

Além do Desempenho: Um Estudo da Confiabilidade de Detectores de Deepfakes

Lucas Lopes¹, Rayson Laroca^{2,1}, André Grégio¹

¹Universidade Federal do Paraná (UFPR), Curitiba, Brasil

²Pontifícia Universidade Católica do Paraná (PUCPR), Curitiba, Brasil

¹{lflopes, gregio}@inf.ufpr.br ²rayson@ppgia.pucpr.br

Abstract. Deepfakes are synthetic media generated by artificial intelligence, with positive applications in education and creativity, but also serious negative impacts such as fraud, misinformation, and privacy violations. Although detection techniques have advanced, comprehensive evaluation methods that go beyond classification performance remain lacking. This paper proposes a reliability assessment framework based on four pillars: transferability, robustness, interpretability, and computational efficiency. An analysis of five state-of-the-art methods revealed significant progress as well as critical limitations.

Resumo. Deepfakes são mídias sintéticas geradas por inteligência artificial, com aplicações positivas na educação e na criatividade, mas também com impactos negativos graves, como fraudes, desinformação e violações de privacidade. Apesar dos avanços em técnicas de detecção, ainda há escassez de métodos de avaliação abrangentes que considerem aspectos além do desempenho em classificação. Este trabalho propõe um framework de avaliação da confiabilidade baseado em quatro pilares: transferibilidade, robustez, interpretabilidade e eficiência computacional. A análise de cinco métodos do estado da arte revelou avanços significativos, mas também limitações críticas.

1. Introdução

Nos últimos anos, a geração de conteúdo sintético por inteligência artificial (IA) tem ganhado destaque tanto na academia quanto na indústria [Abdullah et al., 2024]. Dentre as diversas tecnologias emergentes, os *deepfakes* se destacam pela capacidade de produzir imagens e vídeos altamente realistas [Pei et al., 2024]. Embora essa tecnologia possua aplicações legítimas nos ramos de entretenimento, educação e comércio [Caporusso, 2021; Roe et al., 2024], sua disseminação também levanta sérias preocupações no âmbito social, político e financeiro, especialmente quando utilizada para fraudes, desinformação e ataques à privacidade [Wang et al., 2024a].

O termo deepfake se refere a uma técnica de síntese de mídia baseada em redes neurais profundas. Desde sua popularização em 2017, com um modelo de troca de rostos (*face swap*) divulgado no Reddit [Deepfakes, 2017], a tecnologia evoluiu significativamente, passando a permitir reencenação facial, modificação de expressões, e até geração completa de vídeos reencenados [Suwajanakorn et al., 2017]. No cinema, deepfakes foram utilizados para rejuvenescer atores em filmes como *Gemini Man* [Murphy et al., 2023],

Artigo aceito no Simpósio Brasileiro de Cibersegurança (SBSeg 2025). A versão publicada está disponível na SBC-OpenLib (SOL) (<https://doi.org/10.5753/sbseg.2025.11431>).

enquanto na educação tutores virtuais personalizados foram criados com IA para atender diferentes perfis de alunos [Roe et al., 2024]. No setor de varejo, marcas já exploram o uso da tecnologia para experimentação virtual de roupas e acessórios [Caporusso, 2021].

Contudo, o uso indevido de deepfakes tem crescido de maneira alarmante. Em fevereiro de 2024, um golpe utilizando deepfakes em uma videoconferência levou uma multinacional de Hong Kong a perder 25 milhões de dólares [Melappalayam, 2024]. Em abril do mesmo ano, um fraudador se passando por Elon Musk enganou uma vítima, resultando no desvio do equivalente a 50 mil dólares [Sharma, 2024]. Esses eventos demonstram o avanço das técnicas de manipulação e a urgência do desenvolvimento de sistemas de detecção robustos e confiáveis.

Diante desse cenário, o desenvolvimento de técnicas eficazes para a detecção de deepfakes tornou-se essencial. Diversos métodos têm sido propostos, com abordagens que vão desde o uso de características físicas faciais [Zhou e Lim, 2021; Hernandez-Ortega et al., 2022; Wang et al., 2024a] até arquiteturas sofisticadas baseadas em aprendizado profundo [Jeong et al., 2022; Kong et al., 2024]. No entanto, observa-se que grande parte desses trabalhos concentra sua avaliação em métricas tradicionais de desempenho, como acurácia (ACC) ou o valor da área sob a curva ROC (AUC) em conjuntos de teste padronizados, sem considerar aspectos críticos como robustez a perturbações, interpretabilidade dos resultados, ou viabilidade computacional.

