A primeira etapa do projeto consistirá na condução de uma pesquisa abrangente. Esta etapa é essencial para estabelecer uma base teórica sólida e para identificar trabalhos relacionados que servirão como referência. Através dessa investigação, serão reunidos dados e fatos cruciais para a compreensão e evidenciação dos métodos mais relevantes de reconhecimento facial.

Dentro da fase de pesquisa, serão conduzidos diversos estudos específicos para destacar os métodos de reconhecimento mais expressivos atualmente. Serão apresentadas as explicações de todos esses métodos para a compreensão do leitor durante a fase de experimentos.

A segunda parte do projeto envolverá a implementação prática daquilo que foi concebido na fase inicial da monografia. Com base nas evidências e dados coletados anteriormente, será possível desenvolver e testar os métodos apresentados, fornecendo, assim, indicativos concretos para sustentar a parte investigativa.

Portanto, ao final será feita uma comparação dos algoritmos desenvolvidos e os resultados esperados, baseados nos estudos correlatos. Dessa maneira, se poderá concluir quais os métodos mais precisos e efetivos.

## 1.3 Organização da Pesquisa

Os seguintes capítulos dessa pesquisa serão apresentados da seguinte forma: o Capítulo 2 apresenta os conceitos necessários para o entendimento do trabalho e também resumos de pesquisas relacionados ao tema. O Capítulo 3 traz a descrição do desenvolvimento e resultado dos experimentos desenvolvidos para essa pesquisa. Após isso, o Capítulo 4 descreve a conclusão elaborada a partir do esperado pela introdução e os re-

sultados dos experimentos e, além disso, cita possíveis trabalhos futuros relacionados a esse tema.

# 2 Fundamentação Teórica

Nesse capítulo será apresentada a explicação de diversos conceitos essenciais para o entendimento da monografia em sua totalidade. Além disso, será discorrido o resumo de vários trabalhos correlatos que foram usados para a composição da pesquisa.

## 2.1 Biometria

A vivência em sociedade, em diversas ocasiões, traz a necessidade de o indivíduo provar sua identidade. Assim, com o desenvolver tecnológico, foram montado diversos protocolos de autenticação, como por exemplo: verificação baseada em conhecimento (senhas), verificação baseada em *token* (cartão de identificação), entre outros. Porém, todos esses modos possuem falhas que são exploradas por pessoas mal-intencionadas (HONG; JAIN, 1998).

A maneira mais evidente de evitar esse problema seria um tipo de autenticação no qual a chave de acesso estaria em identificar o indivíduo em questão automaticamente, usando apenas suas características únicas. A autenticação por biometria foi idealizada com foco nessa linha de pensamento.

De acordo com Ross e Jain (2007), a biometria é a ciência de estabelecer a identidade de um indivíduo a partir de seus traços físicos ou comportamentais. Dessa maneira, existem diversas formas de abordagem, no qual são mais viáveis de acordo com as características do sistema.

A aptidão de cada tipo de biometria se dá pelos 7 fatores seguintes (ROSS; JAIN, 2007):

- Universalidade: Todos os indivíduos do sistema devem possuir esse traço.
- Unicidade: Todos os indivíduos devem ter o traço suficientemente diferente entre si para ser possível a filtragem da identidade.
- Permanência: O traço do sujeito deve ter uma invariabilidade pequena durante tempo, para que o sistema possa comparar com o dado previamente coletado e conseguir identificar sua correspondência.
- Mensurabilidade: Deve ser possível adquirir e digitalizar as características do indivíduo com equipamentos que não tragam inconveniência ao usuário.
- Performance: A acurácia do reconhecimento deve cumprir a expectativa do sistema.

- Aceitabilidade: O indivíduo deve estar disposto a conceder as características em questão ao sistema.
- Difícil imitação: O traço deve ter um certo grau de dificuldade para ser imitado.

Baseado nas características biométricas descritas serão analisados os prós e contras de alguns tipos de dados biométricos: impressão digital, íris e face.

### 2.1.1 Impressão digital

A impressão digital é um dos tipos biometria mais conhecidos, tendo variados motivos para essa grande utilização. A digital tem uma unicidade muito grande a ponto de até gêmeos idênticos se diferenciam nesse ponto. A universalidade desta característica também é um forte ponto, mesmo que tenha problemas em pequenos grupos por questões genéticas, ambientais, idade ou profissão. A invariabilidade é um forte ponto, pois esta é formada durante o estado fetal. A análise de grande volumes de dados de impressão digital podem demandar grandes recursos computacionais, além da necessidade de hardware específico para sua coleta. Dessa maneira, a mensurabilidade e a performance podem se tornar um problema (ROSS; JAIN, 2007).

Figura 1 – Impressão digital

Fonte: <https://unsplash.com/pt-br/fotografias/SRFG7iwktDk>

### 2.1.2 Íris

A íris é a região entre a esclera e a pupila (Figura 2). Tal qual a digital, essa região é desenvolvida durante a fase inicial da vida, mudando apenas a pigmentação com o passar do tempo. Dessa maneira, a textura dessa área se torna um traço muito distinto entre

indivíduos, e assim como na impressão digital, até mesmo gêmeos idênticos conseguem ser diferenciados por esse traço. A acurácia e velocidade dos sistemas atuais são muito promissores na autenticação de íris, ou seja, tem uma grande performance. É possível reconhecer lentes com íris falsas (ROSS; JAIN, 2007), o que a torna difícil outra pessoa reproduzir. Atualmente esse tipo de sistema biométrico está se tornando menos custoso e mais facilmente adquirido. Os sistemas de autenticação desse traço normalmente entregam uma pequena taxa de divergência do real.

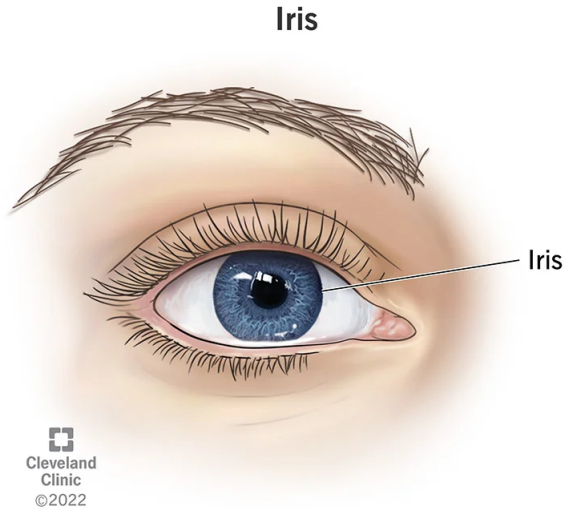



Figura 2 – Iris do olho

Fonte:<https://my.clevelandclinic.org/-/scassets/images/org/health/articles/22502-iris>

### 2.1.3 Face

A biometria da face é o tipo mais "natural" de autenticação, pois é a maneira principal de reconhecimento entre pessoas. Há duas abordagens comumente utilizadas para distinguir faces computacionalmente (ROSS; JAIN, 2007):

1. Localização e formas de atributos faciais, como olhos, boca e nariz.
2. Análise da face completa.

De acordo com Moraes (2010), performance de sistemas de autenticação facial são boas nas condições de tecnologia e custo quando estão em um ambiente controlado. Um problema na extração dessa característica são as diferentes condições de captura

da imagem, ou seja, lugares e iluminações diferentes podem dificultar essa identificação. Outro possível problema é o nível de confiança desta autenticação como único método comprovação de identidade, os níveis de confiança atuais não cumprem o objetivo de vários sistemas.

