

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 5 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.

0.1 *

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 aporte 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 – Modos de operação do NFC	7
Figura 2 – Similaridade entre dois vetores com base no modelo de espaço vetorial.	13
Figura 3 – Espaço de <i>embeddings</i> antes e após o aprendizado.	18
Figura 4 – Pipeline típico de reconhecimento facial	21
Figura 5 – Pipeline metodológico adotado.	28
Figura 6 – Variações sintéticas de uma identidade facial.	32
Figura 7 – Distribuição das distâncias cosseno no espaço de <i>embeddings</i>	38
Figura 8 – Exemplo de par da mesma identidade corretamente aceitos	41
Figura 9 – Exemplo de par de identidades diferentes corretamente rejeitados	41

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	39

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados Pessoais
NFC	Comunicação por Campo de Proximidade, do inglês Near Field Communication
RFID	Identificação por Rádio Frequência, do inglês Radio Frequency Identification
UID	Identificador Único, do inglês Unique Identifier
RGB	Modelo de Cores Vermelho, Verde e Azul, do inglês Red Green Blue
TLS	Segurança de Camada de Transporte, do inglês Transport Layer Security
HTTPS	Protocolo Seguro de Transferência de Hipertexto, do inglês HyperText Transfer Protocol Secure
mTLS	Mutual Transport Layer Security, do inglês Segurança de Camada de Transporte Mútua
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

0.1	*	2
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	5
2.2.1	RFID: conceito e funcionamento básico	5
2.2.2	NFC e sua relação com RFID	6
2.2.3	Custos e limitações operacionais em ambientes reais	7
2.2.4	Vulnerabilidades e riscos em sistemas baseados em cartões	8
2.3	Fundamentos de biometria aplicada ao controle de acesso	8
2.3.1	Conceito de biometria e principais modalidades	9
2.3.2	Verificação biométrica (1:1) e identificação biométrica (1:N)	9
2.3.3	Critérios de qualidade em sistemas biométricos	10
2.4	Representação e processamento de imagens digitais	10
2.4.1	Imagem digital: definição e características	11
2.4.2	Etapas de pré-processamento em imagens faciais	11
2.5	Representação vetorial e medidas de similaridade	12
2.5.1	Conceito de vetor e interpretação geométrica	12
2.5.2	Embeddings como representação de características	13
2.5.3	Métricas de similaridade e distância	14
2.5.4	Limiar de decisão em sistemas de reconhecimento	15
2.6	Aprendizado métrico: redes siamesas e Triplet Loss	15
2.6.1	Classificação tradicional e aprendizado métrico	16
2.6.2	Redes siamesas	16
2.6.3	Função de perda Triplet Loss	17

2.6.4	Aplicação do aprendizado métrico ao reconhecimento facial	18
2.7	Modelos pré-treinados e reconhecimento facial por embeddings	19
2.7.1	Aprendizado por transferência e modelos pré-treinados	19
2.7.2	Embeddings discriminativos para reconhecimento facial	19
2.7.3	Detecção facial e reconhecimento facial	20
2.8	Avaliação biométrica: FAR, FRR e trade-off entre segurança e usabilidade	21
2.8.1	Matriz de confusão	21
2.8.2	Taxas de erro biométrico: FAR e FRR	22
2.8.3	Definição do limiar de decisão em sistemas reais	23
2.9	Privacidade, LGPD e uso de dados sintéticos	23
2.9.1	Dados biométricos e sua sensibilidade	23
2.9.2	Aspectos gerais da LGPD aplicados à biometria	24
2.9.3	Uso de imagens faciais sintéticas em experimentos	24
2.10	Segurança na comunicação e criptografia aplicada	25
2.10.1	Ameaças em sistemas de comunicação	25
2.10.2	Conceitos fundamentais de criptografia	26
2.10.3	TLS, HTTPS e autenticação mútua	26
3	METODOLOGIA	28
3.1	Construção da base de dados sintética	28
3.2	Modelagem do cadastro de identidades	30
3.3	Extração inicial de características faciais (baseline)	31
3.4	Geração de variações sintéticas das imagens	31
3.5	Extração de embeddings faciais por modelo pré-treinado	33
3.6	Definição da métrica de similaridade	34
3.7	Protocolo experimental de avaliação	35
4	RESULTADOS	37
4.1	Separabilidade no espaço de embeddings	37
4.2	Avaliação biométrica por FAR e FRR	38
4.3	Definição do limiar de decisão (threshold)	40
4.4	Análise qualitativa dos pares de comparação	40
4.5	Avaliação do processo de identificação (1 vs N)	42
5	CONCLUSÃO	44

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

Antes de abordar as técnicas biométricas e os métodos computacionais empregados neste trabalho, é importante compreender a tecnologia atualmente utilizada como base para o controle de acesso em muitos ambientes institucionais. O uso de cartões de identificação baseados em radiofrequência constitui o cenário de referência a partir do qual se discute a motivação para alternativas biométricas. Assim, as subseções a seguir apresentam os conceitos fundamentais de RFID e NFC, seu funcionamento básico, bem como limitações e vulnerabilidades associadas ao seu uso em sistemas de autenticação e controle de acesso.

2.1 Contexto do problema e cenário de aplicação

Sistemas de controle de acesso são amplamente utilizados em ambientes acadêmicos para organizar e restringir o uso de espaços e serviços institucionais, como laboratórios, bibliotecas e restaurantes universitários. Nessas aplicações, o objetivo principal é garantir que apenas usuários autorizados tenham acesso a determinados recursos, mantendo ao mesmo tempo um fluxo de entrada rápido e compatível com a rotina de grande circulação de pessoas.

Em muitos desses cenários, o controle de acesso é realizado por meio de cartões de proximidade, como cartões baseados em NFC. Essa abordagem é amplamente adotada por sua simplicidade operacional e facilidade de integração com sistemas computacionais. No entanto, o mecanismo de autenticação baseado em cartões está associado à verificação da posse de um objeto físico, e não diretamente à identidade do usuário, o que pode abrir espaço para usos indevidos, como empréstimos, perdas ou extravios do cartão (Masyuk, 2019).

Como alternativa, sistemas biométricos buscam associar o processo de autenticação a características inerentes ao próprio indivíduo. Entre as diferentes modalidades biométricas, o reconhecimento facial destaca-se por permitir a autenticação sem contato físico e por utilizar dispositivos de captura amplamente disponíveis, como câmeras. Em sistemas desse tipo, a decisão de acesso é tomada com base na comparação entre representações faciais extraídas de imagens e armazenadas

previamente, permitindo tanto cenários de verificação quanto de identificação automática (Parmar; Mehta, 2013).

Apesar de seu potencial, o reconhecimento facial impõe desafios técnicos relevantes, especialmente no que se refere à confiabilidade das comparações em condições variadas de captura e à definição de critérios objetivos para decisão de correspondência entre identidades. Dessa forma, torna-se necessário compreender os fundamentos que permitem representar faces de forma vetorial, comparar essas representações por métricas de similaridade e estabelecer limiares de decisão adequados, aspectos que são discutidos nas seções subsequentes desta fundamentação teórica (Hassaballah; Aly, 2015).

2.2 RFID, NFC e cartões de identificação

O uso de cartões de identificação baseados em tecnologias de radiofrequência é uma solução amplamente adotada em sistemas de controle de acesso por combinar simplicidade operacional e rápida autenticação. Para compreender as motivações que levam à investigação de alternativas biométricas, é necessário apresentar os conceitos fundamentais dessas tecnologias, seu funcionamento básico e as limitações inerentes ao seu uso em ambientes reais (Masyuk, 2019). As subseções a seguir descrevem o funcionamento do RFID e do NFC, bem como aspectos práticos relacionados a custos, operação e segurança.

2.2.1 RFID: conceito e funcionamento básico

RFID (*Radio-Frequency Identification*) é uma tecnologia que permite a identificação automática de objetos ou pessoas por meio da comunicação sem fio entre um leitor e uma etiqueta eletrônica, denominada *tag*. Essa comunicação ocorre por radiofrequência e dispensa contato físico direto entre o cartão e o leitor, o que torna o processo rápido e conveniente (Chatmon; Le; Burmester, 2006).