Neste trabalho, propomos uma abordagem mais abrangente para a avaliação de detectores de deepfakes, estruturada em quatro pilares fundamentais: transferibilidade, robustez, interpretabilidade e eficiência computacional. Além disso, oferecemos uma quantificação objetiva e padronizada desses pilares, consolidando-os em um escore de confiabilidade global que permite comparar métodos sob uma perspectiva mais realista.

Além disso, realizamos uma revisão dos principais métodos de geração e detecção da literatura recente, os quais foram reagrupados em categorias com base em suas estratégias e técnicas predominantes. Como prova de conceito, aplicamos o framework proposto a cinco detectores representativos do estado da arte, analisando seus pontos fortes e limitações em múltiplas dimensões de confiabilidade. Com isso, esperamos contribuir para uma avaliação mais ampla e crítica dos métodos de detecção de deepfakes, estimulando o desenvolvimento de soluções mais transparentes, robustas e acessíveis.

2. Fundamentos e Tecnologias de Geração de Deepfakes

As técnicas de geração de deepfakes podem ser agrupadas em três categorias principais: troca de rostos (*face swap*), que substitui a identidade facial em imagens ou vídeos [Deepfakes, 2017]; recriação de expressões (*face reenactment*), que transfere gestos e emoções de um indivíduo para outro [Suwajanakorn et al., 2017]; e geração de rostos falantes (*talking face generation*), que sincroniza imagens faciais com áudio [Xie et al., 2024].

O avanço dessas técnicas está fortemente associado à evolução de modelos geratitivos [Pei et al., 2024], especialmente *autoencoders*, redes adversárias gerativas (GANs, do Inglês *Generative Adversarial Networks*) [Goodfellow et al., 2014] e, mais adiante, modelos de difusão (DDPM, do Inglês *Denoising Diffusion Probabilistic Models*) [Ho et al., 2020], que possibilitam a síntese de imagens realistas com diferentes graus de controle, fidelidade e qualidade [dos Santos et al., 2024].

2.1. Autoencoders

Autoencoders foram amplamente utilizados nos primeiros modelos de *face swap* e reencenação, com um codificador compartilhado e decodificadores específicos para cada identidade. Como ilustrado na Figura 1, essa arquitetura permite reconstruir a expressão facial original com a identidade do rosto-alvo [Deepfakes, 2017; Wang et al., 2024a]. No entanto, exigem decodificadores treinados por identidade, o que limita sua escalabilidade. Para contornar essa limitação, modelos independentes de identidade passaram a incorporar GANs no processo de geração.

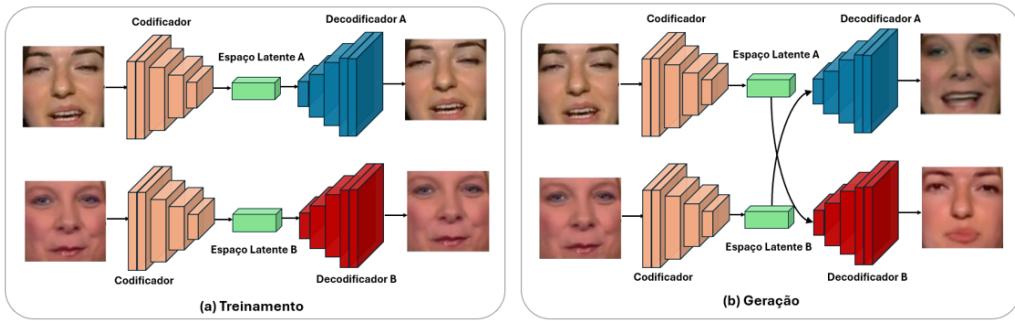


Figura 1. Esquema de uso de autoencoders para reencenação: (a) Treinamento com codificador compartilhado e decodificadores específicos por identidade; (b) Geração da face final, combinando a expressão da imagem de entrada com a identidade do alvo.

