

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS DIVINÓPOLIS

Pablo Sousa da Silva

**AUTENTICAÇÃO BIOMÉTRICA NO CONTROLE DE ACESSO DO CEFET-MG:
MODERNIZAÇÃO TECNOLÓGICA EM RELAÇÃO AO CARTÃO NFC**

Divinópolis - MG

2026

PABLO SOUSA DA SILVA

**AUTENTICAÇÃO BIOMÉTRICA NO CONTROLE DE ACESSO DO CEFET-MG:
MODERNIZAÇÃO TECNOLÓGICA EM RELAÇÃO AO CARTÃO NFC**

Trabalho de Conclusão de Curso apresentado no curso de Graduação em Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais como requisito parcial para obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Me. Diego Ascânio Santos
Coorientador(a): Prof. Dra. Thabatta Moreira Alves de Araújo

DIVINÓPOLIS - MG

2026

PABLO SOUSA DA SILVA

**AUTENTICAÇÃO BIOMÉTRICA NO CONTROLE DE ACESSO DO CEFET-MG:
MODERNIZAÇÃO TECNOLÓGICA EM RELAÇÃO AO CARTÃO NFC**

Trabalho de Conclusão de Curso
apresentado no curso de Graduação em
Engenharia de Computação do Centro
Federal de Educação Tecnológica de Minas
Gerais como requisito parcial para obtenção
do título de Bacharel em Engenharia de
Computação.

Aprovado em 3 de fevereiro de 2026.

Título Nome

CEFET-MG Campus Divinópolis

Título Nome

CEFET-MG Campus Divinópolis

Título Nome

CEFET-MG Campus Divinópolis

Dedico aos meus pais e amigos que
me auxiliaram durante o processo de
construção deste trabalho.

AGRADECIMENTOS

Qual a diferença entre dedicatória e agradecimento?

A dedicatória na maioria das vezes é um texto curto, sucinto e bem objetivo que destaca a pessoa ou pessoas mais importantes na sua vida. Quando relacionada a vida pessoal, o autor deve agradecer a sua esposa, esposo, filhos, mãe, pai e avós.

No caso dos agradecimentos você não precisa se preocupar com o tamanho do texto. Você pode escrever um pouco mais sobre as pessoas que foram essenciais para seu sucesso. Nos agradecimentos, o autor pode falar da instituição, professores, coordenadores e amigos.

Exemplo: [link](#)

Agradeço primeiramente ao professor Msc. Dilson José Aguiar de Souza pela oportunidade de me orientar na conclusão deste trabalho e me ajudar na realização dos ensaios, além de me auxiliar com muita paciência.

Aos meus pais, Rubem Farias da Silva e Regina Cirinéia Menezes da Silva, por terem me dado força e sustentabilidade financeira no início do curso para chegar a esse momento. Aproveito também a oportunidade para agradecer todo o aporte que me deram em casa e o amor dedicado.

Aos meus irmãos Ana Paula Menezes da Silva e Alexandre Menezes da Silva pelas oportunidades de aprendizagem e troca de experiências.

À minha namorada Nicole Luise Fröhlich Kunsler pela dedicação oferecida, pelos momentos de companheirismo e pela compreensão aos momentos de ausência.

À empresa BLEISTAHLS BRASIL METALURGIA S/A, em especial ao funcionário Manfred Kunrath, pela oportunidade de realizar o trabalho de conclusão com materiais fornecidos pela empresa, além de dar apporte financeiro para aquisição de materiais de apoio para a realização dos ensaios.

À empresa LESI Comércio e Representações LTDA, em especial a Fernando Mattes, representante na região da empresa SECO TOOLS que cedeu as ferramentas de corte para os ensaios.

Agradeço à UNISINOS pela cessão dos laboratórios da universidade e ao corpo de

funcionários da casa, principalmente aos que me deram apoio e auxílio quando possível e sempre que necessário.

“O ontem é história, o amanhã é um mistério, mas o hoje é uma dádiva. É por isso que se chama presente.”

Mestre Oogway

RESUMO

O resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento. A ordem e a extensão destes itens dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. Deve ser precedido da referência do documento, com exceção do resumo inserido no próprio documento, e ser composto de uma sequência de frases concisas, de cunho afirmativo e sem enumeração de tópicos, dado que se recomenda o uso de parágrafo único. As palavras-chave devem figurar logo abaixo do resumo, antecedidas da expressão palavras-chave, e finalizadas também por ponto. É importante evitar:

- a) símbolos e contrações que não sejam de uso corrente;
- b) fórmulas, equações, diagramas e similares que não sejam absolutamente necessários; quando seu emprego for imprescindível, deve-se defini-los na primeira vez em que aparecerem.

Quanto à extensão, os resumos devem ter:

- a) de 150 a 500 palavras os de trabalhos acadêmicos (teses, dissertações e outros) e relatórios técnico-científicos;
- b) de 100 a 250 palavras os de artigos de periódicos;
- c) de 50 a 100 palavras os destinados a indicações breves.

Como tratado, o resumo deve ser seguido das palavras representativas do conteúdo do trabalho, isto é, palavras-chave, ou descritores, no idioma em que foi redigido (mínimo 3). Elas devem ser separadas por ponto e vírgula e finalizadas com ponto final.

Palavras-chave: Palavra-chave 1; Palavra-chave 2; Palavra-chave 3; Palavra-chave 4; Palavra-chave 5.

ABSTRACT

Tradução do resumo em português.

Keywords: Keywords 1; Keywords 2; Keywords 3; Keywords 4; Keywords 5.

LISTA DE ILUSTRAÇÕES

Figura 1 – Pipeline metodológico adotado.	9
Figura 2 – Variações sintéticas de uma identidade facial.	13
Figura 3 – Espaço de <i>embeddings</i> antes e após o aprendizado.	16
Figura 4 – Distribuição das distâncias cosseno no espaço de embeddings	19
Figura 5 – Exemplo de par da mesma identidade corretamente aceitos	22
Figura 6 – Exemplo de par de identidades diferentes corretamente rejeitados	22

LISTA DE TABELAS

Tabela 1 – Comparação dos Frameworks	1
Tabela 2 – Resultados de desempenho para diferentes valores de <i>threshold</i> , incluindo TP, FP, TN, FN, FAR e FRR	20