Uma *tag* RFID é composta, de forma simplificada, por um chip eletrônico e uma antena. O chip armazena um identificador único (UID), enquanto a antena permite a comunicação com o leitor. O leitor, por sua vez, emite um campo eletromagnético que

energiza a *tag* (no caso de etiquetas passivas) e recebe as informações transmitidas por ela. Em sistemas com múltiplas *tags* presentes simultaneamente, são utilizados mecanismos de *anticollision* para evitar conflitos na comunicação e permitir a leitura individual de cada identificador (Equipe TOTVS, 2022).

O alcance da comunicação RFID depende do tipo de *tag* e da frequência utilizada, podendo variar de poucos centímetros a vários metros. Em sistemas de controle de acesso, utiliza-se geralmente um alcance reduzido, adequado para identificar um único cartão por vez, associado a uma pessoa específica (Equipe TOTVS, 2022).

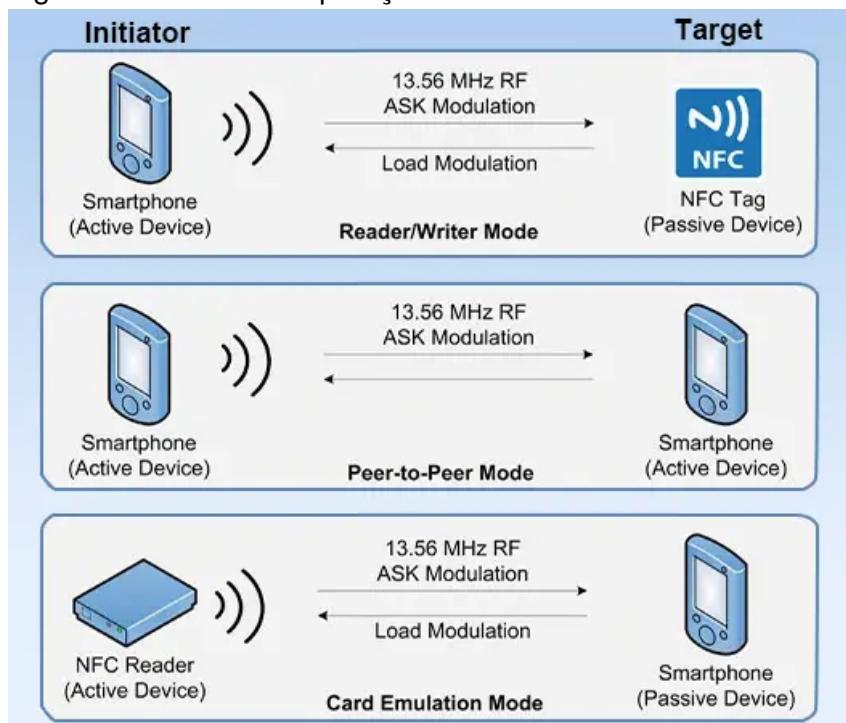
2.2.2 NFC e sua relação com RFID

NFC (*Near Field Communication*) é uma tecnologia derivada do RFID que opera em curto alcance, tipicamente limitado a alguns centímetros. Pode ser compreendida como um subconjunto do RFID, projetado especificamente para aplicações que exigem maior controle da proximidade entre o leitor e o dispositivo identificado (Masyuk, 2019).

Na prática, o NFC é amplamente utilizado em aplicações do cotidiano, como pagamentos por aproximação, cartões de transporte público e crachás de identificação. Em sistemas de controle de acesso, o uso de NFC reduz leituras acidentais e aumenta a previsibilidade da interação, uma vez que exige que o cartão seja deliberadamente aproximado do leitor (Masyuk, 2019).

Embora ofereça vantagens em termos de usabilidade e controle de alcance, o NFC mantém o mesmo princípio fundamental do RFID: a autenticação baseia-se na leitura de um identificador armazenado no cartão, que é utilizado como chave para permitir ou negar o acesso (Masyuk, 2019).

Figura 1 – Modos de operação do NFC



Fonte: (RFID Silicone, 2024)

2.2.3 Custos e limitações operacionais em ambientes reais

Em ambientes institucionais de grande porte, o uso de cartões RFID ou NFC implica custos recorrentes e desafios operacionais. A emissão inicial dos cartões, sua reposição em casos de perda ou dano, e a necessidade de manutenção do parque de leitores representam despesas contínuas para a instituição. Além disso, processos administrativos são necessários para gerenciar cadastros, bloqueios e reemissões.

Do ponto de vista operacional, cartões físicos estão sujeitos a desgaste, esquecimento e extravio. Em cenários de uso intenso, como restaurantes universitários ou portarias em horários de pico, esses fatores podem causar atrasos, interrupções no fluxo de acesso e aumento da demanda por suporte técnico ou administrativo.

Essas limitações motivam a busca por soluções que reduzam a dependência de objetos físicos, simplifiquem o processo de autenticação e diminuam custos indiretos associados à gestão dos cartões.

2.2.4 Vulnerabilidades e riscos em sistemas baseados em cartões

Além das limitações operacionais, sistemas baseados em cartões apresentam vulnerabilidades do ponto de vista da segurança. Como o mecanismo de autenticação se baseia na posse do cartão, situações como empréstimo deliberado, uso indevido após perda ou roubo e compartilhamento não autorizado tornam-se possíveis. Nesses casos, o sistema não é capaz de distinguir o titular legítimo de outra pessoa portando o cartão (Masyuk, 2019).

Existem ainda riscos técnicos associados à cópia do identificador do cartão. Em termos simples, isso significa que o código armazenado na *tag* pode ser lido e replicado em outro dispositivo, permitindo a criação de um cartão clonado. Esse tipo de ataque explora o fato de que o sistema confia exclusivamente no identificador transmitido, sem verificar características adicionais do usuário (Masyuk, 2019).

Esses aspectos evidenciam uma limitação fundamental desse modelo de autenticação: o cartão comprova apenas a posse de um objeto, e não a identidade da pessoa que o utiliza (Masyuk, 2019). Essa distinção é central para a motivação deste trabalho, uma vez que sistemas biométricos buscam verificar diretamente a identidade do indivíduo, reduzindo riscos associados à perda, empréstimo ou clonagem de credenciais físicas (Parmar; Mehta, 2013).

2.3 Fundamentos de biometria aplicada ao controle de acesso

A biometria refere-se ao conjunto de técnicas que utilizam características físicas ou comportamentais de um indivíduo para realizar processos de autenticação ou identificação. Em sistemas de controle de acesso, a biometria busca associar o uso de um serviço ou espaço à própria pessoa, e não apenas à posse de um objeto ou credencial. Essa abordagem é particularmente relevante em cenários nos quais se deseja reduzir fraudes, compartilhamento indevido de credenciais e outras formas de uso não autorizado (Bolle *et al.*, 2013).

2.3.1 Conceito de biometria e principais modalidades

Sistemas biométricos baseiam-se na medição e análise de características inerentes aos indivíduos, que apresentam, em geral, elevado grau de distinção entre pessoas. Entre as modalidades mais conhecidas estão a biometria facial, a biometria por impressão digital e a biometria por íris. Cada uma dessas técnicas explora diferentes tipos de informações fisiológicas, como a geometria do rosto, os padrões das digitais ou as texturas da íris (Bolle *et al.*, 2013).

Do ponto de vista prático, a escolha da modalidade biométrica envolve compromissos entre fatores como facilidade de captura, custo dos sensores, aceitação pelos usuários e robustez frente a tentativas de fraude. No contexto deste trabalho, o foco recai sobre a biometria facial, por permitir a aquisição das amostras por meio de câmeras comuns e por ser compatível com cenários de uso rápido e sem contato físico (Jain; Ross; Prabhakar, 2004).

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

Em sistemas biométricos, é fundamental distinguir entre dois modos de operação: verificação e identificação. A verificação, também conhecida como comparação 1:1, ocorre quando o sistema recebe uma amostra biométrica e a compara com uma única referência previamente associada a um usuário específico. Nesse caso, a pergunta que o sistema busca responder é: “essa pessoa é quem ela afirma ser?”. Esse modo de operação é típico de cenários de autenticação, nos quais o usuário declara sua identidade e o sistema apenas confirma ou rejeita essa afirmação (Jain; Ross; Prabhakar, 2004).