2.2. Redes Adversárias Generativas (GANs)

As GANs, compostas por um gerador e um discriminador treinados de forma adversarial (veja a Figura 2), tornaram-se o principal mecanismo para a geração de faces realistas [Goodfellow et al., 2014]. Abordagens como FaceShifter [Li et al., 2019] e SimSwap [Chen et al., 2020] propõem modelos independentes de identidade que integram características faciais da origem na imagem-alvo, com maior robustez a oclusões. Posteriormente, arquiteturas baseadas no StyleGAN [Karras et al., 2021] viabilizaram a geração de imagens em alta resolução [Wang et al., 2024a]. Apesar da alta qualidade dos resultados, o treinamento de GANs exige cuidados com a estabilidade e a escolha de hiperparâmetros, além de etapas adicionais de pós-processamento para a remoção de artefatos [Kim et al., 2025].

2.3. Modelos de Difusão

Modelos de difusão surgem como alternativa às GANs, oferecendo treinamento mais estável e maior diversidade amostral, ao gerar imagens por meio da reversão de um processo de adição de ruído [Bishop e Bishop, 2024]. Métodos como DiffFace [Kim et al., 2025] e DiffSwap [Zhao et al., 2023] aplicam esse princípio à tarefa de geração e troca de rostos, tratando-a como um problema de *inpainting* condicional, com foco na preservação da identidade e expressividade do alvo. A Figura 3 ilustra o processo de treinamento de um modelo de difusão para geração de faces.

Outro exemplo notável é o *X-Portrait* [Xie et al., 2024], que permite a geração de animações altamente realistas a partir de imagens estáticas. Apesar do potencial, esses modelos ainda enfrentam limitações relacionadas ao alto custo computacional e ao tempo

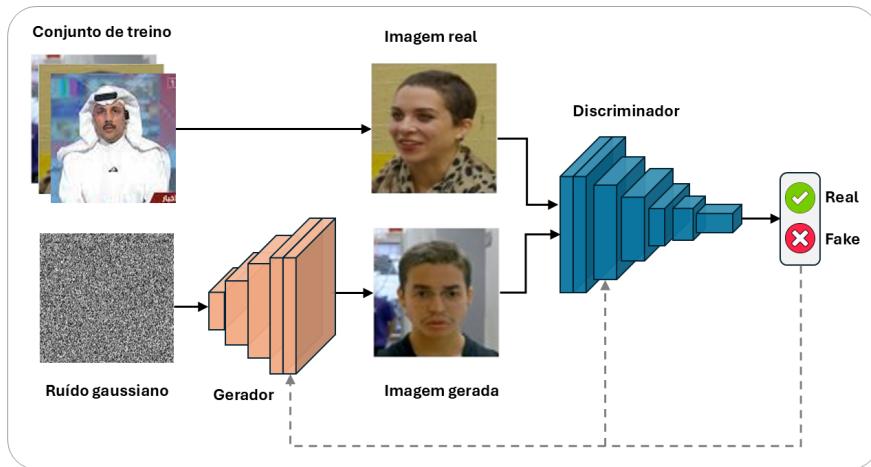


Figura 2. Esquema de treinamento de uma GAN para geração de faces. O gerador cria imagens sintéticas enquanto o discriminador tenta distingui-las das reais, em um processo adversarial que leva à geração de faces mais realistas.

de inferência, decorrentes das múltiplas etapas de denoising exigidas para gerar amostras de alta fidelidade [Bishop e Bishop, 2024; Shen et al., 2025].

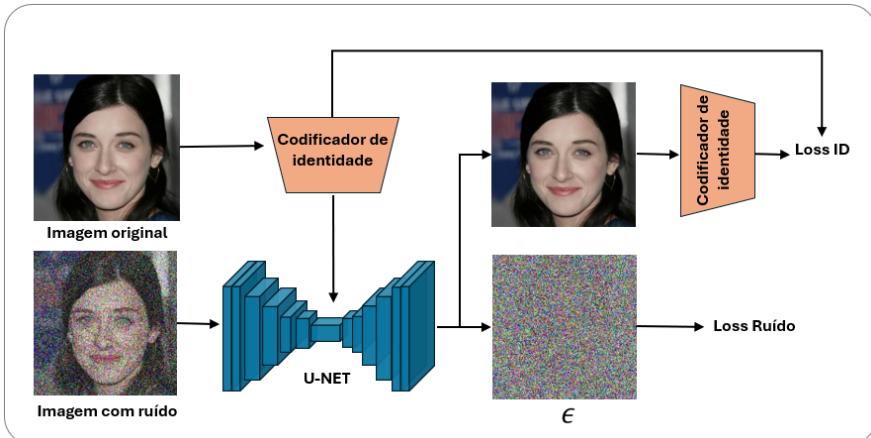


Figura 3. Esquema de treinamento do DiffFace. Um codificador de identidade insere atributos no espaço latente da U-Net, que aprende a reconstruir rostos a partir de imagens ruidosas. As perdas de ruído e identidade orientam o ajuste dos pesos. Adaptado de Kim et al. [2025].