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados Pessoais
NFC	Comunicação por Campo de Proximidade, do inglês Near Field Communication
GANs	Redes Generativas Adversariais, do inglês Generative Adversarial Networks
JSON	Notação de Objeto JavaScript, do inglês JavaScript Object Notation
FAR	Taxa de Falsa Aceitação, do inglês False Acceptance Rate
FRR	Taxa de Falsa Rejeição, do inglês False Rejection Rate
CEFET-MG	Centro Federal de Educação Tecnológica de Minas Gerais
TP	Verdadeiro Positivo, do inglês True Positive
FP	Falso Positivo, do inglês False Positive
TN	Verdadeiro Negativo, do inglês True Negative
FN	Falso Negativo, do inglês False Negative

SUMÁRIO

1	INTRODUÇÃO	1
1.1	Figuras e Tabelas	1
1.2	Citação	1
1.2.1	Início do texto	1
1.3	Alíneas	2
1.4	Customização	2
2	FUNDAMENTAÇÃO TEÓRICA	4
2.1	Contexto do problema e cenário de aplicação	4
2.2	RFID, NFC e cartões de identificação	4
2.2.1	RFID: conceito e funcionamento básico	4
2.2.2	NFC e sua relação com RFID	4
2.2.3	Custos e limitações operacionais em ambientes reais	4
2.2.4	Vulnerabilidades e riscos em sistemas baseados em cartões	4
2.3	Fundamentos de biometria aplicada ao controle de acesso	4
2.3.1	Conceito de biometria e principais modalidades	5
2.3.2	Verificação biométrica (1:1) e identificação biométrica (1:N)	5
2.3.3	Critérios de qualidade em sistemas biométricos	5
2.4	Representação e processamento de imagens digitais	5
2.4.1	Imagem digital: definição e características	5
2.4.2	Etapas de pré-processamento em imagens faciais	5
2.5	Representação vetorial e medidas de similaridade	5
2.5.1	Conceito de vetor e interpretação geométrica	5
2.5.2	Embeddings como representação de características	6
2.5.3	Métricas de similaridade e distância	6
2.5.4	Limiar de decisão em sistemas de reconhecimento	6
2.6	Aprendizado métrico: redes siamesas e Triplet Loss	6
2.6.1	Classificação tradicional e aprendizado métrico	6
2.6.2	Redes siamesas	6
2.6.3	Função de perda Triplet Loss	6
2.6.4	Aplicação do aprendizado métrico ao reconhecimento facial	6

2.7	Modelos pré-treinados e reconhecimento facial por embeddings	7
2.7.1	Aprendizado por transferência e modelos pré-treinados	7
2.7.2	Embeddings discriminativos para reconhecimento facial	7
2.7.3	Detecção facial e reconhecimento facial	7
2.8	Avaliação biométrica: FAR, FRR e trade-off entre segurança e usabilidade	7
2.8.1	Matriz de confusão	7
2.8.2	Taxas de erro biométrico: FAR e FRR	7
2.8.3	Definição do limiar de decisão em sistemas reais	7
2.9	Privacidade, LGPD e uso de dados sintéticos	8
2.9.1	Dados biométricos e sua sensibilidade	8
2.9.2	Aspectos gerais da LGPD aplicados à biometria	8
2.9.3	Uso de imagens faciais sintéticas em experimentos	8
2.10	Segurança na comunicação e criptografia aplicada	8
2.10.1	Ameaças em sistemas de comunicação	8
2.10.2	Conceitos fundamentais de criptografia	8
2.10.3	TLS, HTTPS e autenticação mútua	8
3	METODOLOGIA	9
3.1	Construção da base de dados sintética	9
3.2	Modelagem do cadastro de identidades	11
3.3	Extração inicial de características faciais (baseline)	12
3.4	Geração de variações sintéticas das imagens	12
3.5	Extração de embeddings faciais por modelo pré-treinado	14
3.6	Definição da métrica de similaridade	15
3.7	Protocolo experimental de avaliação	16
4	RESULTADOS	18
4.1	Separabilidade no espaço de embeddings	18
4.2	Avaliação biométrica por FAR e FRR	19
4.3	Definição do limiar de decisão (threshold)	21
4.4	Análise qualitativa dos pares de comparação	21
4.5	Avaliação do processo de identificação (1 vs N)	23
5	CONCLUSÃO	25
	REFERÊNCIAS	26

1 INTRODUÇÃO

1.1 Figuras e Tabelas

Nos elementos flutuantes, as legendas devem estar alinhadas à esquerda com o comando **minipage**.

```
\begin{table}[!ht]
\centering
\begin{minipage}{0.7\textwidth}      <<<<<
\caption{\label{tabela:ComparativoFrameworks}}
Comparaçāo dos Frameworks
\resizebox{\textwidth}{!}{

[...]
}
\caption*{\footnotesize Fonte: Elaborado pelo autor, 2023.}
\end{minipage}
\end{table}
```

Tabela 1 – Comparação dos Frameworks

	MapReduce	Spark	Flink
Armazenamento	Disco	RAM	RAM
Granularidade	Grossa	Grossa	Fina
Estado	Sem	Sem	Com
Processamento	Lote	Micro lotes	Stream
Volume	Finito	Finito	Infinito
Linguagem.	Java	Scala	Java

Fonte: Elaborado pelo autor, 2023.

1.2 Citação

1.2.1 Início do texto

Segundo \textcite{gunther2017debating} Dados se tornaram um

ativo de alto valor no atual cenário tecnológico.

Segundo Günther *et al.* (2017) Dados se tornaram um ativo de alto valor no atual cenário tecnológico.

1.3 Alíneas

Para criar alíneas utilize o comando enumerate, nunca description ou itemize. As alínea devem encerrar com um ponto e vírgula e a última deve encerrar com um ponto final.

```
\begin{enumerate}
    \item Primeiro item da alínea;
    \item Segundo item da alínea;
    \item Terceiro item da alínea.

    \begin{enumerate}
        \item Primeiro item da subalínea;
        \item Segundo item da subalínea;
        \item Terceiro item da subalínea.
    \end{enumerate}
\end{enumerate}
```

- a) Primeiro item da alínea;
- b) Segundo item da alínea;
- c) Terceiro item da alínea.
 - Primeiro item da subalínea;
 - Segundo item da subalínea;
 - Terceiro item da subalínea.

1.4 Customização

Esse pacote pode ser customizado passando argumentos da seguinte forma:

```
\usepackage[acronym, glossaries, index, labelref, debug]{CEFET}
```

- a) **acronym**: adiciona o suporte para lista de abreviaturas e siglas;
- b) **glossaries**: adiciona o suporte para glossário;
- c) **index**: adiciona o suporte para índice de assunto;
- d) **labelref**: \ref{fig:1} retorna Figura 1 em vez de 1 para todas as referências;
- e) **debug**: Ativa as réguas e os quadros para melhorar a visualização das medidas.