A identificação, por sua vez, corresponde à comparação 1:N, em que a amostra biométrica é comparada com todas as referências disponíveis em uma base de dados. Nesse caso, o objetivo é responder à pergunta: “quem é essa pessoa dentre os usuários cadastrados?”. Esse modo de operação é comum em sistemas nos quais o usuário não informa previamente sua identidade, e o sistema precisa determinar automaticamente a correspondência mais provável. Essa distinção é diretamente relacionada aos experimentos deste trabalho, que incluem tanto análises de comparação entre pares quanto um teste funcional de identificação no cenário 1 vs N (Jain; Ross; Prabhakar,

2004).

2.3.3 Critérios de qualidade em sistemas biométricos

A avaliação de sistemas biométricos envolve, em geral, um compromisso entre dois aspectos principais: segurança e usabilidade. Do ponto de vista da segurança, deseja-se minimizar a probabilidade de que um indivíduo não autorizado seja aceito pelo sistema. Do ponto de vista da usabilidade, busca-se reduzir a ocorrência de rejeições indevidas de usuários legítimos, que podem causar frustração, atrasos e problemas operacionais (Jain; Ross; Prabhakar, 2004).

Esse compromisso é normalmente analisado por meio de métricas específicas, como a FAR (*False Acceptance Rate*) e a FRR (*False Rejection Rate*), que quantificam, respectivamente, a taxa de aceitações indevidas e a taxa de rejeições indevidas. A escolha de parâmetros de decisão em um sistema biométrico, como o limiar de aceitação em comparações por similaridade, influencia diretamente essas métricas, tornando necessário um equilíbrio entre maior rigor de segurança e maior conveniência para o usuário (Jain; Ross; Prabhakar, 2004).

2.4 Representação e processamento de imagens digitais

Para que sistemas computacionais possam analisar imagens faciais de forma automática, é necessário que essas imagens sejam representadas em um formato numérico adequado ao processamento. Diferentemente da percepção humana, que interpreta imagens de maneira visual e subjetiva, o computador opera sobre dados estruturados, o que exige que cada imagem seja convertida em valores numéricos organizados de forma padronizada (Marques Filho; Vieira Neto, 1999). Compreender essa representação é fundamental para entender as etapas de processamento que antecedem a extração de características e a comparação entre faces.

2.4.1 Imagem digital: definição e características

Uma imagem digital pode ser compreendida como uma matriz de valores numéricos, na qual cada posição corresponde a um elemento chamado pixel. Cada pixel armazena informações sobre a cor e a intensidade luminosa em um ponto específico da imagem. Em imagens coloridas, é comum utilizar o modelo RGB, no qual cada pixel é representado por três componentes: vermelho (*red*), verde (*green*) e azul (*blue*). A combinação desses três valores determina a cor final exibida em cada ponto da imagem (Gonzalez; Woods, 2018).

A resolução de uma imagem está relacionada ao número de pixels que a compõem, geralmente expressa em termos de largura e altura. Imagens com maior resolução possuem mais detalhes, mas também exigem maior capacidade de armazenamento e processamento. Além disso, os valores dos pixels podem ser normalizados, isto é, ajustados para uma faixa numérica padronizada, de modo a facilitar o processamento por algoritmos e modelos computacionais que operam de forma mais estável quando os dados seguem escalas bem definidas (Gonzalez; Woods, 2018).

2.4.2 Etapas de pré-processamento em imagens faciais

Antes que uma imagem facial seja utilizada em um sistema de reconhecimento automático, é comum aplicar uma série de etapas de pré-processamento. Entre as mais importantes estão o recorte da região do rosto, o redimensionamento da imagem e a padronização de seus valores. O recorte do rosto tem como objetivo eliminar partes irrelevantes da imagem, como fundo e outros objetos, concentrando a análise apenas na região de interesse. O redimensionamento garante que todas as imagens tenham o mesmo tamanho, o que é necessário para que possam ser processadas de forma consistente por algoritmos e modelos que esperam entradas com dimensões fixas (Zhao *et al.*, 2003).

A padronização, por sua vez, inclui operações como normalização dos valores dos pixels e ajustes básicos de formato, garantindo que diferentes imagens, possivelmente capturadas em condições distintas, sejam apresentadas ao sistema de forma mais uniforme. Essas etapas são essenciais em sistemas automáticos porque reduzem

variações indesejadas que não estão relacionadas à identidade da pessoa, como diferenças de escala ou enquadramento, e tornam o processamento mais robusto e previsível(Zhao *et al.*, 2003).

2.5 Representação vetorial e medidas de similaridade

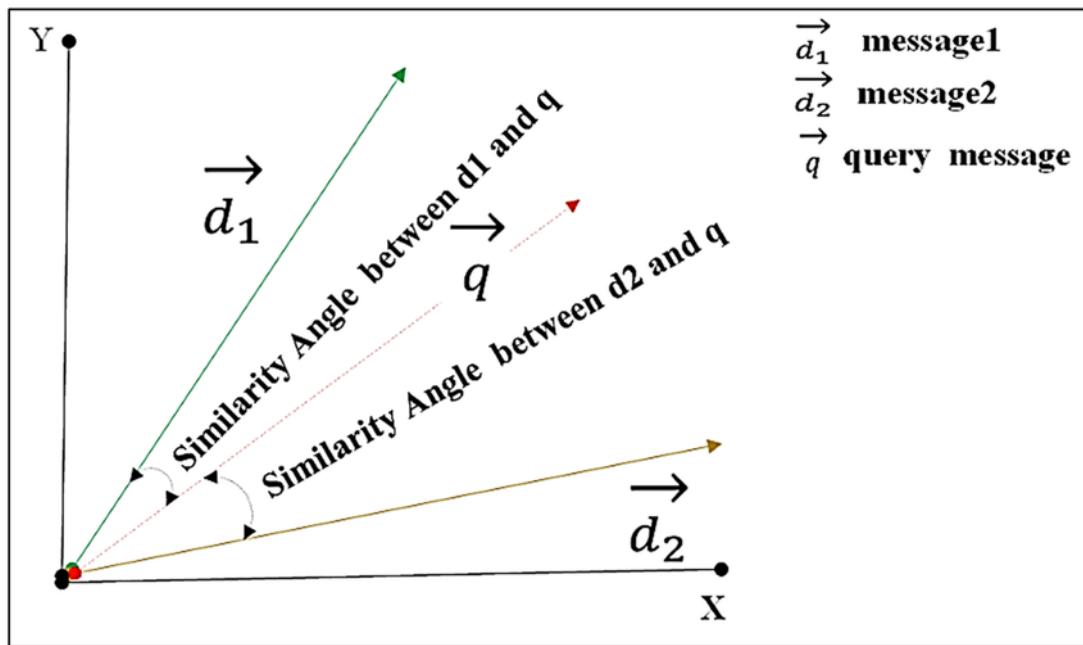
Para que um sistema computacional possa comparar automaticamente informações complexas, como imagens faciais, é necessário convertê-las em representações numéricas que permitam operações matemáticas bem definidas. Nesse contexto, as representações vetoriais e as medidas de distância desempenham um papel central, pois permitem transformar o problema de “duas imagens representam a mesma pessoa?” em uma questão de proximidade entre pontos em um espaço matemático. Essa abordagem está na base dos métodos modernos de reconhecimento facial baseados em *embeddings* (Theodoridis; Koutroumbas, 2009).

2.5.1 Conceito de vetor e interpretação geométrica

De forma intuitiva, um vetor pode ser entendido como um conjunto ordenado de números que representa um ponto em um espaço de múltiplas dimensões. Em duas dimensões, por exemplo, um vetor pode ser representado por um par de valores e visualizado como um ponto em um plano. Em três dimensões, ele pode ser visto como um ponto no espaço tridimensional. De maneira geral, quanto maior o número de valores que compõem o vetor, maior é a dimensão do espaço em que esse ponto está inserido (Bishop, 2006).