3. Panorama dos Métodos de Detecção

Diversas abordagens têm sido propostas para a detecção de deepfakes, geralmente classificadas em três categorias [Moura, 2021]: (i) métodos baseados em inconsistências físicas, (ii) abordagens orientadas por dados, e (iii) técnicas focadas em artefatos de síntese. Neste trabalho, introduzimos uma quarta categoria – (iv) *métodos híbridos*, que combinam múltiplas estratégias.

3.1. Inconsistências Físicas

Deepfakes frequentemente introduzem discrepâncias fisiológicas sutis que, embora imperceptíveis a olho nu, podem ser exploradas para sua detecção. Entre essas anomalias

lias, destacam-se padrões irregulares no piscar dos olhos, inconsistentes na taxa de batimentos cardíacos inferidas pela coloração da pele, e movimentos labiais dessincronizados em relação ao áudio. Abordagens como a proposta por Li et al. [2018] utilizaram CNNs combinadas com redes neurais recorrentes (RNNs, do inglês *Recurrent Neural Networks*), formando uma arquitetura denominada LRCN (*Long-term Recurrent Convolutional Network*), para capturar tanto as correlações espaciais – associadas ao estado de abertura dos olhos – quanto as dinâmicas temporais ao longo de sequências de vídeo.

Avançando na análise espaço-temporal, Hernandez-Ortega et al. [2022] propuseram a detecção de deepfakes baseada em variações sutis de coloração facial, associadas ao fluxo sanguíneo. A abordagem utiliza uma técnica de fotopletismografia remota para identificar padrões de pulsação natural que estão ausentes ou apresentam inconsistências temporais em mídias sintéticas.

Ainda nesta categoria, métodos multimodais têm explorado a dessincronização entre as modalidades visual e auditiva como um indício de manipulação. Zhou e Lim [2021] propuseram a integração de *embeddings* extraídos de quadros faciais e espectrogramas de áudio por meio de mecanismos de atenção cruzada, possibilitando a detecção de inconsistências entre os movimentos labiais e o conteúdo sonoro. Esses avanços evidenciam que a análise de sinais fisiológicos e sua coerência temporal desempenha um papel fundamental na melhoria da eficácia dos sistemas de detecção.

3.2. Modelos Orientados por Dados

Nesta categoria, redes neurais profundas – comumente CNNs e redes de memória de curto e longo prazo (LSTM, do inglês *Long Short-Term Memory*) – são treinadas diretamente em grandes volumes de dados reais e sintéticos. Um exemplo recente é o trabalho de Ezeakunne et al. [2024], que propuseram a geração de amostras auto-misturadas para compor conjuntos de dados com maior diversidade demográfica, favorecendo a robustez do modelo frente a diferentes perfis populacionais. A arquitetura adotada utiliza a EfficientNet [Tan e Le, 2019] como extratora de características e dois classificadores do tipo perceptron multcamada (MLP, do inglês *Multi-Layer Perceptron*): um para a detecção binária de deepfakes e outro para a predição do grupo demográfico. O treinamento é conduzido de forma multi-tarefa, com otimização conjunta das perdas associadas a ambas as saídas, promovendo o aprendizado de representações discriminativas menos sensíveis a variações demográficas.

Um segundo exemplo é a CLRNet [Tariq et al., 2021], que utiliza uma arquitetura baseada em uma rede convolucional residual acoplada a células LSTM, capazes de capturar simultaneamente padrões espaciais e temporais em sequências de vídeo. Explorando diferentes estratégias de treinamento, como aprendizado em domínio único, fusão de domínios e transferência de aprendizado, a CLRNet demonstrou alta capacidade de generalização, mesmo frente a conjuntos de dados desafiadores como o DeepFake-in-the-Wild [Zi et al., 2020].