2 FUNDAMENTAÇÃO TEÓRICA

Texto pequeno de teste.

2.1 Contexto do problema e cenário de aplicação

Texto pequeno de teste.

2.2 RFID, NFC e cartões de identificação

Texto pequeno de teste.

2.2.1 RFID: conceito e funcionamento básico

Texto pequeno de teste.

2.2.2 NFC e sua relação com RFID

Texto pequeno de teste.

2.2.3 Custos e limitações operacionais em ambientes reais

Texto pequeno de teste.

2.2.4 Vulnerabilidades e riscos em sistemas baseados em cartões

Texto pequeno de teste.

2.3 Fundamentos de biometria aplicada ao controle de acesso

Texto pequeno de teste.

2.3.1 Conceito de biometria e principais modalidades

Texto pequeno de teste.

2.3.2 Verificação biométrica (1:1) e identificação biométrica (1:N)

Texto pequeno de teste.

2.3.3 Critérios de qualidade em sistemas biométricos

Texto pequeno de teste.

2.4 Representação e processamento de imagens digitais

Texto pequeno de teste.

2.4.1 Imagem digital: definição e características

Texto pequeno de teste.

2.4.2 Etapas de pré-processamento em imagens faciais

Texto pequeno de teste.

2.5 Representação vetorial e medidas de similaridade

Texto pequeno de teste.

2.5.1 Conceito de vetor e interpretação geométrica

Texto pequeno de teste.

2.5.2 Embeddings como representação de características

Texto pequeno de teste.

2.5.3 Métricas de similaridade e distância

teste

2.5.4 Limiar de decisão em sistemas de reconhecimento

teste

2.6 Aprendizado métrico: redes siamesas e Triplet Loss

teste

2.6.1 Classificação tradicional e aprendizado métrico

teste

2.6.2 Redes siamesas

teste

2.6.3 Função de perda Triplet Loss

teste

2.6.4 Aplicação do aprendizado métrico ao reconhecimento facial

teste

2.7 Modelos pré-treinados e reconhecimento facial por embeddings

teste

2.7.1 Aprendizado por transferência e modelos pré-treinados

teste

2.7.2 Embeddings discriminativos para reconhecimento facial

teste

2.7.3 Detecção facial e reconhecimento facial

teste

2.8 Avaliação biométrica: FAR, FRR e trade-off entre segurança e usabilidade

teste

2.8.1 Matriz de confusão

teste

2.8.2 Taxas de erro biométrico: FAR e FRR

teste

2.8.3 Definição do limiar de decisão em sistemas reais

teste

2.9 Privacidade, LGPD e uso de dados sintéticos

teste

2.9.1 Dados biométricos e sua sensibilidade

teste

2.9.2 Aspectos gerais da LGPD aplicados à biometria

teste

2.9.3 Uso de imagens faciais sintéticas em experimentos

jtujuu teste

2.10 Segurança na comunicação e criptografia aplicada

jhfgjhfj

2.10.1 Ameaças em sistemas de comunicação

hfgh f

2.10.2 Conceitos fundamentais de criptografia

ghfd gf h

2.10.3 TLS, HTTPS e autenticação mútua

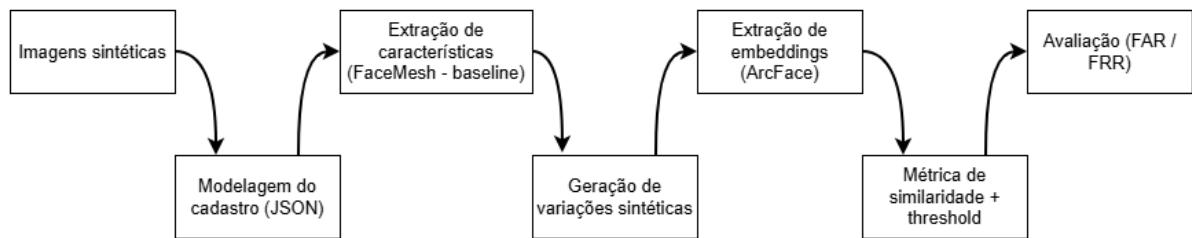
Texto pequeno de teste.

3 METODOLOGIA

Este trabalho adota uma metodologia experimental com o objetivo de avaliar a viabilidade tecnológica do uso de reconhecimento facial como alternativa ao controle de acesso baseado em cartões NFC, no contexto acadêmico do CEFET-MG. A abordagem proposta fundamenta-se no paradigma de aprendizado métrico em espaço de *embeddings*, amplamente discutido na literatura de aprendizado profundo, incluindo estratégias baseadas em redes siamesas e funções de perda do tipo *triplet loss*, conforme apresentado por Andrew Ng (Ng, 2021).

A Figura 1 apresenta uma visão geral do pipeline metodológico adotado neste trabalho, destacando as principais etapas do processo experimental, desde a aquisição das imagens faciais até a avaliação do reconhecimento para fins de controle de acesso.

Figura 1 – Pipeline metodológico adotado.



Fonte: Elaborado pelo autor, 2026.

Nesse contexto, busca-se verificar se *embeddings* faciais extraídos por modelos de reconhecimento permitem a separação adequada entre diferentes identidades por meio de métricas de similaridade, possibilitando decisões confiáveis de autenticação e identificação (Ge *et al.*, 2018). Considerando as restrições éticas e de privacidade associadas ao uso de dados biométricos reais (North-Samardzic, 2020), a metodologia emprega uma base de dados sintética e segue um conjunto estruturado de etapas, descritas a seguir, de forma a garantir reproduzibilidade e clareza na avaliação da abordagem proposta.

3.1 Construção da base de dados sintética

A construção da base de dados utilizada neste estudo teve como objetivo viabilizar a realização de experimentos de reconhecimento facial sem a utilização de dados

biométricos reais, em conformidade com princípios éticos e com a LGPD (Lei nº 13.709/2018) (Presidência da República - Casa Civil, 2018). Para esse fim, foi empregada uma base de imagens faciais sintéticas geradas artificialmente por meio de redes generativas adversariais (GANs), disponibilizadas publicamente pelo projeto *This Person Does Not Exist*, o qual produz imagens fotorrealistas de rostos inexistentes, disponível em (THISPERSONDOESNOTEXIST.COM... s.d.).