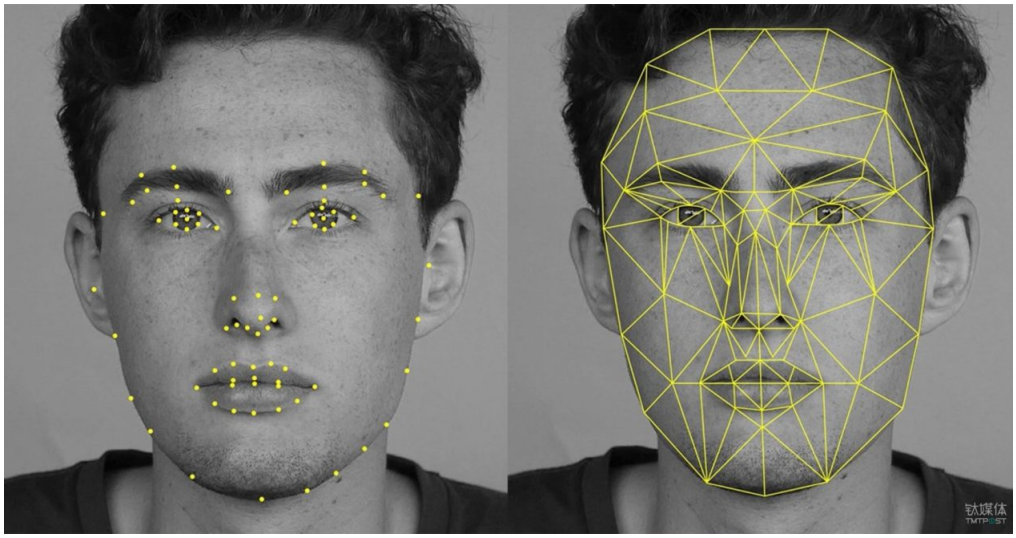


Figura 3 – Biometria Facial

Fonte: <https://macmagazine.com.br/wp-content/uploads/2017/08/21-facial-1260x661.jpg>

## 2.2 Redes Neurais Artificiais

Redes Neurais Artificiais (RNA) são estruturas que simulam um conjunto de neurônios biológicos, que é a unidade básica de processamento dos seres vivos (HAYKIN, 2009). Esse mecanismo foi elaborado pela primeira vez em McCulloch e Pitts (1943) como uma proposta de demonstrar como essas estruturas funcionam em seres vivos.

### 2.2.1 Perceptron

O perceptron é uma implementação mais desenvolvida do neurônio artificial inicial. Essa estrutura foi desenvolvido por Rosenblatt em 1958 e atualizado posteriormente adicionando pesos e o termo Bias que possibilitaram a divisão de classes linearmente separáveis (SILVA, 2022).

A Figura 4 ilustra a estrutura do perceptron com as melhorias descritas. Observa-se que esse neurônio artificial recebe diversas entradas que são somadas multiplicando pelo pesos escolhidos e, após isso, soma-se o termo Bias que visa evitar que a saída seja

nula. Após esse processo, o valor encontrado é inserido em uma função de ativação que varia de acordo com a implementação.

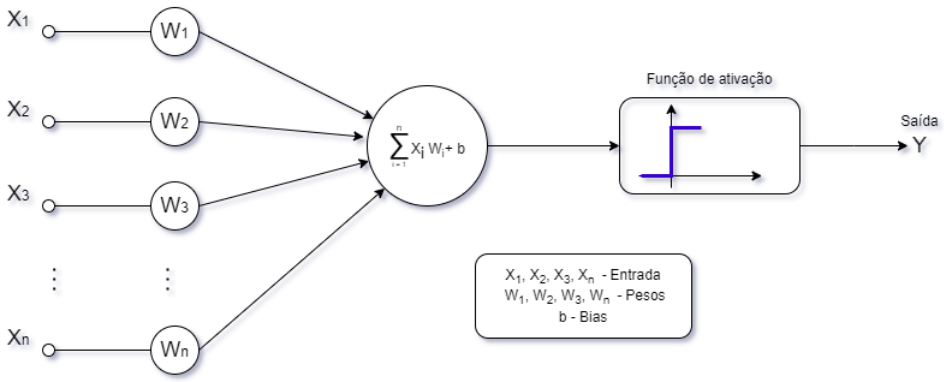



Figura 4 – Estrutura do perceptron

Fonte: Adaptado de Silva (2022)

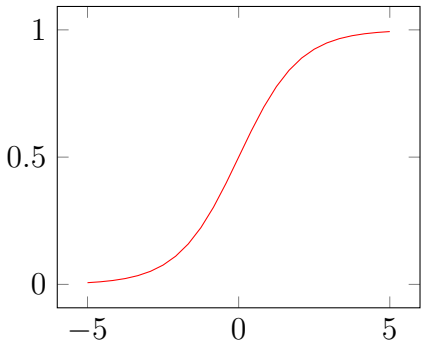
### 2.2.2 Funções de ativação

Funções de ativação são fórmulas matemáticas que definirão as saídas dos neurônios artificiais. Dessa maneira, existem diversas possíveis funções que serão aplicadas a cada perceptron, de acordo com o problema que se busca resolver.

As seguintes fórmulas matemáticas são exemplos de funções de ativação muito utilizados para problemas lineares, ou seja, cenários que podem ser resolvidos com apenas uma divisão (SILVA, 2022):

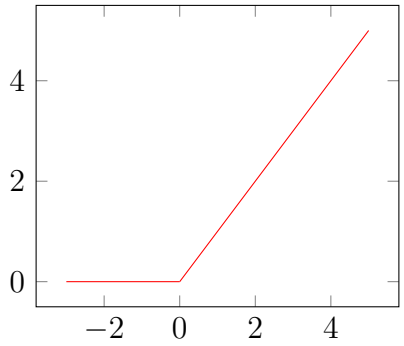
- Função Sigmóide:

$$\frac{1}{1+e^{-}x} \tag{2.1}$$




- Função ReLU (*Rectified Linear Unit*):

$$ReLU = \begin{cases} x, & \text{se } x > 0 \\ 0, & \text{Caso contrario} \end{cases} \tag{2.2}$$




### 2.2.3 Problemas não lineares

A funções descritas na subseção 2.2.2 são úteis para problemas resolvidos pela classificação de duas classes por uma única linha continua. Dessa maneira, há a necessidade de outra abordagem para situações mais complexas, como por exemplo, o problema $XOR$ ilustrado na Figura 5.

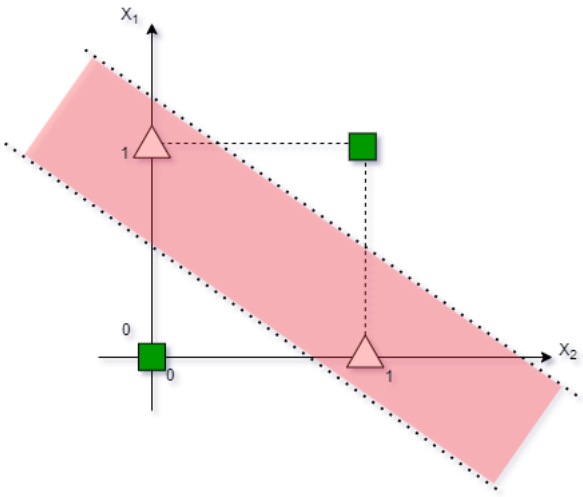



Figura 5 – Divisão de classes $XOR$

Fonte: Géron (2017)

A maneira encontrada para resolver esse problema foi a adição de camadas de perceptrons, ou seja, perceptron de múltiplas camadas (SILVA, 2022).

### 2.2.4 Perceptron de Múltiplas Camadas

O perceptron de múltiplas camadas é o empilhamento de dois ou mais perceptrons de modo que a saída dos neurônios das camadas inferiores servem como entradas para as próximas. Dessa maneira, essa nova arquitetura (Figura 6) consegue resolver problemas não lineares (GÉRON, 2017).