Mais recentemente, esta categoria passou a contar com abordagens de detecção baseadas em aprendizado não supervisionado. Nesta perspectiva, Diniz e Rocha [2024] propuseram uma abordagem de detecção open-set, onde apenas amostras genuínas são usadas no treinamento. Para facilitar a separação entre padrões reais e falsificados no espaço latente, foi aplicada a função de perda triplet loss [Schroff et al., 2015] com mi-

neração de exemplos difíceis. Utilizando classificadores leves, como One-Class SVM, Isolation Forest e Extreme Value Machine, o método alcançou AUC superior a 0,80, sem exposição prévia a exemplos falsificados.

3.3. Detecção por Artefatos

A geração sintética comumente introduz artefatos específicos, como distorções, desfoques ou padrões anômalos em domínios freqüenciais – sinais que podem ser explorados por métodos de detecção. O método FWA (*Face Warping Artifacts*), proposto por [Li e Lyu, 2019], por exemplo, explora deformações faciais decorrentes da etapa final de redimensionamento aplicada às faces sintetizadas. Essa operação, utilizada para alinhar a face gerada ao rosto-alvo, gera inconsistências de resolução entre a região facial e as áreas adjacentes. Para detectar tais artefatos, o FWA emprega CNNs treinadas com dados sintéticos obtidos por meio de simples transformações geométricas, dispensando o uso de exemplos negativos (deepfakes) durante o treinamento.

Outra abordagem de detecção por artefatos atua no domínio da frequência, utilizando transformadas espectrais para capturar padrões sutis introduzidos durante o processo de síntese. Giudice et al. [2021] propuseram a técnica CTF-DCT (*Capture The Fake via Discrete Cosine Transform*), que identifica assinaturas específicas de redes geradoras – denominadas Frequências Específicas de GAN – por meio da análise da distribuição dos coeficientes AC da Transformada Discreta do Cosseno (DCT, do inglês *Discrete Cosine Transform*) aplicada a blocos de 8×8 pixels. A abordagem estima estatísticas baseadas em distribuições Laplacianas para detectar anomalias de forma robusta, mesmo na presença de perturbações como compressão JPEG, espelhamento ou rotação.

Com o avanço dos modelos de difusão [Shen et al., 2025], tornaram-se necessárias novas abordagens para detectar artefatos mais refinados. O método Synthbuster [Bammey, 2024] introduz uma metodologia baseada em análise espectral de resíduos de alta frequência. Inicialmente, é aplicado um filtro de diferença cruzada para ressaltar componentes de alta frequência, seguido da análise da Transformada Rápida de Fourier (FFT, do inglês *Fast Fourier Transform*) para extrair magnitudes específicas associadas a períodos de 2, 4 e 8 pixels – padrões característicos da etapa de amostragem e *upsampling* dos modelos de difusão. Assim, um classificador leve baseado em *Gradient Boosting Trees* é então treinado apenas utilizando os picos de magnitude extraídos, alcançando alta acurácia mesmo em imagens comprimidas e demonstrando capacidade de generalização para modelos de geração não vistos durante o treinamento.

3.4. Métodos Híbridos

Métodos híbridos de detecção de deepfakes têm sido desenvolvidos com o objetivo de combinar os pontos fortes de diferentes abordagens, resultando em modelos mais resilientes. O método FrePGAN [Jeong et al., 2022], por exemplo, utiliza GANs para aplicar perturbações no domínio da frequência em ambas as classes (real e fake) durante o treinamento, reduzindo o *overfitting* a artefatos específicos de determinados geradores. De forma complementar, o FreqNET [Tan et al., 2024] propõe um módulo integrado de aprendizado no domínio espacial e espectral, baseado em uma camada convolucional de Fourier, projetada para capturar tanto a distribuição de magnitude quanto de fase das componentes da Transformada de Fourier, demonstrando alta eficácia na detecção de mídias sintéticas geradas por 17 tipos distintos de GANs.