Foram coletadas 400 imagens faciais sintéticas, cada uma representando uma identidade distinta. As imagens foram armazenadas em formato digital e organizadas em diretórios específicos do projeto, adotando-se um padrão de nomenclatura que permitisse a associação direta entre cada imagem e seu respectivo identificador de identidade. A utilização de dados sintéticos assegura que não exista qualquer vínculo com indivíduos reais, eliminando riscos de identificação pessoal e atendendo às diretrizes de privacidade estabelecidas pela LGPD (Presidência da República - Casa Civil, 2018).

Com o objetivo de estruturar adequadamente os experimentos, a base de dados foi particionada em dois conjuntos principais: um conjunto de desenvolvimento, composto por 300 identidades, e um conjunto de teste final, composto por 100 identidades distintas. O conjunto de desenvolvimento foi subdividido em três subconjuntos, denominados treino, validação e teste, utilizados exclusivamente para organização experimental, construção da base de referência e calibração de limiares, contendo, respectivamente, 240, 30 e 30 identidades. Embora não haja treinamento ou ajuste dos modelos de reconhecimento, essa subdivisão permite a avaliação controlada do comportamento do sistema e evita vazamento de identidades entre diferentes fases do experimento.

Essa organização possibilita a realização de experimentos de reconhecimento facial de forma reproduzível e controlada, simulando um cenário de cadastramento e validação de usuários em sistemas de controle de acesso. A base de dados sintética construída nesta etapa constitui o insumo fundamental para as etapas subsequentes da metodologia, incluindo a extração de características faciais, a geração de *embeddings* e a avaliação da separabilidade entre identidades no espaço métrico (Ge *et al.*, 2018).

3.2 Modelagem do cadastro de identidades

Após a construção e organização da base de dados sintética, procedeu-se à modelagem do cadastro de identidades a ser utilizado nos experimentos de reconhecimento facial. Essa modelagem teve como objetivo estruturar as informações de cada indivíduo de forma padronizada, facilitando o armazenamento, o processamento e a reproduzibilidade das etapas subsequentes da metodologia.

Cada identidade foi representada por um registro estruturado em formato JSON, contendo os seguintes atributos: um identificador único (*id*), um nome fictício, o nome do arquivo da imagem facial associada e um campo destinado ao armazenamento da representação vetorial da face (*embeddings*), inicialmente não preenchido. Essa estrutura permite a separação clara entre os dados descritivos da identidade e as informações extraídas automaticamente a partir das imagens faciais.

Com o intuito de organizar adequadamente os experimentos e evitar sobreposição de identidades entre diferentes fases de avaliação, o cadastro foi dividido em dois arquivos JSON distintos. O primeiro arquivo corresponde ao conjunto de desenvolvimento, contendo as identidades destinadas às etapas de treino, validação e teste. Nesse arquivo, cada registro inclui um atributo adicional que indica a qual subconjunto a identidade pertence (treino, validação ou teste), respeitando a divisão previamente definida de 240, 30 e 30 identidades, respectivamente.

O segundo arquivo JSON foi destinado exclusivamente ao conjunto de teste final, composto por 100 identidades distintas e não presentes no conjunto de desenvolvimento. Esse conjunto tem como finalidade permitir uma avaliação independente da abordagem proposta, simulando um cenário em que o sistema é exposto a identidades não utilizadas nas fases anteriores do processo experimental.

A adoção de arquivos JSON distintos para o conjunto de desenvolvimento e para o teste final contribui para a organização do fluxo experimental, reduzindo riscos de vazamento de dados entre conjuntos e garantindo maior clareza na definição dos protocolos de avaliação. Além disso, o uso de um formato estruturado e amplamente suportado facilita a integração com os scripts de processamento, extração de *embeddings* e análise de similaridade empregados nas etapas subsequentes da metodologia.

3.3 Extração inicial de características faciais (baseline)

Como etapa inicial do estudo de viabilidade, foi implementada uma abordagem baseada na extração de características geométricas do rosto, utilizando o modelo MediaPipe FaceMesh (Google Developers, 2026), com o objetivo de validar o *pipeline* de processamento e estabelecer uma linha de base (*baseline*) para comparação com abordagens mais avançadas de reconhecimento facial. Essa etapa não tem como finalidade propor uma solução final, mas sim verificar a adequação do uso de representações vetoriais e métricas de similaridade no contexto do problema investigado.

Inicialmente, para cada imagem presente no conjunto de desenvolvimento, realizou-se a detecção automática da face por meio de um detector facial. Em seguida, a região facial detectada foi processada pelo modelo MediaPipe FaceMesh, o qual fornece um conjunto denso de pontos característicos (*landmarks*) distribuídos ao longo da face, cada um associado a coordenadas espaciais tridimensionais (Google Developers, 2026).

As coordenadas (x, y, z) correspondentes a cada *landmark* foram então concatenadas, formando um vetor numérico de dimensão fixa que representa a geometria facial associada à imagem analisada. Esse vetor passou a ser utilizado como uma representação vetorial inicial da face, sendo armazenado no campo de *embedding* do cadastro de identidades em formato JSON.

A comparação entre diferentes faces foi realizada por meio da aplicação de uma métrica de similaridade entre os vetores gerados, permitindo o cálculo de distâncias entre pares de imagens (Ge *et al.*, 2018). Essa abordagem possibilita observar o comportamento das distâncias para identidades iguais e distintas, servindo como referência experimental para a análise posterior de métodos baseados em aprendizado profundo e *embedding* treinados especificamente para reconhecimento facial.

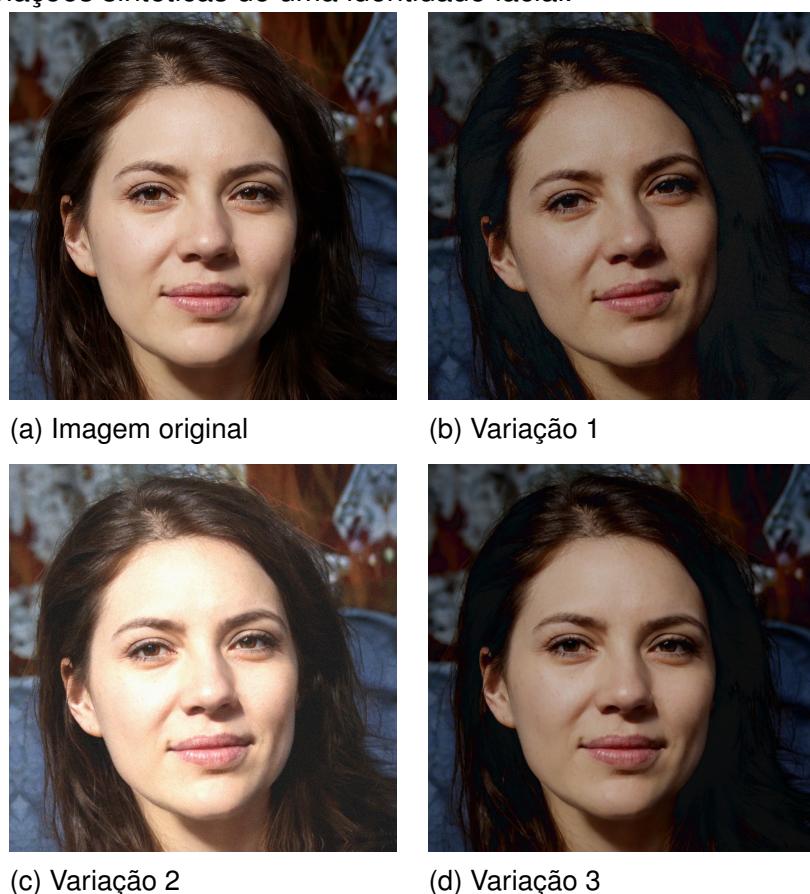
3.4 Geração de variações sintéticas das imagens