Essa interpretação geométrica é útil porque permite comparar vetores por meio de distâncias ou ângulos entre eles. Se dois vetores estão próximos no espaço, diz-se que eles são semelhantes segundo o critério adotado; se estão distantes, considera-se que representam coisas diferentes. Em sistemas de reconhecimento, cada objeto de interesse, como uma imagem facial, pode ser representado por um vetor, e a comparação entre objetos passa a ser feita pela análise da posição relativa desses pontos no espaço vetorial (Bishop, 2006).

Figura 2 – Similaridade entre dois vetores com base no modelo de espaço vetorial.



Fonte: (ResearchGate, s.d.)

2.5.2 Embeddings como representação de características

Um *embedding* pode ser entendido como um “resumo numérico” de características relevantes extraídas de um dado complexo, como uma imagem, um som ou um texto. No caso do reconhecimento facial, o *embedding* é um vetor que busca concentrar, em um conjunto de números, as informações mais discriminativas da face, de modo que diferentes imagens da mesma pessoa resultem em vetores próximos entre si, enquanto imagens de pessoas diferentes resultem em vetores mais distantes (Schroff; Kalenichenko; Philbin, 2015).

A principal vantagem desse tipo de representação é que ela permite comparar objetos complexos de forma simples e eficiente, utilizando apenas operações matemáticas entre vetores. Assim, em vez de comparar diretamente imagens pixel a pixel, o sistema compara seus *embeddings*, que são muito mais compactos e adequados para medir similaridade. Essa abordagem torna viável a construção de sistemas de reconhecimento baseados em métricas de distância no espaço vetorial (Schroff; Kalenichenko; Philbin, 2015).

2.5.3 Métricas de similaridade e distância

Para comparar vetores, é necessário definir uma métrica que quantifique o quanto próximos ou distantes eles estão. Uma das métricas mais intuitivas é a distância euclidiana, que corresponde, em termos geométricos, à distância em linha reta entre dois pontos no espaço. Essa medida é uma extensão natural da distância conhecida no plano ou no espaço tridimensional para espaços de maior dimensão (Bishop, 2006). Matematicamente, a distância euclidiana entre dois vetores \mathbf{x} e \mathbf{y} em um espaço n -dimensional é definida por:

$$d_E(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}. \quad (2.1)$$

Outra métrica amplamente utilizada, especialmente em sistemas de reconhecimento baseados em *embeddings*, é a distância cosseno. Essa métrica não mede diretamente a distância entre os pontos, mas sim o ângulo entre dois vetores, avaliando o quanto eles apontam na mesma direção, independentemente de seu comprimento (Schroff; Kalenichenko; Philbin, 2015). A similaridade cosseno entre dois vetores pode ser expressa como:

$$\text{cos_sim}(\mathbf{x}, \mathbf{y}) = \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|}. \quad (2.2)$$

A partir dessa definição, a distância cosseno é usualmente obtida como o complemento da similaridade cosseno, sendo dada por:

$$d_{\cos}(\mathbf{x}, \mathbf{y}) = 1 - \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{x}\| \|\mathbf{y}\|}. \quad (2.3)$$

Quando os vetores são previamente normalizados para terem norma unitária, isto é, quando $\|\mathbf{x}\| = \|\mathbf{y}\| = 1$, a comparação passa a depender apenas da orientação dos vetores no espaço. A normalização de um vetor \mathbf{x} pode ser expressa por:

$$\hat{\mathbf{x}} = \frac{\mathbf{x}}{\|\mathbf{x}\|}. \quad (2.4)$$

Por essa razão, a distância cosseno é frequentemente adotada em aplicações de reconhecimento facial baseadas em *embeddings*, uma vez que muitos modelos são

treinados para produzir vetores normalizados, nos quais a direção carrega a maior parte da informação discriminativa(Schroff; Kalenichenko; Philbin, 2015).

2.5.4 Limiar de decisão em sistemas de reconhecimento

A partir da definição de uma métrica de similaridade ou distância, é possível transformar o valor numérico obtido na comparação entre dois *embeddings* em uma decisão prática. Para isso, define-se um limiar de decisão, ou *threshold*, que separa os casos considerados semelhantes dos casos considerados diferentes. Em termos simples, se a distância entre dois vetores for menor que esse limiar, as amostras são interpretadas como pertencentes à mesma identidade; caso contrário, são tratadas como identidades distintas(Jain; Ross; Prabhakar, 2004). Essa regra de decisão pode ser formalizada da seguinte forma:

$$\text{decisão} = \begin{cases} \text{mesma identidade,} & \text{se } d(\mathbf{x}, \mathbf{y}) \leq \tau, \\ \text{identidades diferentes,} & \text{caso contrário.} \end{cases} \quad (2.5)$$

Esse mecanismo permite converter uma medida contínua de similaridade em uma decisão binária, adequada para aplicações de autenticação e identificação. A escolha do valor do *threshold* τ (Tau) influencia diretamente o comportamento do sistema, pois limiares mais rigorosos tendem a reduzir aceitações indevidas, enquanto limiares mais permissivos tendem a reduzir rejeições indevidas (Jain; Ross; Prabhakar, 2004). Por esse motivo, a definição desse parâmetro é tratada como uma etapa experimental e avaliada por meio de métricas de desempenho, como discutido em seções posteriores.

2.6 Aprendizado métrico: redes siamesas e Triplet Loss

Os conceitos de *embeddings* e de medidas de distância explicam como comparar representações vetoriais, mas não descrevem, por si só, como obter um espaço vetorial no qual identidades diferentes fiquem bem separadas e amostras da mesma identidade fiquem próximas. Essa organização do espaço é resultado de um paradigma conhecido como aprendizado métrico, amplamente discutido na literatura de aprendizado profundo e popularizado em cursos e materiais didáticos de autores como Andrew Ng. Nesse

paradigma, o objetivo principal não é apenas classificar amostras em categorias, mas aprender uma representação em que a noção de similaridade tenha significado geométrico (Bellet; Habrard; Sebban, 2015).

2.6.1 Classificação tradicional e aprendizado métrico

Em abordagens tradicionais de classificação, o modelo é treinado para associar cada entrada a um rótulo específico, como, por exemplo, identificar a qual classe uma imagem pertence. Nesse caso, o foco está em produzir uma decisão direta do tipo “esta imagem pertence à classe A ou à classe B”, sem que haja, necessariamente, uma preocupação explícita com a organização geométrica das representações internas do modelo (Bishop, 2006).

No aprendizado métrico, a ideia é diferente. Em vez de aprender apenas a prever rótulos, o modelo é treinado para construir um espaço de representação no qual amostras semelhantes fiquem próximas entre si e amostras diferentes fiquem afastadas. Assim, o resultado principal do modelo é um *embedding* que pode ser comparado com outros por meio de uma métrica de distância. Essa abordagem é particularmente adequada para problemas de reconhecimento, nos quais o interesse está em medir similaridade entre amostras, e não apenas em atribuir uma classe fixa(Bellet; Habrard; Sebban, 2015).

2.6.2 Redes siamesas

As redes siamesas, ou *Siamese Networks*, são uma arquitetura clássica utilizada em aprendizado métrico. Elas consistem em duas redes neurais idênticas, que compartilham os mesmos pesos e processam duas entradas diferentes em paralelo. Cada uma das entradas é transformada em um *embedding*, e a saída do sistema é obtida a partir da comparação entre esses dois vetores, geralmente por meio de uma medida de distância ou similaridade (Koch; Zemel; Salakhutdinov, 2015).