Outro exemplo relevante é o método OSDFD [Kong et al., 2024] que emprega uma arquitetura baseada em Transformers visuais (ViT), combinada com LoRA – uma técnica leve de ajuste fino que reduz os custos de adaptação de grandes modelos. O método incorpora ainda a estratégia de mistura de estilos de falsificação (*forgery style mixture*), promovendo maior diversidade no espaço latente durante o treinamento e aprimorando a capacidade do detector de lidar com técnicas de falsificação inéditas. Esses avanços ilustram o potencial das abordagens combinatórias na construção de detectores de deepfakes mais robustos e generalizáveis.

4. Métodos de Prevenção a Deepfakes

Além das estratégias de detecção discutidas neste trabalho, também foram propostas abordagens preventivas contra o uso malicioso de deepfakes. Uma das mais exploradas é a *deepfake destruction*, que insere perturbações cuidadosamente calculadas nas imagens para desestabilizar o processo de geração, impedindo a criação eficaz de falsificações [Ruiz et al., 2020]. Outra linha promissora é a *scapegoat generation* [Kato et al., 2023], que modifica adversarialmente o rosto original com o objetivo de produzir uma imagem reconhecível pelo usuário como um avatar, mas com identidade suficientemente alterada para inviabilizar sua utilização por modelos de síntese.

Mais recentemente, destacam-se iniciativas de marcação digital invisível, como o SynthID, desenvolvido pelo Google DeepMind para embutir marcas d'água imperceptíveis em conteúdos gerados por IA. Em parceria com a NVIDIA, o SynthID passou a ser integrado aos modelos generativos na plataforma build.nvidia.com, ampliando sua aplicação a diferentes ecossistemas de IA [Google, 2025]. Essas estratégias reforçam a importância de uma abordagem integrada que combine prevenção e detecção, a fim de mitigar os impactos sociais e informacionais dos deepfakes em escala.

5. Confiabilidade na Detecção de Deepfakes

Apesar dos avanços recentes nos mecanismos de defesa, os métodos de detecção ainda estão longe de alcançar um desempenho confiável em cenários não controlados [Wang et al., 2024a]. Muitos modelos apresentam resultados expressivos em ambientes laboratoriais, mas demonstram queda de desempenho ao lidar com dados provenientes de diferentes origens, resoluções ou técnicas de manipulação [Pei et al., 2024].

Mais do que considerar métricas isoladas, como acurácia ou AUC, é fundamental avaliar a confiabilidade dos detectores, entendida como a capacidade de manter um desempenho estável e robusto em condições variadas. Conforme proposto por Wang et al. [2024a], três pilares centrais orientam essa avaliação: transferibilidade, robustez e interpretabilidade. Neste trabalho, propomos inclusão de um quarto pilar, a *eficiência computacional*, visando contemplar também a viabilidade prática dos modelos em ambientes com restrições de tempo e recursos.

Esses quatro pilares fornecem uma base abrangente para uma avaliação alinhada com cenários realistas, permitindo que os modelos de detecção sejam analisados não apenas em termos de precisão, mas também sob outras dimensões cruciais de confiabilidade.

5.1. Transferibilidade

Transferibilidade refere-se à capacidade dos modelos de generalizarem para dados não vistos, especialmente aqueles gerados por técnicas diferentes daquelas utilizadas durante

o treinamento [Abdullah et al., 2024; Wang et al., 2024a]. Detectores que dependem fortemente de artefatos específicos dos conjuntos de dados tendem a sofrer quedas significativas de desempenho em cenários de avaliação entre datasets distintos (*cross-dataset*) [Abdullah et al., 2024]. Para mitigar esse problema, têm sido exploradas estratégias como o aumento de dados com mapas de perturbação [Jeong et al., 2022] e a mistura de estilos entre diferentes tipos de deepfakes [Kong et al., 2024]. Embora esses métodos apresentem resultados promissores, eles ainda se mostram insuficientes para assegurar uma transferibilidade ampla e consistente.

5.2. Robustez

Robustez diz respeito à capacidade do modelo de manter seu desempenho diante de perturbações naturais ou artificiais, como compressão, ruídos, distorções ou ataques adversariais [Wang et al., 2024a]. Estudos mostram que detectores treinados em condições ideais tendem a sofrer quedas significativas de desempenho quando expostos a cenários de baixa qualidade ou manipulações maliciosas. Abdullah et al. [2024], por exemplo, avaliaram oito métodos de detecção sob ataques adversariais baseados em gradiente aplicados diretamente à entrada, evidenciando a fragilidade de todos os modelos frente a esse tipo de perturbação. Em resposta, exploram-se estratégias como o treinamento com dados degradados [Jeong et al., 2022], o uso de representações mais robustas [Kong et al., 2024], e o desenvolvimento de arquiteturas mais resilientes à compressão [Kundu et al., 2025].