Com o objetivo de aumentar a diversidade das amostras disponíveis para cada identidade e simular variações comuns no processo de captura de imagens faciais em ambientes reais, foi realizada a geração de variações sintéticas das imagens originais presentes no conjunto de desenvolvimento. Essa etapa visa tornar o processo de avaliação

mais robusto frente a alterações de condições que podem ocorrer em cenários de controle de acesso, como mudanças de iluminação, pequenas variações de pose e degradações na qualidade da imagem.

Para cada imagem facial original associada a uma identidade, foram aplicadas transformações artificiais controladas, resultando na criação de múltiplas amostras derivadas da mesma identidade. As transformações empregadas incluem operações geométricas, como rotações leves e ajustes de escala, bem como transformações fotométricas, como variações de brilho, contraste e saturação. Adicionalmente, foram aplicadas técnicas de degradação da imagem, incluindo a inserção de ruído e a aplicação de filtros de desfoque, com o objetivo de simular condições adversas de captura. A Figura 2 ilustra um exemplo de imagem facial original e suas respectivas variações sintéticas, evidenciando o efeito das transformações artificiais aplicadas para uma mesma identidade.

Figura 2 – Variações sintéticas de uma identidade facial.



Fonte: Elaborado pelo autor a partir de imagens sintéticas do projeto *This Person Does Not Exist*, 2026

As imagens geradas por meio desse processo foram armazenadas em um diretório específico, mantendo-se a associação com o identificador da identidade original. Para refletir essa ampliação do conjunto de dados, foi criado um novo arquivo JSON contendo múltiplos registros por identidade, cada um referenciando uma variação distinta da imagem facial, preservando-se o mesmo identificador único (id). Dessa forma, todas as variações de uma mesma identidade são tratadas como amostras positivas associadas a um único indivíduo (Ge *et al.*, 2018).

A geração dessas variações sintéticas é particularmente relevante no contexto de abordagens baseadas em aprendizado de representações em espaço métrico, nas quais se busca reduzir a distância entre diferentes amostras da mesma identidade e aumentar a separação em relação a amostras de identidades distintas (Ge *et al.*, 2018). Embora nesta etapa não seja realizado treinamento de redes neurais, o conjunto de imagens gerado fornece subsídios adequados para avaliar o comportamento de *embeddings* faciais frente a variações de uma mesma identidade, conceito central em estratégias inspiradas em funções de perda do tipo *triplet loss* (Kaya; Bilge, 2019).

3.5 Extração de embeddings faciais por modelo pré-treinado

Após a geração das variações sintéticas das imagens faciais, procedeu-se à extração de *embeddings* faciais por meio de um modelo de reconhecimento facial pré-treinado baseado em aprendizado profundo (Abdullah; Stephan, 2021). Essa etapa tem como objetivo representar cada face em um espaço vetorial no qual identidades iguais apresentem maior proximidade entre si, enquanto identidades distintas sejam mapeadas para regiões mais distantes, característica essencial para sistemas de reconhecimento facial baseados em métricas de similaridade (Ge *et al.*, 2018).

Para essa finalidade, foi adotado um modelo amplamente utilizado na literatura e em aplicações práticas de reconhecimento facial, treinado previamente em grandes bases de dados de faces (Schroff; Kalenichenko; Philbin, 2015). O modelo empregado segue a filosofia de aprendizado de representações em espaço métrico, sendo treinado com funções de perda do tipo *margin-based*, conceitualmente relacionadas à *triplet loss*, cujo objetivo é maximizar a separação entre diferentes identidades e reduzir a distância entre amostras da mesma identidade (Ge *et al.*, 2018).

Cada imagem presente no conjunto de dados ampliado foi processada individualmente pelo modelo, sendo inicialmente realizada a detecção da face e, em seguida, a extração do vetor de características correspondente. O *embedding* resultante consiste em um vetor numérico de dimensão fixa, capaz de capturar características discriminativas da face, de forma robusta a variações de iluminação, expressão facial e pequenas alterações de pose (Kaya; Bilge, 2019).

Os *embeddings* extraídos foram associados às respectivas identidades e armazenados no cadastro estruturado em formato JSON, substituindo o campo previamente reservado para a representação vetorial. Esse procedimento permitiu a construção de uma base de dados composta por múltiplas representações vetoriais por identidade, viabilizando a comparação entre amostras da mesma identidade e de identidades distintas nas etapas subsequentes da metodologia.

3.6 Definição da métrica de similaridade

Com os *embeddings* faciais extraídos e associados às respectivas identidades, definiu-se o método para quantificar a similaridade entre diferentes representações vetoriais. Essa etapa é fundamental em sistemas de reconhecimento facial baseados em aprendizado métrico, nos quais a decisão de correspondência entre identidades é realizada a partir da distância entre *embeddings* no espaço vetorial (Schroff; Kalenichenko; Philbin, 2015).