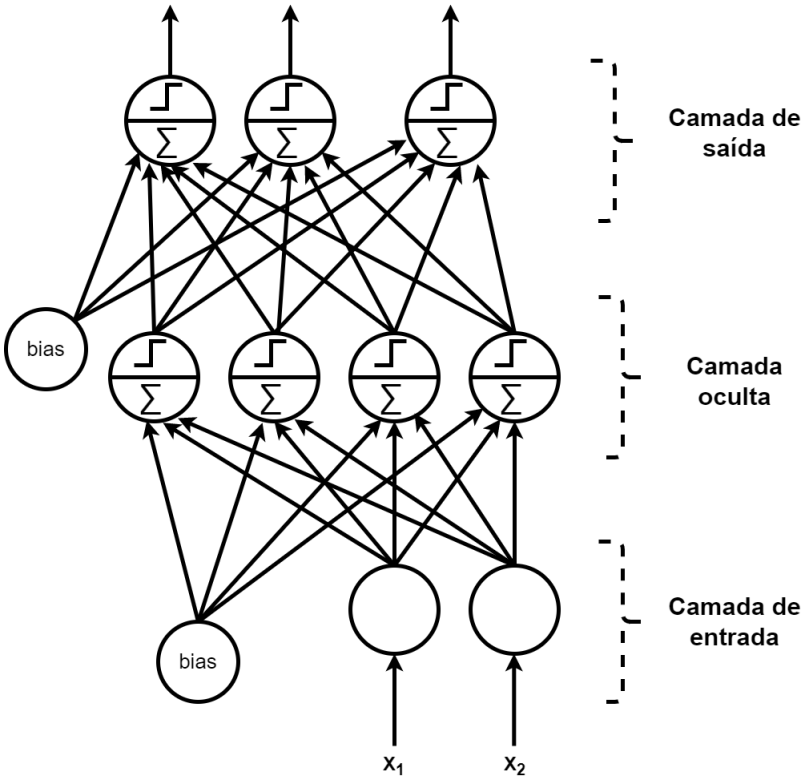



Figura 6 – Perceptron de Múltiplas Camadas

Fonte: adaptado de Silva (2022)

Em problemas como o $XOR$ (Figura 5), somente as múltiplas camadas não são o bastante para realizar a classificação, também é necessário a que os pesos se atualizem dinamicamente (RAUBER, 2014).

### 2.2.5 Redes Neurais Convolucionais

Rumelhart, Hinton e Williams (1986) propuseram o algoritmo de *backpropagation*, isto é, uma retroalimentação de erros para as camadas neurais. Esse algoritmo calcula o erro apos a execução do neurônio e esse gradiente e novamente inserido nos perceptrons repetidamente até o resultado convergir ao esperado.

Essa estrutura foi a origem para a criação das Redes Neurais Convolucionais (CNN). Estas redes são muito adaptativas, o que tornam essas uma grande opção para o reconhecimento computacional de imagens. Dessa maneira, essa estrutura é amplamente usada como classificador de sistemas de reconhecimento facial (O'SHEA; NASH, 2015).

## 2.3 Transfer Learning

Existem vários métodos que foram criados para aprimorar CNN, ou seja, a partir da criação dessas redes é possível adicionar algumas etapas adicionais, além do treinamento padrão, para ter resultados ainda melhores.

O *transfer learning* é um método criado para redes neurais que visa aprimorar os resultados com um "pré-treinamento". Dessa maneira, esse artificio é implementado treinando modelos com tipos específicos de dados e, após esse treino, é adicionado novas camadas nessa rede. Dessa maneira, essa rede se torna "pré-treinada" para aquele tipo de dado especifico, tendo assim, muitas vezes resultados muito favoráveis ao ser treinada com novos dados do mesmo tipo (TORREY; SHAVLIK, 2010).

## 2.4 Detecção Facial

O primeiro desafio na biometria facial é a identificação da face na imagem, ou seja, limitar a parte da imagem no qual o rosto do individuo está. Para isso, foram desenvolvidas diversas técnicas computacionais para executar esse processamento da forma mais eficaz possível, os dois métodos mais amplamente usados são Viola-Jones e *Multi-Task Cascaded Convolutional Neural Network* (MTCNN).

Viola e Jones (2004) propuseram um algoritmo robusto de detecção de objetos, que foi muito usado para a detecção facial. Essa proposta faz o uso de imagem integral para o extração rápida de características, seleção de características *Haar-like*, algoritmo de *Adaptive-boosting* e classificação em cascata (SILVA, 2022).

O algoritmo de Viola-Jones traz um resultado bastante satisfatório na detecção de faces, porém a precisão média de Viola-Jones se mostra inferior quando comparada ao MTCNN (SILVA, 2022).

### 2.4.1 *Multi-Task Cascaded Convolutional Neural Network*

O *Multi-Task Cascaded Convolutional Neural Network* (MTCNN) é uma *Framework* de detecção facial proposto por Zhang et al. (2016). Esse algoritmo, por meio de CNN, redimensiona a imagem de entrada em tamanhos variados, seleciona as possíveis faces e por meio da retro-alimentação vai se adaptando até encontrar o local mais provável da face e os marcadores faciais (Figura 7).

## 2.5 Abordagens de identificação facial

Os estudos conduzidos por Lazarini, Rossi e Hirama (2022) proporcionaram uma análise abrangente das abordagens de detecção facial, destacando quatro métodos notáveis

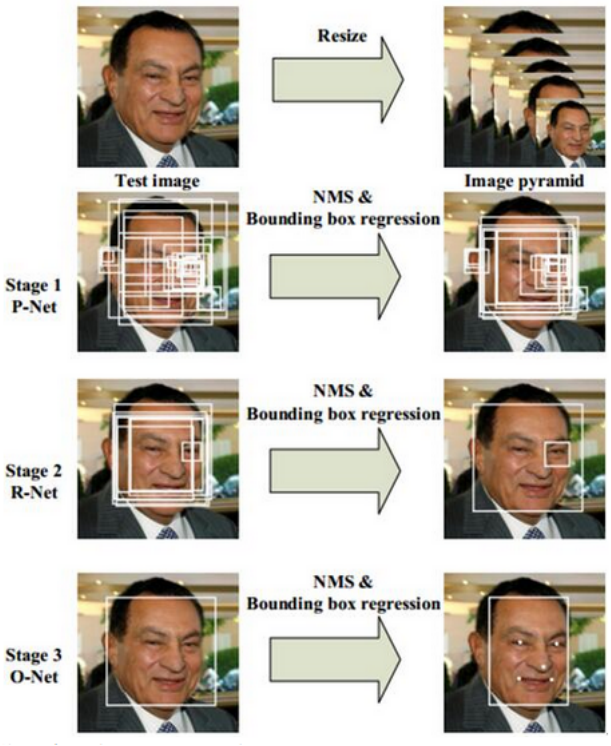



Figura 7 – Exemplo da *Multi-Task Cascaded Convolutional Neural Network*

Fonte: Zhang et al. (2016)

em termos de precisão: *Local Binary Patterns Histograms* (LBPH), EigenFace, FisherFace e Facenet. Dessa maneira, essas serão as técnicas avaliadas na pesquisa.

### 2.5.1 Local Binary Patterns Histograms

O *Local Binary Patterns Histograms* (LBPH) é um algoritmo que consiste na combinação dos métodos de *Local Binary Pattern* (LBP) e *Histogram Oriented Gradients* (HOG) sendo conhecido por sua performance e e acurácia que podem reconhecer uma face de lado e de frente (BUDIMAN et al., 2023).

A partir de um ponto, esse método seleciona blocos de mesmo valor de largura e altura para transformar converter em padrões binários, e dessa maneira e calculado o valor do pixel central o transformando em um limiar para os pixeis vizinhos, ou seja, a partir do cálculo do limiar os pixeis que forem maiores serão transformados em 1 e os menores em 0. A partir disso esse bloco e concatenado com valores do padrão linear binário, transformando esse pixels e os seus vizinhos (Figura 8) (WANG; SIDDIQUE, 2020).