5.3. Interpretabilidade

A interpretabilidade é essencial em contextos críticos, como segurança, processos jurídicos e perícia digital [Wang et al., 2024a]. Nesse contexto, ela diz respeito à capacidade de explicar e justificar as decisões tomadas por um algoritmo – por exemplo, apontar que uma imagem foi classificada como falsa devido à presença de artefatos anômalos em determinadas regiões, como bordas borradas ou padrões de iluminação inconsistentes [Trinh et al., 2021]. Modelos de detecção baseados em redes neurais profundas, por exemplo, são frequentemente criticados por sua natureza de “caixa-preta”, pois não oferecem uma compreensão clara dos fatores que motivaram determinada decisão [Pedulla, 2022].

Nesta direção, algumas abordagens têm explorado o uso de mapas de saliência [Pontorno et al., 2024] e análises espectrais [Bammey, 2024] para explicar o comportamento dos modelos. No entanto, essas soluções ainda enfrentam desafios relacionados à clareza, consistência e padronização das explicações fornecidas. Um dos métodos mais promissores em termos de interpretabilidade foi proposto por Kundu et al. [2025], que utilizaram uma arquitetura multimodal baseada em modelos de linguagem natural para gerar explicações em linguagem humana sobre as decisões de classificação.

5.4. Eficiência Computacional

Eficiência computacional envolve a capacidade de realizar inferências rápidas com uso moderado de recursos, aspecto fundamental para aplicações em tempo real ou em dispositivos com restrições de hardware [Wang et al., 2024b]. No entanto, detectores de alta capacidade, baseados em transformers [Kong et al., 2024; Kundu et al., 2025] ou ensembles [Zhou e Lim, 2021], frequentemente demandam alto poder computacional. Dessa forma, arquiteturas neurais mais leves, como no método proposto por Luo et al. [2024], que utiliza a EfficientNet-B4 como classificador, buscam equilibrar capacidade de classificação e eficiência computacional.

6. Proposta de Framework de Avaliação

A aplicação prática de detectores de deepfakes exige mais do que alta acurácia em ambientes controlados – requer também confiabilidade sob diferentes condições e restrições operacionais [Wang et al., 2024a]. Embora a maioria dos métodos citados neste trabalho concentrem suas avaliações em métricas tradicionais, como o desempenho em testes *cross-dataset* e eventuais avaliações de robustez, aspectos críticos como interpretabilidade e eficiência computacional permanecem, em grande parte, negligenciados.

Com base nessa lacuna, propomos um framework de avaliação estruturado nos quatro pilares fundamentais: transferibilidade, robustez, interpretabilidade e eficiência computacional, conforme detalhado na seção anterior. Diferentemente de abordagens existentes, nossa proposta oferece uma *quantificação formal e integrada* desses quatro pilares, permitindo comparar modelos sob uma perspectiva multidimensional de confiabilidade. A Figura 4 ilustra a distinção entre a abordagem tradicional de avaliação e a metodologia abrangente aqui proposta.