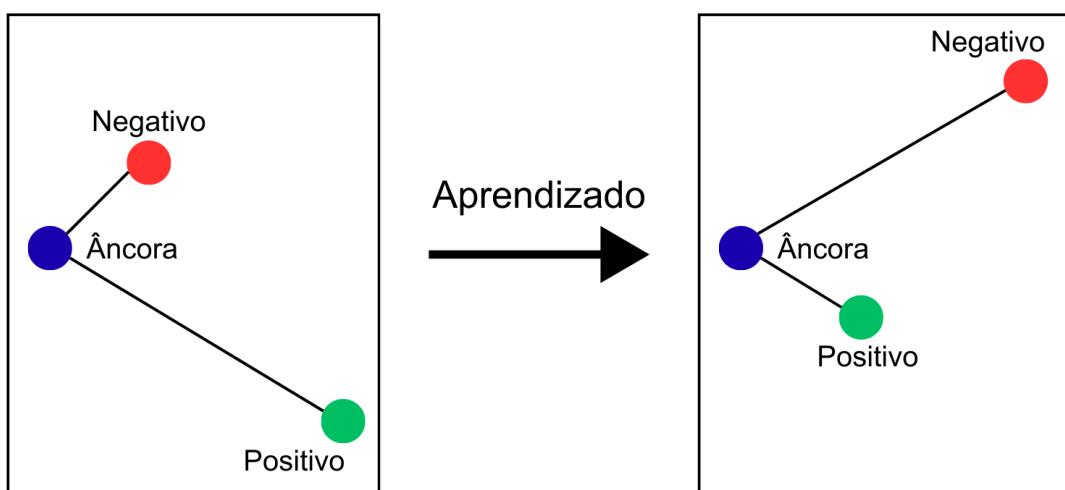
Neste trabalho, foi adotada a métrica de distância cosseno para a comparação entre pares de *embeddings* faciais. Essa métrica avalia o ângulo entre dois vetores, sendo amplamente utilizada em aplicações de reconhecimento facial por apresentar bom desempenho na comparação de vetores normalizados e por ser menos sensível à magnitude absoluta dos *embeddings* (Schroff; Kalenichenko; Philbin, 2015). A distância cosseno permite, assim, mensurar o grau de similaridade entre duas amostras faciais de forma consistente.

A partir da métrica de similaridade definida, estabeleceu-se um limiar de decisão (*threshold*) para determinar se dois *embeddings* correspondem à mesma identidade ou a identidades distintas (Schroff; Kalenichenko; Philbin, 2015). Distâncias inferiores ao limiar são interpretadas como correspondências positivas, enquanto distâncias superiores

indicam não correspondência. A definição desse limiar é tratada como um parâmetro experimental, cuja adequação é avaliada por meio de análises quantitativas descritas nas etapas subsequentes da metodologia.

Esse procedimento reflete diretamente o princípio das abordagens inspiradas em redes siamesas e funções de perda do tipo *triplet loss*, nas quais o aprendizado visa estruturar o espaço de *embeddings* de modo que amostras da mesma identidade apresentem distâncias reduzidas, enquanto amostras de identidades diferentes sejam separadas por distâncias maiores, possibilitando decisões baseadas em métricas de similaridade (Ge *et al.*, 2018). A Figura 3 ilustra, de forma conceitual, a organização do espaço de *embeddings* em abordagens baseadas em aprendizado métrico.

Figura 3 – Espaço de *embeddings* antes e após o aprendizado.



Fonte: Elaborado pelo autor, 2026.

3.7 Protocolo experimental de avaliação

O protocolo experimental adotado neste trabalho tem como finalidade avaliar o comportamento das representações faciais no espaço de *embeddings* e verificar a capacidade da abordagem proposta em distinguir identidades distintas por meio de métricas de similaridade (Schroff; Kalenichenko; Philbin, 2015). Para isso, foram definidas estratégias de comparação entre amostras faciais, bem como métricas quantitativas para

análise do desempenho do sistema, sem a realização de ajustes ou treinamentos adicionais dos modelos empregados.

As comparações foram organizadas a partir da definição de dois tipos de pares. Os pares genuínos correspondem a comparações entre amostras pertencentes à mesma identidade, incluindo imagens originais e variações sintéticas associadas a um mesmo identificador. Já os pares impostores correspondem a comparações entre amostras de identidades distintas. Essa distinção permite analisar o comportamento das distâncias de similaridade tanto em situações de correspondência legítima quanto em tentativas de correspondência indevida.

Para cada par de amostras, foi calculada a distância entre os *embeddings* faciais utilizando a métrica definida na etapa anterior. A partir dessas distâncias, avaliou-se o impacto de diferentes valores do limiar de decisão (*threshold*) na classificação das comparações como correspondências positivas ou negativas. Esse procedimento possibilita observar como variações no limiar influenciam o comportamento do sistema frente a pares genuínos e impostores (Jain; Ross; Prabhakar, 2004).

Como métricas de avaliação, foram consideradas a taxa de falsa aceitação (*False Acceptance Rate* - FAR) e a taxa de falsa rejeição (*False Rejection Rate* - FRR). Essas métricas são amplamente utilizadas em sistemas biométricos e permitem caracterizar o compromisso entre segurança e usabilidade, aspecto fundamental em aplicações de controle de acesso (Jain; Ross; Prabhakar, 2004). A análise conjunta dessas métricas fornece subsídios para a avaliação da separabilidade das identidades no espaço de *embeddings* e para a definição de critérios de viabilidade da abordagem estudada.

Esse protocolo experimental foi aplicado tanto à abordagem inicial baseada em características geométricas quanto à abordagem baseada em *embeddings* extraídos por modelo pré-treinado, permitindo uma avaliação consistente do comportamento das diferentes representações faciais consideradas neste estudo.

4 RESULTADOS

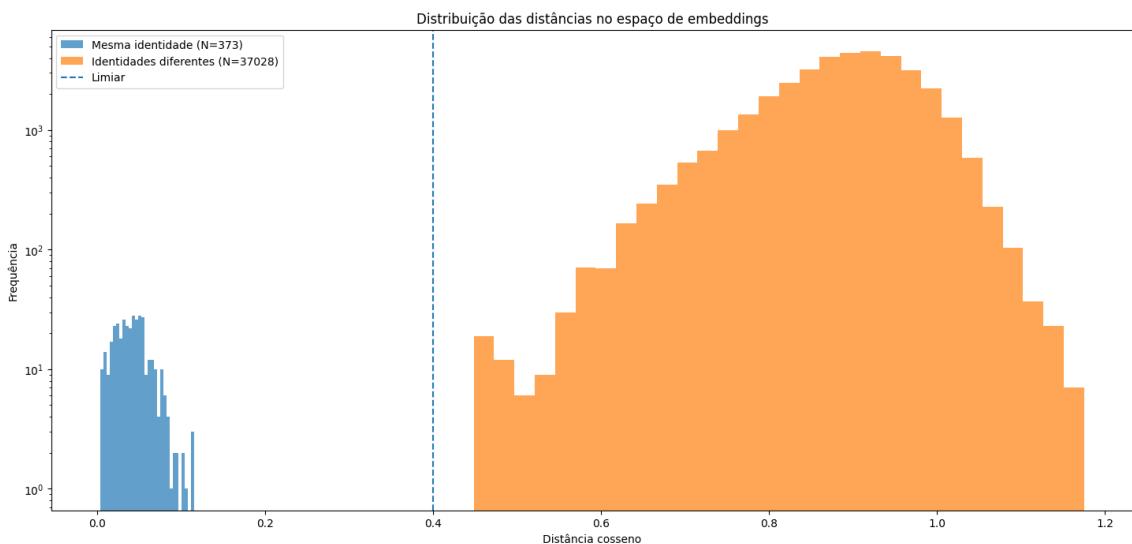
Este capítulo apresenta os resultados obtidos a partir dos experimentos realizados com a base de dados sintética e os modelos de reconhecimento facial descritos na metodologia. Os resultados concentram-se na análise da separabilidade das representações faciais no espaço de *embeddings*, na avaliação do desempenho biométrico por meio das métricas de falsa aceitação e falsa rejeição, e na validação do processo de identificação baseado em similaridade, considerando diferentes valores de limiar de decisão. O objetivo é verificar, de forma objetiva, a viabilidade do uso do reconhecimento facial como alternativa ao controle de acesso baseado em cartões NFC no contexto acadêmico.