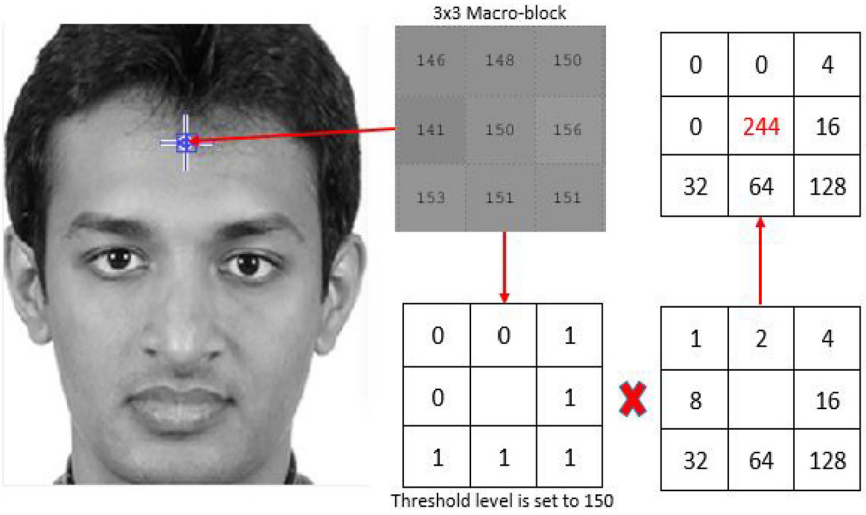



Figura 8 – Exemplo de funcionamento do LBPH

Fonte: Wang e Siddique (2020)

### 2.5.2 Eingenface

Eigenface refere-se ao conjunto de autovetores derivados da matriz de covariância de um conjunto de rostos. Este método visa identificar um conjunto de características independentes das formas geométricas do rosto, como olhos, boca, nariz e orelhas, utilizando a informação de representação facial (LAZARINI; ROSSI; HIRAMA, 2022).

O Eigenface utiliza o algoritmo de Análise de Componentes Principais (PCA) para reduzir a dimensionalidade, o que é muito útil para diminuir a quantidade de dados e, consequentemente, otimizar o número de imagens no conjunto de dados. Dessa maneira,quando esse algoritmo é aplicado ao reconhecimento facial, é denominado Eigenface (LAZARINI; ROSSI; HIRAMA, 2022).

O PCA, ao analisar estatisticamente a redundância e variância dos dados, promove a redução de dimensionalidade sem alterar a informação, garantindo que o resultado permaneça consistente. O algoritmo Eigenface é baseado na aparência, já que não exige conhecimento prévio sobre o que será reconhecido, e um aspecto notável é que busca os principais componentes durante o processo de reconhecimento: os autovetores que descrevem o rosto de uma pessoa, e a partir desse processo é criado um tipo de imagem "média" da face (Figura 9). Contudo, é importante frisar que o algoritmo Eigenface é sensível às condições de iluminação e a certos tipos de ruído, o que pode comprometer sua eficácia e reduzir a precisão do sistema (LAZARINI; ROSSI; HIRAMA, 2022).

Figura 9 – Exemplo faces médias do Eigenface

Fonte: Zhang, Yan e Lades (1997)

### 2.5.3 FisherFace

Fisherface é um algoritmo muito similar ao Eigenface, e de acordo com Lazarini, Rossi e Hirama (2022) ele é considerado uma evolução do método acima, porém utiliza um algoritmo diferente do PCA.

A principal diferença entre os mecanismos de FisherFace e Eigenface é a substituição do do PCA pelo *Linear Discriminant Analysis* (LDA). Essa técnica visa a redução de dimensionalidade a partir de dados multidimensionais rotulados, assim gerando um conjunto de dados com menores dimensões representando os mesmos dados (BISSI, 2018).

O LDA é um método que busca otimizar a separação das classes, o que no contexto de reconhecimento facial, é a separação otimizada das pessoas pelos seus rótulos. Dessa maneira, agrupando as identidades com seus rótulos, esses são reconhecidos como classes e, a partir disso, o método tenta representar a distribuição dos pontos com o objetivo de aumentar a confiabilidade na classificação (BISSI, 2018).

### 2.5.4 Facenet

A partir da pesquisa de Schroff, Kalenichenko e Philbin (2015), a rede neural convolucional Facenet foi construída. Essa CNN foi criada e treinada com o intuito de ter uma grande acurácia no reconhecimento facial em diversos tipos de imagem e iluminação.

Dessa maneira, essa rede neural de múltiplas camadas pode ser usada em diversas bases de dados, ou seja, a partir dos pesos gravados para esses neurônios artificiais é pos-

sível aplicar o treinamento de múltiplas bases de dados (SCHROFF; KALENICHENKO; PHILBIN, 2015).

O estudo de Schroff, Kalenichenko e Philbin (2015) traz diversas experiencias em múltiplas bases de dados. Desse modo, os resultados apresentados trazem uma grande precisão nesse algoritmo, com taxas de acurácia acima de 90%.

## 2.6 Desempenho de sistemas biométricos

Para aplicar a autenticação biométrica em um sistema é necessário ter conhecimento da sua acurácia, ou seja, a taxa de acerto dos classificadores, para que assim seja possível saber se cumpre as exigências do projeto. Dessa maneira, é necessário juntar os dados de teste desse sistema e retornar um tipo de medidor numérico de precisão do sistema.

O sistema biométrico de autenticação ao processar o dado de um indivíduo deve retornar se esse foi validado ou não. Dessa maneira, só é possível um dos quatro seguintes cenários (FAWCETT, 2006):

- **Verdadeiro Positivo (TP)**: O sistema reconheceu o usuário corretamente e liberou o acesso desse aos recursos que tem direito.
- **Verdadeiro Negativo (TN)**: O sistema não reconheceu um usuário, pois ele não está registrado no sistema, ou seja, não libera acesso aos recursos requisitados.
- **Falso Positivo (FP)**: O sistema reconhece um usuário incorretamente, liberando acesso de recursos ao usuário "farsante".
- **Falso Negativo (FN)**: O sistema não reconhece um usuário que deveria ser reconhecido, ou seja, não libera acesso dos recursos erroneamente.

Levando em consideração os cenários mencionados e na Figura 10, é possível calcular as seguintes métricas de acurácia dos sistemas (MORAES, 2010):

- **Taxa de Falsa Aceitação (FAR)**: Essa métrica calcula a possibilidade de o sistema classificar um "farsante" como usuário legitimo. Ela é construída a partir da divisão dos falsos positivos em relação a falsos positivos e verdadeiros negativos

$$FAR = \frac{FP}{FP + TN} \tag{2.3}$$

- **Taxa de Falsa Rejeição (FRR)**: Essa métrica calcula a possibilidade de um usuário legitimo ser classificado como farsante. Esse é construído a partir da divisão de Falsos negativos pela soma de falsos negativos e verdadeiros positivos.