Esse tipo de arquitetura é naturalmente adequado para tarefas de verificação no formato 1:1, pois permite responder à pergunta: “essas duas amostras representam a mesma entidade?”. Em vez de classificar cada entrada isoladamente, a rede aprende a produzir representações que podem ser comparadas diretamente, tornando a decisão

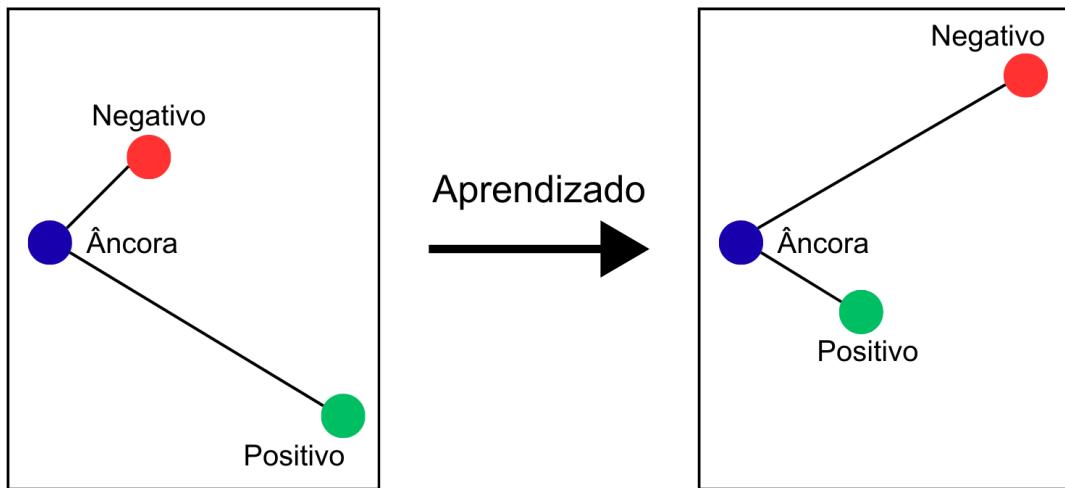
dependente da proximidade entre os *embeddings* gerados (Koch; Zemel; Salakhutdinov, 2015).

2.6.3 Função de perda Triplet Loss

Uma extensão importante dessa ideia é o uso da função de perda conhecida como *Triplet Loss*. Nessa abordagem, o treinamento é feito a partir de trios de amostras: uma amostra âncora, uma amostra positiva (da mesma identidade da âncora) e uma amostra negativa (de identidade diferente). O objetivo da função de perda é garantir que a distância entre a âncora e a amostra positiva seja menor do que a distância entre a âncora e a amostra negativa por, pelo menos, uma certa margem (Schroff; Kalenichenko; Philbin, 2015).

Em termos geométricos, isso significa forçar o modelo a organizar o espaço de *embeddings* de modo que pontos correspondentes à mesma identidade fiquem agrupados, enquanto pontos de identidades diferentes sejam empurrados para regiões mais distantes. Essa interpretação visual é frequentemente utilizada para ilustrar o funcionamento do aprendizado métrico e está diretamente relacionada à ideia de estruturar o espaço vetorial para tornar a separação entre classes mais clara e consistente. A Figura 3 ilustra, de forma conceitual, a organização do espaço de *embeddings* em abordagens baseadas em aprendizado métrico (Schroff; Kalenichenko; Philbin, 2015).

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



Fonte: Elaborado pelo autor, 2026.

2.6.4 Aplicação do aprendizado métrico ao reconhecimento facial

No contexto do reconhecimento facial, o aprendizado métrico é especialmente relevante porque as imagens de uma mesma pessoa podem apresentar variações significativas, como mudanças de iluminação, pequenas diferenças de pose, expressões faciais ou ruído na captura. Um bom espaço de *embeddings* deve ser capaz de absorver essas variações, mantendo as representações da mesma identidade próximas entre si, ao mesmo tempo em que preserva a separação em relação a outras identidades (Schroff; Kalenichenko; Philbin, 2015).

A filosofia apresentada por autores como Andrew Ng, ao discutir redes siamesas e *Triplet Loss*, fundamenta justamente essa organização do espaço de representação. Na prática, a qualidade desse espaço pode ser avaliada observando-se a separabilidade entre pares da mesma identidade e de identidades diferentes, como realizado nos experimentos deste trabalho. Dessa forma, os resultados obtidos empiricamente refletem diretamente os princípios teóricos do aprendizado métrico, confirmando a importância desse paradigma para sistemas modernos de reconhecimento facial baseados em *embeddings* (Schroff; Kalenichenko; Philbin, 2015).

2.7 Modelos pré-treinados e reconhecimento facial por embeddings

O treinamento de modelos de aprendizado profundo para reconhecimento facial a partir do zero exige grandes volumes de dados, infraestrutura computacional significativa e longos tempos de treinamento. Por esse motivo, em muitas aplicações práticas, adota-se o uso de modelos pré-treinados, que já foram ajustados previamente em grandes bases de dados e são capazes de produzir representações faciais de alta qualidade. Esses modelos seguem a mesma filosofia do aprendizado métrico discutido anteriormente, gerando *embeddings* nos quais a distância entre vetores reflete a similaridade entre identidades (Schroff; Kalenichenko; Philbin, 2015).

2.7.1 Aprendizado por transferência e modelos pré-treinados

O *transfer learning*, ou aprendizado por transferência, é uma estratégia na qual o conhecimento adquirido por um modelo em uma tarefa ou conjunto de dados é reaproveitado em outra aplicação relacionada. Em vez de treinar uma rede neural do zero, utiliza-se um modelo que já aprendeu a extrair características relevantes a partir de um grande conjunto de exemplos, adaptando-o ou simplesmente reutilizando suas saídas para uma nova finalidade (Pan; Yang, 2010).

No contexto do reconhecimento facial, modelos pré-treinados são ajustados previamente em bases de dados extensas e diversificadas, contendo milhões de imagens de diferentes pessoas. Como resultado, esses modelos aprendem a extrair características faciais robustas e discriminativas, que podem ser utilizadas diretamente como *embeddings*. Essa abordagem permite obter bons resultados mesmo em cenários com conjuntos de dados menores, além de reduzir significativamente o custo computacional e a complexidade do desenvolvimento (Schroff; Kalenichenko; Philbin, 2015).

2.7.2 Embeddings discriminativos para reconhecimento facial

Modelos modernos de reconhecimento facial, como aqueles inspirados em abordagens do tipo FaceNet ou ArcFace, são treinados com o objetivo de produzir *embeddings* que maximizem a separação entre identidades diferentes e minimizem a

distância entre amostras da mesma identidade. Em nível conceitual, isso significa que a rede aprende a transformar uma imagem facial em um vetor que captura características essenciais da estrutura do rosto, descartando variações irrelevantes, como pequenas mudanças de iluminação ou expressão (Schroff; Kalenichenko; Philbin, 2015) e (Deng *et al.*, 2019).

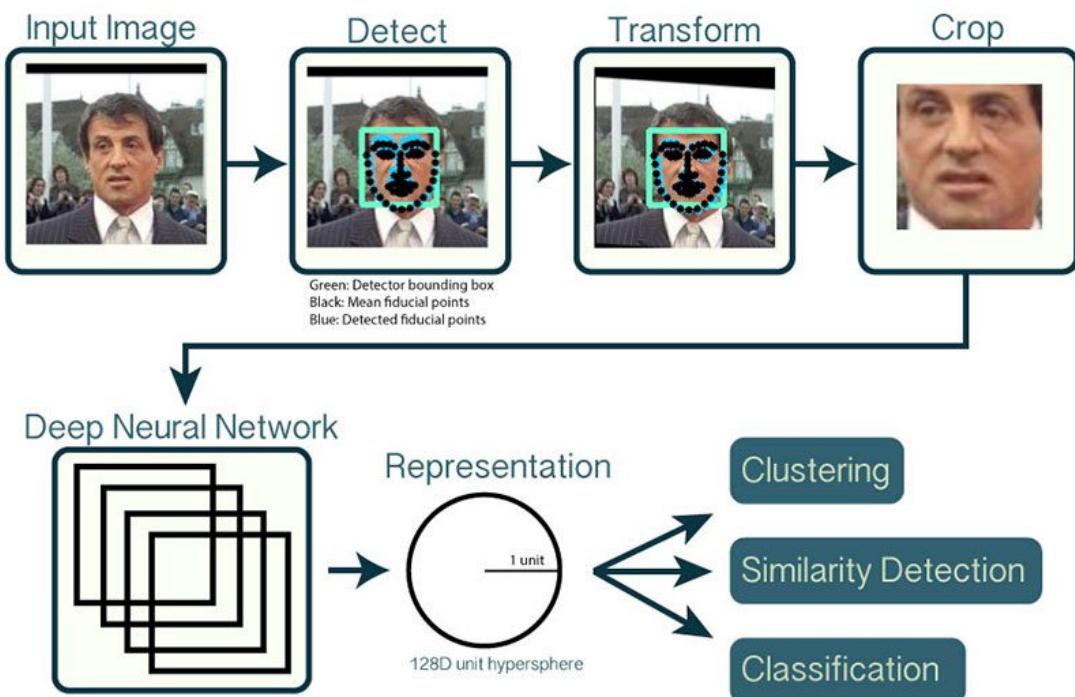
Embora o processo interno de aprendizado envolva operações matemáticas complexas, a ideia fundamental pode ser entendida de forma simples: o modelo aprende a destacar aquilo que torna um rosto diferente de outros rostos, e a representar essas diferenças em forma de números organizados em um vetor. Dessa forma, duas imagens da mesma pessoa tendem a gerar *embeddings* semelhantes, enquanto imagens de pessoas diferentes tendem a gerar *embeddings* mais distantes no espaço vetorial (Schroff; Kalenichenko; Philbin, 2015) e (Deng *et al.*, 2019).