4.1 Separabilidade no espaço de embeddings

Esta seção analisa a separabilidade das representações faciais no espaço de embeddings a partir da distribuição das distâncias cosseno calculadas entre pares de imagens. O objetivo é verificar se amostras da mesma identidade apresentam maior similaridade entre si do que amostras pertencentes a identidades distintas.

Para isso, todas as combinações possíveis de pares foram comparadas e classificadas em dois grupos: pares da mesma identidade, formados por imagens diferentes associadas ao mesmo identificador, e pares de identidades diferentes, formados por imagens pertencentes a indivíduos distintos. No experimento realizado, foram obtidos 373 pares da mesma identidade e 37.028 pares de identidades diferentes. Essa diferença numérica é esperada, uma vez que o número de pares impostores cresce de forma combinatória quando se consideram todas as combinações entre identidades distintas, enquanto os pares genuínos dependem apenas do número de variações disponíveis por identidade.

Figura 4 – Distribuição das distâncias cosseno no espaço de embeddings



Fonte: Elaborado pelo autor, 2026.

A Figura 4 apresenta a distribuição das distâncias cosseno para ambos os grupos. Observa-se que os pares da mesma identidade concentram-se em valores menores de distância, enquanto os pares de identidades diferentes apresentam distâncias predominantemente maiores, indicando separação entre os grupos no espaço de embeddings. O limiar de referência de 0,4 é exibido apenas como apoio visual, ilustrando a região em que ocorreria a decisão de correspondência, sem ser utilizado nesta etapa para classificação.

De forma geral, os resultados indicam que o espaço de embeddings apresenta separabilidade adequada entre identidades, constituindo a base para as análises quantitativas de desempenho apresentadas a seguir.

4.2 Avaliação biométrica por FAR e FRR

Nesta seção é avaliado o desempenho do sistema de reconhecimento facial por meio das métricas biométricas de falsa aceitação (FAR) e falsa rejeição (FRR), calculadas a partir das distâncias cosseno entre pares de embeddings para diferentes valores de limiar de decisão (threshold). O objetivo é analisar como a escolha do limiar influencia o comportamento do sistema em termos de segurança e confiabilidade.

Para essa avaliação, foram considerados 37.401 pares de comparação, obtidos a

partir de 274 amostras faciais com embeddings válidos. Cada par foi classificado de acordo com sua identidade real (mesma identidade ou identidades distintas) e comparado com base na distância cosseno. A decisão de correspondência foi tomada comparando-se essa distância com um valor de threshold, sendo considerada uma correspondência positiva quando a distância é inferior ao limiar.

Tabela 2 – Resultados de desempenho para diferentes valores de *threshold*, incluindo TP, FP, TN, FN, FAR e FRR

Threshold	TP	FP	TN	FN	FAR (%)	FRR (%)
0,20	373	0	37028	0	0,000	0,000
0,30	373	0	37028	0	0,000	0,000
0,35	373	0	37028	0	0,000	0,000
0,40	373	0	37028	0	0,000	0,000
0,45	373	2	37026	0	0,005	0,000
0,50	373	32	36996	0	0,086	0,000

Fonte: Elaborado pelo autor (2026).

Os resultados são organizados em termos de quatro categorias: verdadeiros positivos (TP), correspondentes a pares da mesma identidade corretamente aceitos; falsos negativos (FN), pares da mesma identidade incorretamente rejeitados; falsos positivos (FP), pares de identidades diferentes incorretamente aceitos; e verdadeiros negativos (TN), pares de identidades diferentes corretamente rejeitados. A partir dessas quantidades, são calculadas as métricas FAR, definida como a proporção de falsos positivos em relação ao total de pares impostores, e FRR, definida como a proporção de falsos negativos em relação ao total de pares genuínos.

A Tabela 2 apresenta os resultados obtidos para diferentes valores de threshold. Observa-se que, para limiares entre 0,20 e 0,40, o sistema apresentou FAR e FRR iguais a zero, indicando ausência de erros tanto de aceitação indevida quanto de rejeição indevida nesse intervalo. A partir do limiar 0,45, passam a ocorrer falsas aceitações, refletidas no aumento gradual da FAR, enquanto a FRR permanece nula em todos os valores avaliados, indicando que nenhuma comparação genuína foi rejeitada.

Esses resultados evidenciam que o sistema apresenta alta separabilidade entre identidades, permitindo a definição de um limiar de decisão que elimina erros de falsa

rejeição e mantém taxas de falsa aceitação extremamente baixas. Essa análise quantitativa fornece subsídios diretos para a escolha do threshold mais adequado, discutida na seção subsequente.

4.3 Definição do limiar de decisão (threshold)

Com base nos resultados apresentados na seção anterior, definiu-se o limiar de decisão (*threshold*) a ser adotado no sistema de reconhecimento facial. A escolha do limiar tem como objetivo equilibrar segurança e confiabilidade, priorizando a redução de falsas aceitações, aspecto crítico em aplicações de controle de acesso.

A análise dos valores avaliados mostrou que, para *thresholds* entre 0,20 e 0,40, o sistema apresentou taxas nulas de falsa aceitação (FAR) e falsa rejeição (FRR). A partir do valor 0,45, passaram a ocorrer falsas aceitações, ainda que em baixa proporção, indicando perda gradual de segurança conforme o limiar é relaxado. Em todos os casos analisados, a FRR permaneceu nula, evidenciando a ausência de rejeições indevidas de pares genuínos.