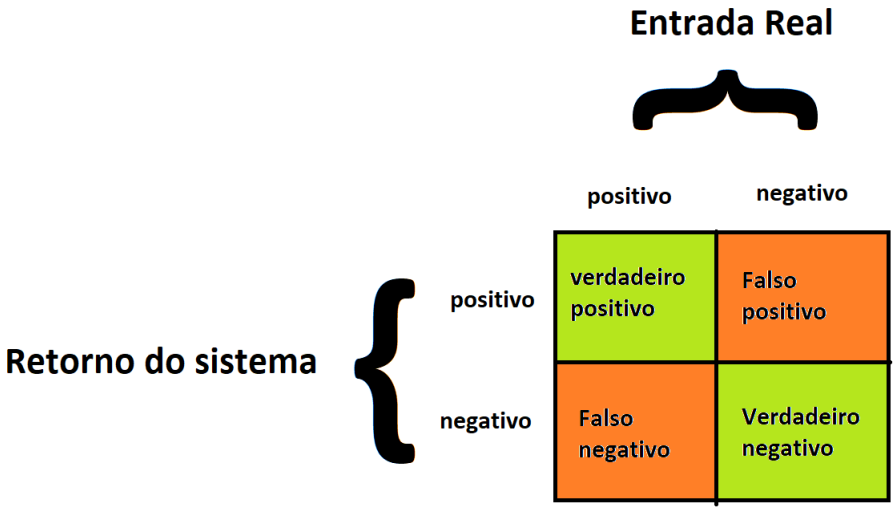



Figura 10 – Gráfico de possíveis situações

Fonte: Adaptado de Moraes (2010)

$$FRR = \frac{FN}{FN + TP} \tag{2.4}$$

- **Taxa de Verdadeiros Positivos (Recall)**: Essa métrica calcula a possibilidade de o sistema identificar o usuário legitimo corretamente. Essa métrica é construída a partir da divisão do número de verdadeiros pela soma de falsos negativos e verdadeiros positivos.

$$Recall = \frac{TP}{FN + TP} \tag{2.5}$$

- **Acurácia**: A taxa de acurácia total calcula a porcentagem de identificações corretas do sistema. Dessa maneira, essa métrica é feita a partir da divisão das identificações corretas (TP + TN) em relação a todo o espaço amostral.(FAWCETT, 2006)

$$Accuracy = \frac{TP + TN}{P + N} \tag{2.6}$$

Levando em consideração as informações observadas acima, é possível descrever um sistema de autenticação biométrica com a Figura 11.

Dessa maneira, para que seja possível separar a resposta do sistema em todas as possíveis classes citadas, é necessário escolher um limite de aceitação e rejeição de acordo com as necessidades do sistema. Dessa maneira, o ponto escolhido irá influenciar diretamente a taxa de falsos positivos e falsos negativo (Figura 12).

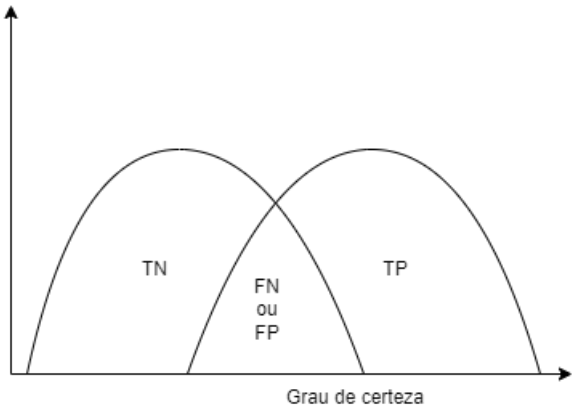



Figura 11 – Distribuição de possíveis cenários

Fonte: Adaptado de Moraes (2010)

Portanto, para sistemas que requerem uma maior segurança é necessário um maior limiar para evitar ao máximo falsos positivos, porém isso acarretara uma maior taxa de falsos negativos. Dessa maneira, sistemas que requerem uma menor taxa de segurança terão a reação inversa.

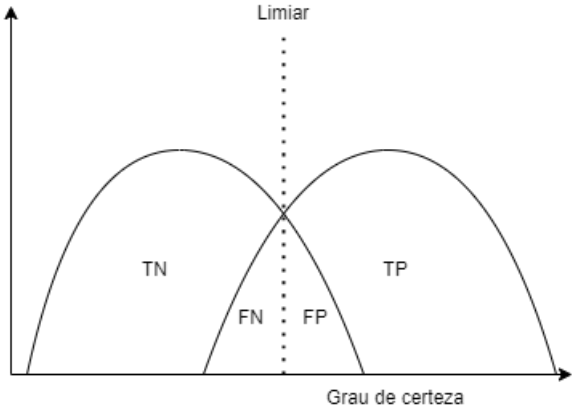



Figura 12 – Distribuição de possíveis cenários com limiar de aceitação

Fonte: Adaptado de Moraes (2010)

Levando em consideração as informações apresentadas, esses conceitos e fórmulas serão usados para medir a performance do sistema, principalmente nas etapas de desenvolvimento e testes.

## 2.7 Trabalhos Correlatos

De acordo com Moraes (2010) a biometria facial deve ser estudada graças a sua grande gama de aplicabilidade, e por ser plausível de ser usada amplamente com as tecnologias atuais. Dessa maneira, o uso da biometria facial se torna muito viável por ser uma biometria fácil de ser coletada e de grande aceitabilidade.

Com o intuito de testar e avaliar as melhores maneiras de detectar e reconhecer pessoas Moraes (2010) desenvolve um protótipo e verifica sua qualidade a partir de testes com banco de imagens e um ambiente real. Para isso, foi usado o método de Viola Jones para a detecção de faces, uma *Virtual Generalizing Random Access Memory* (VG-RAM), ou seja, uma rede neural sem peso e técnicas probabilísticas bayesianas para o controle de acesso.

Segundo os autores, os ensaios trouxeram resultados relativamente satisfatórios, de acordo com a necessidade do sistema. Os testes com bancos de imagens trouxeram resultados entre 90 e 93 % de Recall e um índice de 0,77 a 4,76 % de FAR. Além disso, sua aplicação em um ambiente real com poucos indivíduos trouxe um Recall de 91,67 % e um FAR de 10 %.

O artigo de Almeida et al. (2022) busca desenvolver um sistema para reconhecimento facial conectado a chamada escolar. Dessa maneira, o autor escolhe desenvolver essa pesquisa na linguagem Python com a biblioteca Opencv.

A pesquisa foi separada em 3 partes principais: captura e tratamento de imagem, detecção de face e reconhecimento. Para tratar a imagem, é feita uma conversão para a escala de cinza. Na segunda etapa, a face é encontrada na imagem a partir dos algoritmos de Viola Jones e um classificador Haar. Dessa maneira, os dados coletados podem ser comparados com novas imagens para reconhecer faces.

O artigo não apresenta um resultado numérico sobre a eficácia o sistema desenvolvido. Entretanto, a pesquisa traz dados de comparação da acurácia de sistemas de reconhecimento de faces de acordo com gênero e cor de pele. Dessa maneira, traz à tona a problemática desses sistemas em mulheres negras na faixa de 18 a 30 anos.

Saxberg, Cai e Li (2018) evidenciam que a autenticação facial tem grandes utilidades no contexto histórico atual, mas, em contrapartida, precisam ser usadas com outra camada de segurança para impedir as falhas causados por essa abordagem “pura”. Desse modo, para evitar a necessidade de equipamentos de maior custo, os escritores propõem que o usuário faça um gesto aleatório especificado pelo sistema, para provar a presença real do usuário.

Usando *deep learning*, a linguagem Python com a biblioteca Scikit, os autores criaram um sistema com um servidor web, uma API e um banco de dados. Este projeto

identifica se o usuário é compatível com os dados da pessoa salvos no banco de dados, sendo compatível, o programa requer que o indivíduo faça um gesto específico que também será reconhecido.

O projeto conclui com uma acurácia de reconhecimento de 99% comparando o usuário diretamente a pessoa que reivindica ser. Além disso, o projeto pretende ser uma espécie de sistema de reconhecimento independente, ou seja, este pode ser ligado a outros sistemas para que faça o reconhecimento desses de maneira privada, não precisando dar todas as informações para o sistema que foi conectado.

A dissertação de Silva (2022), foi escrita durante a pandemia iniciada em 2020. Diante esse contexto, é proposto a criação de um *plugin* de autenticação para um sistema de ensino online, pois era o único método de ensino viável.

O sistema proposto utilizou as Redes Neurais Convolucionais Profundas para a detecção da face e para a verificação facial. Na etapa de localização da face, foi usado o método MTCNN para apresentar o local do rosto e marcadores faciais. Na etapa de autenticação, foi utilizado uma Rede Neural Residual (ResNet) para a extração de características em um vetor de 128 dimensões.