2.7.3 Detecção facial e reconhecimento facial

É importante distinguir duas etapas conceitualmente diferentes em sistemas de reconhecimento facial: a detecção da face e o reconhecimento da identidade. A detecção facial tem como objetivo localizar “onde está a face” em uma imagem, isto é, identificar a região que contém um rosto, separando-a do fundo e de outros elementos da cena. Essa etapa responde apenas à pergunta “existe um rosto aqui e onde ele está?” (Zhao *et al.*, 2003).

O reconhecimento facial, por sua vez, ocorre após a face já ter sido detectada e recortada. Nessa etapa, o sistema busca responder à pergunta “quem é essa pessoa?”, extraíndo um *embedding* da região facial e comparando-o com representações previamente armazenadas. Separar essas duas etapas é fundamental para compreender o funcionamento do pipeline de reconhecimento, pois a qualidade da detecção influencia diretamente a qualidade das representações utilizadas na comparação, mas os objetivos de cada processo são distintos (Zhao *et al.*, 2003).

Figura 4 – Pipeline típico de reconhecimento facial



Fonte: (PyImageSearch, 2018)

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

A avaliação de sistemas biométricos não se limita a verificar se o sistema “funciona” em alguns exemplos, mas exige a análise sistemática de como ele se comporta diante de diferentes tipos de erros. Em aplicações de controle de acesso, esses erros têm impactos distintos: aceitar indevidamente um usuário não autorizado compromete a segurança, enquanto rejeitar indevidamente um usuário legítimo compromete a usabilidade. Por esse motivo, métricas específicas são utilizadas para quantificar esses comportamentos e orientar a escolha de parâmetros de decisão, como o *threshold* adotado na comparação entre *embeddings* (Jain; Ross; Prabhakar, 2004).

2.8.1 Matriz de confusão

A análise de desempenho de um sistema de decisão binária costuma ser organizada por meio da chamada matriz de confusão, que categoriza os resultados das comparações em quatro grupos. Os verdadeiros positivos (TP) correspondem aos casos em que o sistema aceita corretamente uma comparação que realmente pertence à

mesma identidade. Os verdadeiros negativos (TN) correspondem aos casos em que o sistema rejeita corretamente uma comparação entre identidades diferentes (Bishop, 2006).

Por outro lado, os falsos positivos (FP) representam situações em que o sistema aceita indevidamente uma comparação entre identidades diferentes, caracterizando um erro de segurança. Já os falsos negativos (FN) correspondem aos casos em que o sistema rejeita indevidamente uma comparação que deveria ser aceita, caracterizando um erro que afeta a experiência do usuário. Essas quatro categorias formam a base para o cálculo das métricas biométricas mais utilizadas(Jain; Ross; Prabhakar, 2004).

2.8.2 Taxas de erro biométrico: FAR e FRR

A FAR (*False Acceptance Rate*) é definida como a proporção de falsos positivos em relação ao total de comparações entre identidades diferentes. Em termos práticos, essa métrica indica a probabilidade de o sistema aceitar indevidamente um usuário não autorizado. Já a FRR (*False Rejection Rate*) é definida como a proporção de falsos negativos em relação ao total de comparações entre amostras da mesma identidade, indicando a probabilidade de o sistema rejeitar indevidamente um usuário legítimo (Jain; Ross; Prabhakar, 2004). Essas métricas podem ser formalmente expressas pelas seguintes equações:

$$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}}, \quad (2.6)$$

$$\text{FRR} = \frac{\text{FN}}{\text{FN} + \text{TP}}. \quad (2.7)$$

Essas duas métricas expressam, de forma complementar, o comportamento do sistema frente a erros de decisão. Em geral, ao tornar o sistema mais rigoroso, reduz-se a FAR, mas aumenta-se a FRR. Por outro lado, ao tornar o sistema mais permissivo, reduz-se a FRR, mas aumenta-se a FAR. Essa relação evidencia a existência de um compromisso entre segurança e usabilidade (Jain; Ross; Prabhakar, 2004).

2.8.3 Definição do limiar de decisão em sistemas reais

A escolha do *threshold* que separa decisões de aceitação e rejeição influencia diretamente os valores de FAR e FRR. Um limiar mais baixo tende a tornar o sistema mais rigoroso, reduzindo a probabilidade de aceitar indevidamente uma identidade incorreta, mas aumentando a chance de rejeitar usuários legítimos. Por outro lado, um limiar mais alto torna o sistema mais permissivo, diminuindo as rejeições indevidas, mas aumentando o risco de aceitações indevidas (Jain; Ross; Prabhakar, 2004).

Em aplicações de controle de acesso, esse compromisso costuma ser resolvido com prioridade para a redução da FAR, pois aceitar um usuário não autorizado representa um risco direto à segurança do sistema. Embora rejeições indevidas também sejam indesejáveis, elas tendem a ser tratadas como um problema operacional, enquanto falsas aceitações podem comprometer o propósito principal do controle de acesso. Por esse motivo, a definição do *threshold* é tratada como uma decisão baseada em critérios de segurança, apoiada por análises quantitativas das métricas biométricas (Jain; Ross; Prabhakar, 2004).

2.9 Privacidade, LGPD e uso de dados sintéticos

O uso de sistemas biométricos levanta questões importantes relacionadas à privacidade e à proteção de dados pessoais, uma vez que características biométricas estão diretamente ligadas à identidade dos indivíduos. Diferentemente de senhas ou cartões, dados biométricos não podem ser simplesmente substituídos em caso de vazamento ou uso indevido, o que torna necessário um cuidado especial tanto no desenvolvimento quanto na avaliação de soluções baseadas nesse tipo de informação (Ratha; Connell; Bolle, 2001). Por esse motivo, aspectos éticos e legais são parte fundamental da discussão sobre a viabilidade de sistemas de reconhecimento facial.

2.9.1 Dados biométricos e sua sensibilidade

Dados biométricos correspondem a informações obtidas a partir de características físicas ou comportamentais de uma pessoa, como rosto, impressões digitais ou íris. Essas

informações permitem identificar ou autenticar indivíduos de forma relativamente precisa, o que as torna particularmente valiosas em sistemas de controle de acesso e segurança (Jain; Ross; Prabhakar, 2004).

Ao mesmo tempo, essa capacidade de identificação torna os dados biométricos sensíveis. Caso sejam utilizados de forma indevida ou sofram vazamentos, podem expor os indivíduos a riscos que não podem ser facilmente revertidos, já que não é possível “trocar” o rosto ou a impressão digital como se troca uma senha. Por essa razão, o tratamento desse tipo de dado exige medidas rigorosas de proteção e justificativas claras para sua coleta e uso (Ratha; Connell; Bolle, 2001).

2.9.2 Aspectos gerais da LGPD aplicados à biometria

No contexto brasileiro, o tratamento de dados pessoais é regulado pela LGPD, que estabelece princípios e obrigações para a coleta, o armazenamento e o uso dessas informações. Entre os princípios centrais estão a existência de uma base legal para o tratamento, a definição clara da finalidade do uso dos dados, a minimização da coleta ao estritamente necessário e a adoção de medidas de segurança para proteger as informações contra acessos não autorizados ou vazamentos (Presidência da República - Casa Civil, 2018).

No caso de dados biométricos, esses cuidados tornam-se ainda mais relevantes, pois se trata de uma categoria de dados pessoais sensíveis. Isso implica que projetos que envolvem reconhecimento facial devem considerar desde o início como garantir a conformidade legal, a proteção da privacidade dos usuários e a redução de riscos associados ao uso dessas informações (Presidência da República - Casa Civil, 2018).