Diante desses resultados, foi adotado o valor 0,40 como limiar de decisão, por representar o maior valor testado que mantém FAR e FRR iguais a zero, oferecendo maior margem de segurança em relação a valores mais permissivos. Esse limiar foi utilizado nas etapas subsequentes de validação e identificação, servindo como critério para aceitação ou rejeição de correspondências faciais no sistema proposto.

4.4 Análise qualitativa dos pares de comparação

Esta seção apresenta uma análise qualitativa dos resultados obtidos, com o objetivo de complementar as métricas quantitativas discutidas anteriormente por meio da inspeção visual de pares de imagens faciais. Essa análise busca verificar se o comportamento observado nas distâncias entre embeddings é consistente com a percepção visual das imagens comparadas, contribuindo para a validação empírica do sistema.

Foram selecionados exemplos representativos de pares da mesma identidade e de pares de identidades diferentes, considerando o limiar de decisão definido na seção anterior (distância cosseno inferior a 0,40 para correspondência positiva). Nos pares da mesma identidade, são comparadas imagens distintas associadas a um mesmo

identificador, incluindo variações sintéticas decorrentes de transformações aplicadas às imagens originais. Nos pares de identidades diferentes, são comparadas imagens pertencentes a indivíduos distintos corretamente rejeitados pelo sistema.

Figura 5 – Exemplo de par da mesma identidade corretamente aceitos

MESMA PESSOA | Distância: 0.0458



Fonte: Elaborado pelo autor, 2026.

Figura 6 – Exemplo de par de identidades diferentes corretamente rejeitados

PESSOAS DIFERENTES | Distância: 0.8941



Fonte: Elaborado pelo autor, 2026.

As figuras apresentadas evidenciam que, nos casos classificados como pertencentes à mesma identidade, as imagens compartilham características faciais

visuais compatíveis, mesmo diante de variações de iluminação, ruído ou pequenas alterações de aparência introduzidas artificialmente. Por outro lado, nos pares de identidades diferentes, observa-se divergência visual clara entre os rostos comparados, coerente com as maiores distâncias no espaço de embeddings e com a decisão de não correspondência adotada pelo sistema.

De forma geral, a análise qualitativa confirma que as decisões baseadas em similaridade no espaço de embeddings refletem adequadamente as diferenças e semelhanças perceptíveis entre as imagens faciais, reforçando a confiabilidade dos resultados quantitativos apresentados nas seções anteriores.

4.5 Avaliação do processo de identificação (1 vs N)

Nesta seção é avaliado o funcionamento do processo de identificação facial no cenário 1 vs N, no qual uma imagem de consulta é comparada com todas as representações faciais armazenadas na base de dados, com o objetivo de determinar a identidade mais semelhante. Essa avaliação tem caráter funcional e demonstra a aplicação prática do critério de similaridade definido nas seções anteriores.

Para o teste realizado, foram consideradas 300 identidades com *embeddings* válidos no conjunto de referência. Uma identidade foi selecionada como consulta, e seu embedding foi comparado com os *embeddings* das demais identidades por meio da distância cosseno. O processo de identificação consistiu em selecionar a identidade que apresentou a menor distância em relação à consulta, caracterizando o candidato mais próximo no espaço de *embeddings*.

Como resultado, a identidade consultada foi associada à identidade mais próxima na base, apresentando uma distância cosseno de 0,0002, valor significativamente inferior ao limiar de decisão adotado. Com base nesse critério, a identidade foi corretamente confirmada pelo sistema, evidenciando que o método de identificação por similaridade é capaz de localizar a representação mais próxima de forma consistente no conjunto avaliado.

Esse experimento demonstra, de forma objetiva, a viabilidade do uso de *embeddings* faciais e métricas de similaridade para identificação automática em um cenário compatível com aplicações de controle de acesso. Embora não constitua uma

avaliação estatística completa de desempenho, essa validação funcional complementa os resultados quantitativos apresentados anteriormente, ilustrando o comportamento do sistema em uma situação de uso realista.

5 CONCLUSÃO

The typesetting markup language is specially suitable for documents that include

REFERÊNCIAS

- ABDULLAH, Ihab Amer; STEPHAN, Jane Jaleel. Face Recognition Using Face Embedding Method. **Turkish Journal of Computer and Mathematics Education**, v. 12, n. 10, p. 3383–3394, 2021.
- GE, Weifeng *et al.* Deep Metric Learning with Hierarchical Triplet Loss. *In:* PROCEEDINGS of the European Conference on Computer Vision (ECCV). [S. l.]: Springer, 2018.
- GOOGLE DEVELOPERS. **ML Kit Vision – Detecção de Face Mesh**. [S. l.: s. n.], 2026. <https://developers.google.com/ml-kit/vision/face-mesh-detection?hl=pt-br>. acesso em: 31 jan. 2026.
- GÜNTHER, Wendy Arianne *et al.* Debating big data: A literature review on realizing value from big data. **The Journal of Strategic Information Systems**, Elsevier, v. 26, n. 3, p. 191–209, 2017.
- JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil. An Introduction to Biometric Recognition. **IEEE Transactions on Circuits and Systems for Video Technology**, IEEE, v. 14, n. 1, p. 4–20, 2004.
- KAYA, Mahmut; BILGE, Hasan Sakir. Deep Metric Learning: A Survey. **Symmetry**, MDPI, v. 11, n. 9, p. 1066, 2019. DOI: 10.3390/sym11091066.
- NG, Andrew. **Deep Learning Specialization**. [S. l.: s. n.], 2021. <https://www.coursera.org/specializations/deep-learning>. Curso online.
- NORTH-SAMARDZIC, Anna. Biometric Technology and Ethics: Beyond Security Applications. **Journal of Business Ethics**, Springer, v. 167, n. 3, p. 433–450, 2020. DOI: 10.1007/s10551-019-04143-6.
- PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL. **Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018**. [S. l.: s. n.], 2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, acesso em: 30 jan. 2026. Brasil.
- SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. FaceNet: A Unified Embedding for Face Recognition and Clustering. *In:* PROCEEDINGS of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). [S. l.: s. n.], 2015. p. 815–823.

THISPERSONDOESNOTEXIST.COM – AI GENERATED HUMAN FACES. [S. I.: s. n.]. <http://thispersondoesnotexist.com/>. Gerador de faces humanas sintéticas com redes neurais (acesso em: 30 jan. 2026).