Segundo os autores, o programa foi testado em ambiente de produção com alguns alunos durante 2 períodos de aulas online. Houve uma aprovação media de 75% pelos usuários e uma acurácia do sistema de até 98,96%.

# 3 Experimentos

Os experimentos dessa pesquisa visam comparar os resultados das diferentes abordagens de identificação facial e demonstrar qual técnica seria mais eficiente e de melhor implementação em um contexto geral.

Para a implementação dos diferentes métodos foi utilizado a biblioteca OpenCV para os modelos de EigenFace, FisherFace e LBPH, e as bibliotecas Sklearn e Keras para o implementação do modelo Facenet.

O modelo pré-treinado do FaceNet foi obtido a partir do repositório Taniai (2021) que é um dos diversos modelos pré-treinados do Facenet que podem ser encontrados. Dessa maneira, esse modelo utiliza o método de *Transfer Learning* para o reconhecimento de faces.

## 3.1 Datasets

A primeira base de dados selecionada para os experimentos foi a *Labelled Faces in the Wild* (LFW), esta é uma base de dados disponibilizada online [1] pela Universidade de Massachusetts. Este *dataset* é muito usado em diversas pesquisas pois traz uma ampla quantidade de pessoas separadas e rotuladas com diferentes quantidades de imagens, sendo assim, uma boa escolha para treinar e testas algoritmos de reconhecimento facial (LEARNED-MILLER et al., 2016).

Para o uso da base de dados de LFW, foi feito um tratamento prévio para torná-la mais coerente com os objetivos dessa pesquisa. Dessa maneira, houve a seleção apenas de indivíduos com 10 ou mais fotos para serem usadas, assim excluindo todos os indivíduos que tivessem uma quantidade menor de imagens. Portanto, após esse processo, permaneceram 158 pessoas diferentes com o total somado de 4.324 imagens.

A segunda base de dados escolhida foi o *Celebrity Face Image Dataset*, que é um *dataset* de diversas imagens de 17 famosos distintos, também disponibilizada online[2]. Dessa maneira, essa base de dados foi escolhida por ter uma menor quantidade de pessoas em relação ao LFW, e ao mesmo tempo, uma grande quantidade de imagens para todos eles. Dessa maneira, o *Celebrity Face Image Dataset* foi usado em sua totalidade, assim contemplando 1.800 imagens de 17 indivíduos distintos.

[1] <https://vis-www.cs.umass.edu/lfw/index.html>
[2] <https://www.kaggle.com/datasets/vishesh1412/celebrity-face-image-dataset>

## 3.2 Implementação

Os dois métodos de detecção facial (Viola-Jones e MTCNN) foram testados nas duas bases de dados. Dessa maneira, pôde-se analisar qual método de detecção seria mais adequado para este contexto.

Como mencionado por Silva (2022), MTCNN foi capaz de detectar mais faces do que o algoritmo de Viola-Jones. Porém, como esse método detecta faces que não estão em primeiro plano, o que não se alinha com os objetivos da pesquisa.

Um exemplo desse comportamento pode ser visto na aplicação desses algoritmos na Figura 13. Como afirmado anteriormente, o algoritmo de Viola-Jones (Figura 14) extraiu apenas a face em primeiro plano, enquanto o MTCNN extraiu uma face de segundo plano (Figura 15).

Figura 13 – Imagem do *dataset* LFW para detecção.

Figura 14 – Face detectado por Viola-Jones

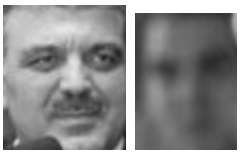


Figura 15 – Faces detectadas por MTCNN

Como o algoritmo de Viola-Jones é suficientemente satisfatório para este contexto, foi optado o uso dele para os testes de eficiência dos métodos de reconhecimento.

Os modelos apresentados pela biblioteca OpenCV, trazem a necessidade de que as imagens de teste e treino estejam em escala de cinza, e o modelo de Facenet requer

imagens coloridas com o tamanho 160x160 pixels. Dessa maneira, para todos os seguintes testes foram aplicadas esses requisitos nas imagens e foi fixado o tamanho 160x160 pixels para faces extraídas das imagens de teste. Além disso, em todos os testes optou-se pela proporção de 70% das imagens para treinamento e 30% para testes por ser uma um razão apresentada em diversas pesquisas.

### 3.2.1 Experimento 1

O primeiro experimento foi realizado da seguinte forma: o LFW por ter uma grande quantidade de indivíduos, e relativamente poucas imagens por pessoa, foi testado gradualmente começando de 10% do tamanho total e aumentando 10% a cada passo até sua totalidade. Dessa maneira, pode-se analisar o quanto a quantidade de personagens afeta os algorítimos.

Portanto, inicialmente foi feito o tratamento das imagens da maneira mencionada anteriormente para os métodos de reconhecimento apresentados pelo OpenCV (Eigenface, Fisherface e LBPH). Após isso, foi realizado o treinamento desses modelos com 10% até 100% nos *datasets*. Os resultados de todas as etapas foram armazenados em um arquivo de texto separado, para fazer a comparação dos métodos posteriormente.

Sequencialmente, foi feito o tratamento das imagens para o uso com Facenet. Após isso, foi carregado o modelo pré-treinado do Facenet e as imagens foram colocadas para treinamento e testes. Em seguida, todas as análises de qualidade desse modelo também foram salvas em um arquivo de texto separado.

Portanto, a partir dos experimentos descritos, foi possível juntar a informações de todos os resultados de acurácia (Tabela 1).

Tabela 1 – Resultado das acurácias dos testes para o *dataset* LFW.

| Imagens | LBPH | EIGENFACE | FISHERFACE | FACENET |
|---|---|---|---|---|
| 10% | 0,7879 | 0,5152 | 0,6364 | 0,9899 |
| 20% | 0,7293 | 0,3094 | 0,5028 | 0,9890 |
| 30% | 0,6877 | 0,2702 | 0,3789 | 0,9895 |
| 40% | 0,6691 | 0,2038 | 0,3189 | 0,9928 |
| 50% | 0,6844 | 0,2145 | 0,2979 | 0,9947 |
| 60% | 0,7058 | 0,2349 | 0,2849 | 0,9884 |
| 70% | 0,6840 | 0,2106 | 0,2219 | 0,9898 |
| 80% | 0,6589 | 0,1966 | 0,2022 | 0,9898 |
| 90% | 0,6507 | 0,1845 | 0,1640 | 0,9863 |
| 100% | 0,6467 | 0,1778 | 0,1568 | 0,9860 |

Dessa maneira, foi possível criar um gráfico com essas informações para analisar a mudança de comportamento de acordo com o aumento de indivíduos nos modelos (Figura 16).

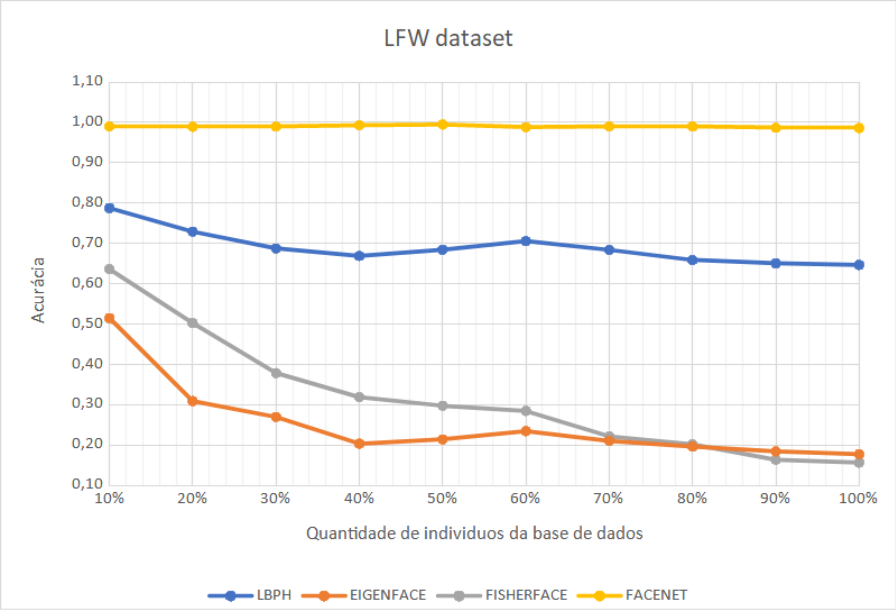



Figura 16 – Resultado das acurácias dos testes para o *dataset* LFW.