2.9.3 Uso de imagens faciais sintéticas em experimentos

Diante dessas preocupações, uma estratégia adotada neste trabalho foi o uso de imagens faciais sintéticas, geradas por modelos baseados em *GANs* (*Generative Adversarial Networks*). Essas imagens representam rostos inexistentes e não estão associadas a pessoas reais, o que elimina riscos de identificação indevida e problemas relacionados à exposição de dados biométricos reais (Goodfellow *et al.*, 2020).

Além de reduzir significativamente os riscos éticos e legais, o uso de dados sintéticos facilita a condução de experimentos e a reprodutibilidade dos resultados, pois a base de dados pode ser compartilhada e reutilizada sem violar a privacidade de indivíduos. Dessa forma, é possível avaliar o comportamento do *pipeline* de reconhecimento facial de maneira controlada, mantendo o foco nos aspectos técnicos do método proposto, sem comprometer princípios de proteção de dados (Shorten; Khoshgoftaar, 2019).

2.10 Segurança na comunicação e criptografia aplicada

Em sistemas distribuídos, como aqueles que envolvem captura de imagens, processamento em servidor e retorno de resultados ao cliente, a segurança não depende apenas dos algoritmos de reconhecimento utilizados, mas também da forma como os dados são transmitidos entre os diferentes componentes. Mesmo que o modelo de reconhecimento seja confiável, a exposição das informações durante a comunicação pode comprometer todo o sistema (Stallings, 2017). Por esse motivo, é necessário distinguir a segurança do canal de comunicação da segurança do modelo de reconhecimento, tratando cada uma dessas dimensões de forma adequada.

2.10.1 Ameaças em sistemas de comunicação

Quando dados trafegam por uma rede, existem ameaças conhecidas que podem afetar sua confidencialidade e confiabilidade. Uma dessas ameaças é a escuta não autorizada, na qual um terceiro intercepta a comunicação para obter informações transmitidas. Outra ameaça é a adulteração, que ocorre quando os dados são modificados durante o trânsito, podendo levar o sistema a processar informações incorretas ou maliciosas (Stallings, 2017).

Há também o risco de ataques de *replay*, nos quais mensagens legítimas capturadas anteriormente são reenviadas por um atacante para tentar obter uma resposta indevida do sistema. Em aplicações de controle de acesso, esse tipo de ataque pode permitir, por exemplo, que uma requisição válida seja reutilizada fora de contexto. Essas ameaças mostram que a simples troca de dados em rede, sem proteção adequada, pode

comprometer seriamente a segurança do sistema como um todo (Stallings, 2017).

2.10.2 Conceitos fundamentais de criptografia

A criptografia oferece mecanismos para mitigar essas ameaças por meio de três objetivos principais: confidencialidade, integridade e autenticidade. A confidencialidade garante que apenas as partes autorizadas consigam ler o conteúdo transmitido, mesmo que os dados sejam interceptados por terceiros. A integridade assegura que qualquer modificação nos dados durante a transmissão possa ser detectada, evitando que informações adulteradas sejam aceitas pelo sistema (Stallings, 2017).

A autenticidade, por sua vez, permite verificar a identidade das partes envolvidas na comunicação, garantindo que o cliente está realmente se comunicando com o servidor legítimo, e vice-versa. Em conjunto, esses três princípios formam a base da comunicação segura em sistemas modernos, especialmente quando dados sensíveis, como informações biométricas ou representações faciais, precisam ser transmitidos entre diferentes componentes (Stallings, 2017).

2.10.3 TLS, HTTPS e autenticação mútua

Na prática, esses princípios são implementados por meio de protocolos amplamente utilizados, como TLS (*Transport Layer Security*), que está na base do HTTPS. O uso de TLS permite estabelecer um canal de comunicação criptografado entre cliente e servidor, protegendo os dados contra escuta e adulteração, além de permitir a verificação da identidade do servidor por meio de certificados digitais (Rescorla, 2018).

Em cenários que exigem maior nível de confiança, pode-se empregar a autenticação mútua, conhecida como mTLS, na qual tanto o servidor quanto o cliente apresentam certificados para provar suas identidades. Isso cria um vínculo de confiança bidirecional entre as partes, reduzindo o risco de comunicação com entidades não autorizadas. No contexto do pipeline considerado neste trabalho, esse mecanismo é relevante para proteger a troca de informações entre o componente de captura e o servidor de processamento (Rescorla, 2018).

É importante ressaltar, contudo, que a segurança do canal não garante, por si

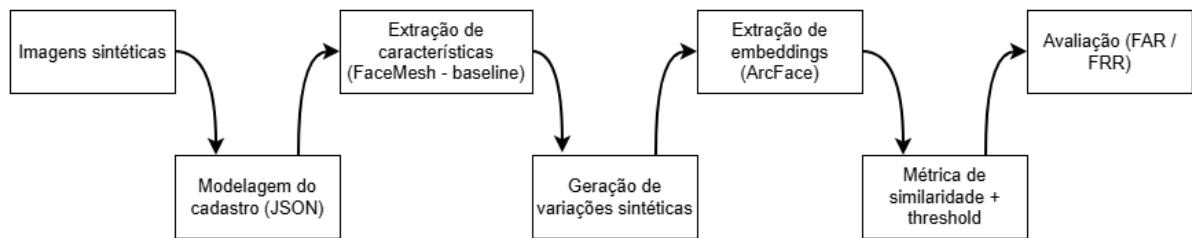
só, a segurança do modelo de reconhecimento ou das decisões tomadas pelo sistema. Protocolos como TLS e mTLS protegem a comunicação, mas não impedem, por exemplo, erros de classificação ou vulnerabilidades inerentes ao modelo. Por isso, a segurança da transmissão e a confiabilidade do reconhecimento devem ser tratadas como aspectos complementares de um mesmo sistema (Anderson, 2020).

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 5 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 5 – 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.

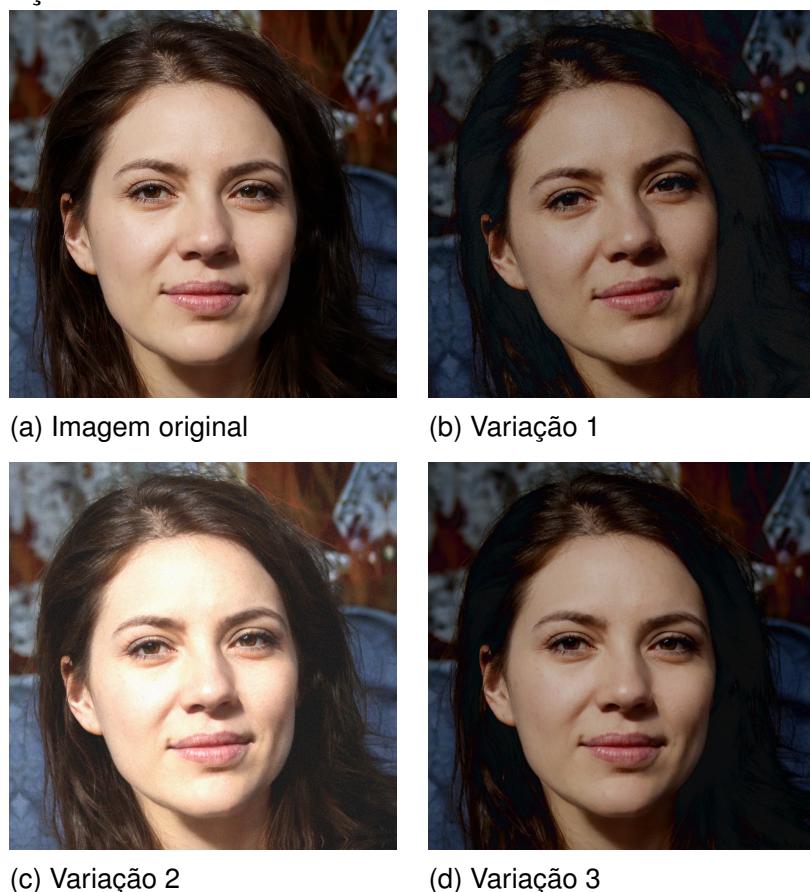
3.4 Geração de variações sintéticas das imagens

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 6 ilustra um exemplo de imagem facial original e suas respectivas variações sintéticas, evidenciando o efeito das transformações artificiais aplicadas para uma mesma identidade.

Figura 6 – 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).

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

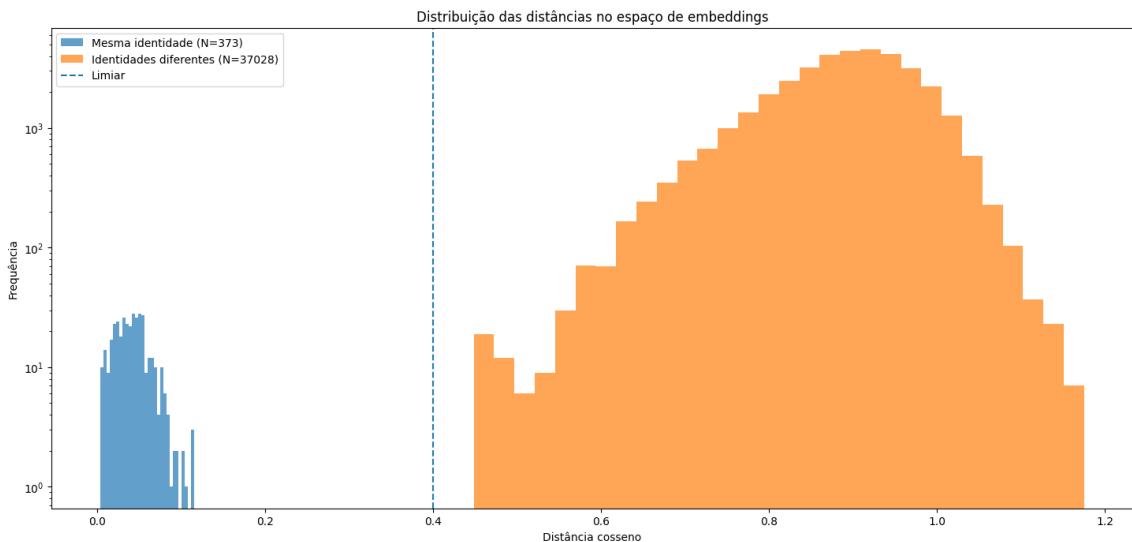
Este capítulo apresenta os resultados obtidos a partir dos experimentos realizados com a base de dados sintética e os modelos de reconhecimento facial descritos na metodologia. Os resultados concentram-se na análise da separabilidade das representações faciais no espaço de *embeddings*, na avaliação 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 7 – Distribuição das distâncias cosseno no espaço de *embeddings*



Fonte: Elaborado pelo autor, 2026.

A Figura 7 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 8 – Exemplo de par da mesma identidade corretamente aceitos

MESMA PESSOA | Distância: 0.0458



Fonte: Elaborado pelo autor, 2026.

Figura 9 – 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.

ANDERSON, Ross J. **Security Engineering: A Guide to Building Dependable Distributed Systems**. 3. ed. Hoboken, NJ, USA: Wiley, 2020. ISBN 9781119642787.

BELLET, Aurélien; HABRARD, Amaury; SEBBAN, Marc. A Survey on Metric Learning for Feature Vectors and Structured Data. **Journal of Machine Learning Research**, v. 16, p. 1–45, 2015.

BISHOP, Christopher M. **Pattern Recognition and Machine Learning**. New York: Springer, 2006. ISBN 9780387310732.

BOLLE, Ruud M. *et al.* **Guide to Biometrics**. [S. l.]: Springer, 2013.

CHATMON, Christy; LE, Tri Van; BURMASTER, Mike. Secure Anonymous RFID Authentication Protocols. **Florida State University / Florida A&M University (Technical Report)**, 2006.

DENG, Jiankang *et al.* ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In: PROCEEDINGS of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). [S. l.: s. n.], 2019. p. 4690–4699.

EQUIPE TOTVS. **O que é RFID, como funciona e aplicações dessa tecnologia**. [S. l.: s. n.], 2022. <https://www.totvs.com/blog/gestao-industrial/rfid/>. acesso em: 1 fev. 2026.

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.

GONZALEZ, Rafael C.; WOODS, Richard E. **Digital Image Processing**. 4. ed. New York: Pearson, 2018.

GOODFELLOW, Ian *et al.* Generative Adversarial Networks. **Communications of the ACM**, ACM, v. 63, n. 11, p. 139–144, 2020. DOI: 10.1145/3422622.

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.

HASSABALLAH, Mahmoud; ALY, Saleh. Face Recognition: Challenges, Achievements and Future Directions. **IET Computer Vision**, The Institution of Engineering e Technology, v. 9, n. 4, p. 614–626, 2015. DOI: 10.1049/iet-cvi.2014.0084.

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.

KOCH, Gregory; ZEMEL, Richard; SALAKHUTDINOV, Ruslan. Siamese Neural Networks for One-shot Image Recognition. In: PROCEEDINGS of the 32nd International Conference on Machine Learning (ICML). [S. I.: s. n.], 2015. p. 1–8.

MARQUES FILHO, Ogê; VIEIRA NETO, Hugo. **Processamento Digital de Imagens**. Rio de Janeiro: Brasport, 1999. ISBN 8574520098.

MASYUK, M. A. Information Security of RFID and NFC Technologies. **Journal of Physics: Conference Series**, IOP Publishing, v. 1399, p. 033093, 2019. DOI: 10.1088/1742-6596/1399/3/033093.

NG, Andrew. **Deep Learning Specialization**. [S. I.: 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.

PAN, Sinno Jialin; YANG, Qiang. A Survey on Transfer Learning. **IEEE Transactions on Knowledge and Data Engineering**, IEEE, v. 22, n. 10, p. 1345–1359, 2010. DOI: 10.1109/TKDE.2009.191.

PARMAR, Divyarajsingh N.; MEHTA, Brijesh B. Face Recognition Methods & Applications. **International Journal of Computer Technology & Applications**, v. 4, n. 1, p. 84–86, 2013.

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)** - Lei nº 13.709/2018. [S. I.: s. n.], 2018.

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, acesso em: 30 jan. 2026. Brasil.

PYIMAGESEARCH. **OpenCV Face Recognition Tutorial.** [S. l.: s. n.], 2018. <https://pyimagesearch.com/2018/09/24/opencv-face-recognition/>. Acesso em: 04 fev. 2026.

RATHA, Nalini K.; CONNELL, Jonathan H.; BOLLE, Ruud M. Enhancing Security and Privacy in Biometrics-Based Authentication Systems. **IBM Systems Journal**, v. 40, n. 3, p. 614–634, 2001.

RESCORLA, Eric. **The Transport Layer Security (TLS) Protocol Version 1.3.** [S. l.], 2018. Disponível em: <https://www.rfc-editor.org/rfc/rfc8446>.

RESEARCHGATE. **Trigonometric words ranking model for spam message classification.** [S. l.: s. n.]. https://www.researchgate.net/publication/363771554_Trigonometric_words_ranking_model_for_spam_message_classification. Acesso em: 04 fev. 2026.

RFID SILICONE. **What Is NFC (Near Field Communication) and How Does It Work?** [S. l.: s. n.], 2024. <https://www.rfidsilicone.com/blog/industry-news/what-is-nfc-near-field-communication-how-does-it-work.html>. Acesso em: 18 mar. 2024.

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.

SHORTEN, Connor; KHOSHGOFTAAR, Taghi M. A Survey on Image Data Augmentation for Deep Learning. **Journal of Big Data**, v. 6, n. 60, 2019. DOI: 10.1186/s40537-019-0197-0.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 7. ed. Boston: Pearson, 2017.

THEODORIDIS, Sergios; KOUTROUMBAS, Konstantinos. **Pattern Recognition**. 4. ed. Burlington, MA, USA: Academic Press, 2009. ISBN 9780123695312.

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

ZHAO, Weny i et al. Face Recognition: A Literature Survey. **ACM Computing Surveys**, v. 35, n. 4, p. 399–458, 2003. DOI: 10.1145/954339.954342.