Portanto, é notável a superioridade do Facenet em relação aos outros métodos, já que teve uma acurácia maior em todas as fases e, além disso, manteve uma acurácia com pouca variação em todas as etapas. Também é notável que os algoritmos de LBPH, Fisherface e Eigenface demonstraram uma queda na acurácia de acordo com o aumento de indivíduos na base de dados, porém nos algoritmos de Fisherface e Eigenface esse diminuição foi mais significativa.

### 3.2.2 Experimento 2

O segundo experimento foi realizado com a totalidade do *Celebrity Face Image Dataset*, pois esse tem uma quantidade mais elevada de imagens por indivíduo. Portanto, com esse teste pode se analisar se há uma grande melhora no algoritmo tendo mais imagens por indivíduo e menos personagens distintos.

Primeiramente, foi feita todo o tratamento de imagem desta segunda base de dados para os três primeiros métodos (LBPH, Eigenface e Fisherface), da mesma maneira que foi feita para o primeiro experimento. Assim, após tratadas foi feita a separação de 70% e 30% das imagens de cada indivíduo para treino e teste respectivamente. Após isso, os três métodos foram treinados e testados, e por seguinte, todos os resultados foram exportados para um arquivo de texto.

Assim como o primeiro experimento, todos os tratamentos de imagem e repartição de imagens foi feita aos requisitos do Facenet. E, da mesma maneira, todos os resultados foram salvos em um arquivo de texto.

Portanto, após a juntar esses dados é possível criar a Tabela 2 e a Figura 17 para a análise de comportamento dos algoritmos.

Tabela 2 – Resultados das acurácias para o *dataset Celebrity*.

| LBPH | EIGENFACE | FISHERFACE | FACENET |
|---|---|---|---|
| 0,7216 | 0,3118 | 0,1114 | 1,0000 |

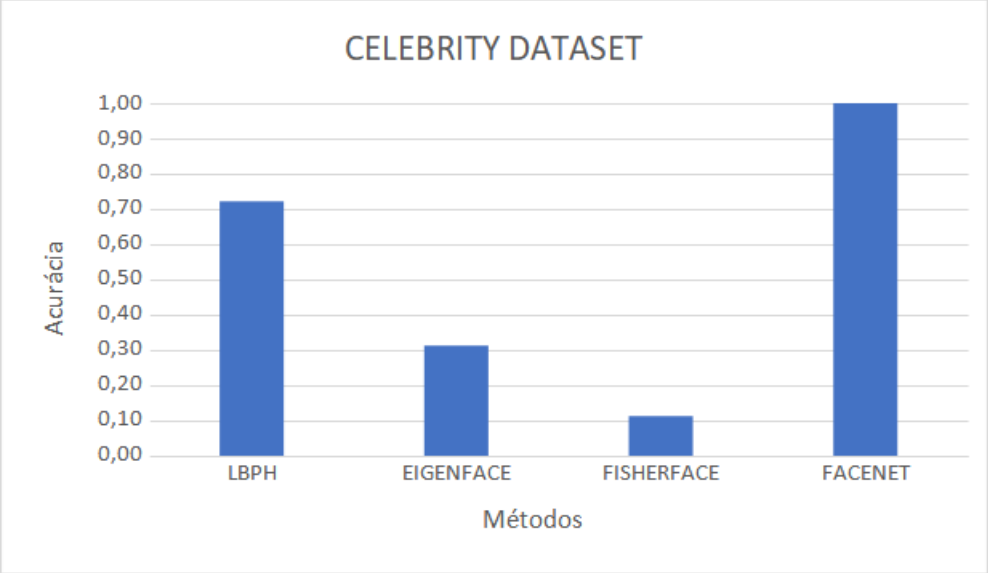



Figura 17 – Gráfico com os resultados das acurácias para o *dataset Celebrity*.

Dessa maneira, como pode ser observado na Figura 17, Facenet se manteve superior aos outros tendo uma acurácia perfeita. Entretanto, levando em consideração que a quantidade de pessoas nesse experimento é próxima da quantidade de pessoas na primeira etapa do primeiro experimento, este teve uma pior acurácia em todos os outros métodos além do facenet. Dessa maneira, pode ser observado que o modelo LBPH teve apenas um pequeno decréscimo, porem nos outros 2 métodos esse resultado caiu drasticamente.

### 3.2.3 Comparações

Existem outras pesquisas que usam esses métodos com a base de dados LFW. Dessa maneira, pode ser comparado os resultados obtidos nos testes apresentados anteriormente com artigos da literatura (Tabela 3).

Tabela 3 – Tabela comparativa dos métodos que utilizaram o *dataset* LFW.

| **Método** | **Artigo de Referência** | **Acurácia de referência** | **Acurácia Obtida** |
|---|---|---|---|
| FaceNet | Learned-Miller et al. (2016) | Entre 98,87% até 99,6% | 98,6% |
| Fisherface | Learned-Miller et al. (2016) | 87,47 +/- 1,49% | 15% |
| Eigenfaces | Learned-Miller et al. (2016) | 60,02 +/- 0,79% | 17% |
| LBPH | Alamri et al. (2022) | 88% | 64% |

# 4 Conclusão

Essa pesquisa visa contribuir para o entendimento de métodos de reconhecimento facial muito reconhecidos pela comunidade acadêmica e seus resultados em diferentes situações. Dessa maneira, a intenção é deixar os dados claros para futuras pesquisas.

A partir dos experimentos e comparações com outros estudos, pode se concluir que é possível fazer melhores implementação do métodos Eigenface, FisherFace e LBPH, do que os estudados nessa pesquisa. Dessa maneira, é possível notar que essas implementações tiveram resultados menos favoráveis em comparação a outros estudos que aplicaram os mesmos métodos e base de dados.

O modelo de reconhecimento Facenet trouxe resultados bastante satisfatórios em termos de acurácia. Dessa maneira, este método se provou digno de seu grande reconhecimento e também demonstrou que o uso do artifício de *Transfer Learning* é muito adequado para esse contexto.

A proposta inicial deste trabalho foi publicada nos anais do XVII Workshop de Teses e Dissertações em Ciência da Computação (WTDCC) no ano de 2023 com o título: ”Estudo e Análise de Algoritmos modernos para reconhecimento facial” (SILVA; RIBEIRO, 2023).

## 4.1 Trabalhos Futuros

A partir dos dados apresentados nessa pesquisa é possível originar diversas novas pesquisas como as apresentadas abaixo.

- Um estudo focado na implementação dos modelos de EigenFace, FisherFace e LBPH com o intuito de encontrar os melhores resultados possíveis utilizando esses métodos.
- Aplicação do modelo Facenet sem o uso de *Transfer Learning* para se comparar o real impacto dessa prática.
- Implementação dos modelos apresentados em aplicações reais e estudar se esses métodos são apropriados para o uso em aplicativos com resultados imediatos.

# Referências

ALAMRI, H.; ALSHANBARI, E.; ALOTAIBI, S.; ALGHAMDI, M. Face recognition and gender detection using sift feature extraction, lbph, and svm. **Engineering, Technology & Applied Science Research**, v. 12, n. 2, p. 8296–8299, Apr. 2022. Disponível em: <https://www.etasr.com/index.php/ETASR/article/view/4735>. Citado na página 35.

ALMEIDA, L. F. d. O.; TANAKA, P. A. d. S.; OLIVEIRA, V. H. M.; VALDO, C. A. Sistema de chamada escolar com reconhecimento facial utilizando opencv. **Revista de Ubiquidade**, v. 5, n. 2, p. 1–16, 2022. Disponível em: <https://revistas.anchieta.br/index.php/RevistaUbiquidade/article/view/2030/1753>. Citado na página 28.

BISSI, T. **Reconhecimento facial com os algoritmos eigenfaces e fisherfaces**. Tese (Dissertation) — Universidade Federal de Uberlândia, Universidade Federal de Uberlândia, Jul 2018. Disponível em: <https://repositorio.ufu.br/handle/123456789/22158>. Citado na página 24.

BUDIMAN, A.; FABIAN; YAPUTERA, R. A.; ACHMAD, S.; KURNIAWAN, A. Student attendance with face recognition (lbph or cnn): Systematic literature review. **Procedia Computer Science**, v. 216, p. 31–38, 2023. ISSN 1877-0509. 7th International Conference on Computer Science and Computational Intelligence 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S187705092202186X>. Citado na página 22.

FAWCETT, T. An introduction to roc analysis. **Pattern Recognition Letters**, v. 27, n. 8, p. 861–874, Jun 2006. Disponível em: <https://doi.org/10.1016/j.patrec.2005.10.010>. Citado 2 vezes nas páginas 25 e 26.

GÉRON, A. **Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems**. O'Reilly Media, 2017. ISBN 9781491962244. Disponível em: <https://books.google.com.br/books?id=bRpYDgAAQBAJ>. Citado na página 19.

HAYKIN, S. **Neural Networks and Learning Machines**. Prentice Hall, 2009. (Neural networks and learning machines, v. 10). ISBN 9780131471399. Disponível em: <https://books.google.com.br/books?id=K7P36lKzI_QC>. Citado na página 17.

HONG, L.; JAIN, A. Integrating faces and fingerprints for personal identification. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 20, n. 12, p. 1295–1307, 1998. Disponível em: <https://doi.org/10.1109/34.735803>. Citado na página 14.

LAZARINI, M. A.; ROSSI, R.; HIRAMA, K. A systematic literature review on the accuracy of face recognition algorithms. **EAI Endorsed Transactions on Internet of Things**, v. 8, n. 30, p. e5, Sep. 2022. Disponível em: <https://publications.eai.eu/index.php/IoT/article/view/2346>. Citado 3 vezes nas páginas 21, 23 e 24.

LEARNED-MILLER, E.; HUANG, G. B.; ROYCHOWDHURY, A.; LI, H.; HUA, G. Labeled faces in the wild: A survey. In: _____. **Advances in Face Detection and Facial Image Analysis**. Cham: Springer International Publishing, 2016. p. 189–248. ISBN 978-3-319-25958-1. Disponível em: <https://doi.org/10.1007/978-3-319-25958-1_8>. Citado 2 vezes nas páginas 30 e 35.

MCCULLOCH, W. S.; PITTS, W. A logical calculus of the ideas immanent in nervous activity. **The Bulletin of Mathematical Biophysics**, v. 5, n. 4, p. 115–133, 1943. Disponível em: <https://doi.org/10.1007/BF02478259>. Citado na página 17.

MORAES, J. Controle de acesso baseado em biometria facial. 2010. 102 f. dissertação (mestrado em informática). Santo, Centro Tecnológico, Vitória, 2010. Disponível em: <http://repositorio.ufes.br/handle/10/4231>. Citado 6 vezes nas páginas 11, 16, 25, 26, 27 e 28.

O'SHEA, K.; NASH, R. An introduction to convolutional neural networks. **CoRR**, abs/1511.08458, 2015. Disponível em: <https://doi.org/10.48550/arXiv.1511.08458>. Citado na página 20.

RAUBER, T. Redes neurais artificiais. 2014. Disponível em: <https://www.researchgate.net/profile/Thomas-Rauber-2/publication/228686464_Redes_neurais_artificiais/links/02e7e521381602f2bd000000/Redes-neurais-artificiais.pdf>. Citado na página 20.

ROSS, A.; JAIN, A. K. Human recognition using biometrics: an overview. **Annales Des Télécommunications**, v. 62, n. 1-2, p. 11–35, Jan 2007. Disponível em: <https://doi.org/10.1007/bf03253248>. Citado 4 vezes nas páginas 11, 14, 15 e 16.

RUMELHART, D. E.; HINTON, G. E.; WILLIAMS, R. J. Learning internal representations by error propagation. In: _____. **Parallel Distributed Processing: Explorations in the Microstructure of Cognition, Vol. 1: Foundations**. Cambridge, MA, USA: MIT Press, 1986. p. 318–362. ISBN 026268053X. Citado na página 20.

SAXBERG, T.; CAI, S.; LI, R. Login authentication with facial gesture recognition. p. 111, 2018. Disponível em: <https://scholarcommons.scu.edu/cgi/viewcontent.cgi?article=1110&context=cseng_senior>. Citado na página 28.

SCHROFF, F.; KALENICHENKO, D.; PHILBIN, J. Facenet: A unified embedding for face recognition and clustering. **CoRR**, abs/1503.03832, 2015. Disponível em: <http://arxiv.org/abs/1503.03832>. Citado 2 vezes nas páginas 24 e 25.

SILVA, D. G. d. **Autenticação utilizando Atributos Faciais obtidos por Redes Neurais Convolucionais em Sistema de Gestão de Aprendizado**. Tese (Doutorado) — Universidade Federal do ABC, Feb 2022. Disponível em: <http://biblioteca.ufabc.edu.br/index.php?codigo_sophia=122442>. Citado 7 vezes nas páginas 17, 18, 19, 20, 21, 29 e 31.

SILVA, E. V. C. e; RIBEIRO, T. P. Estudo e análise de algoritmos modernos para reconhecimento facial. In: **Anais do X FACOM TECHWEEK e XVII Workshop de Teses e Dissertações em Ciência da Computação (WTDCC)**. Uberlândia - MG: [s.n.], 2023. Citado na página 36.

TANIAI, H. **nyoki-mtl/keras-facenet**. 2021. Disponível em: <https://github.com/nyoki-mtl/keras-facenet>. Citado na página 30.

TORREY, L.; SHAVLIK, J. Transfer learning. In: **Handbook of research on machine learning applications and trends: algorithms, methods, and techniques**. [S.l.]: IGI global, 2010. p. 242–264. Citado na página 21.

VIOLA, P.; JONES, M. J. Robust real-time face detection. **International Journal of Computer Vision**, v. 57, n. 2, p. 137–154, May 2004. Disponível em: <https://doi.org/10.1023/b:visi.0000013087.49260.fb>. Citado na página 21.

WANG, L.; SIDDIQUE, A. A. Facial recognition system using lbph face recognizer for anti-theft and surveillance application based on drone technology. **Measurement and Control**, v. 53, n. 7-8, p. 1070–1077, 2020. Disponível em: <https://doi.org/10.1177/0020294020932344>. Citado 2 vezes nas páginas 22 e 23.

ZHANG, J.; YAN, Y.; LADES, M. Face recognition: eigenface, elastic matching, and neural nets. **Proceedings of the IEEE**, v. 85, n. 9, p. 1423–1435, 1997. Citado na página 24.

ZHANG, K.; ZHANG, Z.; LI, Z.; QIAO, Y. Joint face detection and alignment using multitask cascaded convolutional networks. **IEEE Signal Processing Letters**, Institute of Electrical and Electronics Engineers (IEEE), v. 23, n. 10, p. 1499–1503, oct 2016. Disponível em: <https://doi.org/10.1109%2Flsp.2016.2603342>. Citado 2 vezes nas páginas 21 e 22.