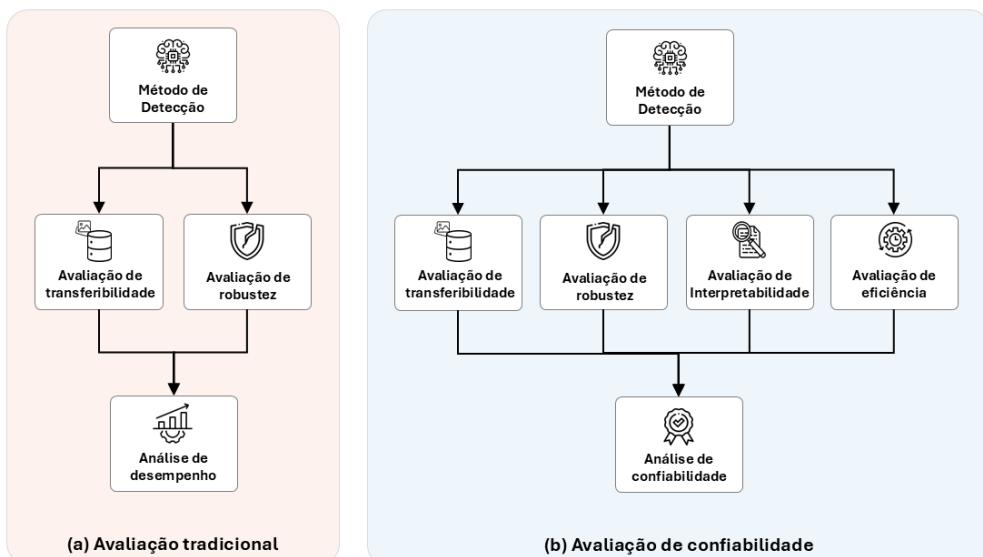


Figura 4. Comparação entre (a) a abordagem tradicional de avaliação de detectores de deepfakes, centrada apenas em métricas de desempenho e robustez, e (b) o framework proposto neste trabalho, que incorpora e quantifica os quatro pilares da confiabilidade.

Cada pilar é mensurado por métricas específicas e complementares. Para os dois primeiros (transferibilidade e robustez) optamos por permitir o uso de AUC ou ACC, dada a ausência de consenso na literatura. Essa escolha visa compatibilidade entre diferentes práticas experimentais, mantendo a comparabilidade entre métodos.

A **transferibilidade** é avaliada pela média da AUC ou ACC obtida em testes *cross-dataset*, refletindo a capacidade do modelo de generalizar para dados oriundos de diferentes técnicas e domínios. Formalmente, seja N o número de conjuntos de dados não vistos usados nos testes, a métrica de transferibilidade T é definida pela Equação 1:

$$T = \frac{1}{N} \sum_{i=1}^N \text{Score}_{\text{cross}}(i). \quad (1)$$

De forma análoga, a **robustez** considera o desempenho médio do modelo frente a três categorias de perturbações: compressão, ruído e ataques adversariais. Para garantir uma avaliação equilibrada entre esses tipos de degradação, a métrica de robustez R é definida como a média das médias obtidas em cada grupo de testes, conforme a Equação 2:

$$R = \frac{1}{3} \left(\frac{1}{C} \sum_{i=1}^C \text{Score}_{\text{comp}}(i) + \frac{1}{P} \sum_{j=1}^P \text{Score}_{\text{perturb}}(j) + \frac{1}{A} \sum_{k=1}^A \text{Score}_{\text{adv}}(k) \right), \quad (2)$$

onde:

- C , P e A representam, respectivamente, o número de testes realizados sob compressão, perturbações com ruídos, e ataques adversariais;
- $\text{Score}_{\text{comp}}(i)$ é a AUC ou ACC obtida no i -ésimo teste com compressão;
- $\text{Score}_{\text{perturb}}(j)$ é a AUC ou ACC obtida no j -ésimo teste com perturbações por ruídos;
- $\text{Score}_{\text{adv}}(k)$ é a AUC ou ACC obtida no k -ésimo teste com ataque adversarial.

A **interpretabilidade** é quantificada segundo uma escala qualitativa, apresentada na Tabela 1, que atribui valores de 0 a 1 com base no grau de profundidade e na integração dos mecanismos explicativos ao modelo.

Tabela 1. Critérios de quantificação para interpretabilidade.

Critério	Valor	Descrição
Nenhuma explicação	0.0	Modelo “caixa-preta”, sem qualquer visualização ou justificativa.
Visualizações básicas	0.3 – 0.5	Uso de técnicas como Grad-CAM (mapas de saliência) ou t-SNE, sem análise crítica.
Análises interpretativas	0.6 – 0.8	Aplicação de métodos como LIME ou SHAP, com explicações baseadas em atributos.
Explicabilidade integrada	0.9 – 1.0	Mecanismos explicativos integrados ao modelo

A **eficiência computacional** é avaliada com base no número total de parâmetros do modelo (P), por ser um indicador atrelado ao custo de inferência e uso de recursos computacionais [Wang et al., 2024b]. Essa escolha se justifica por dois fatores: (i) a ausência de código disponibilizado publicamente para os métodos analisados, o que inviabiliza medições consistentes de tempo de inferência; e (ii) a correlação entre P e variáveis como consumo de memória, latência e viabilidade de execução em tempo real.

A atribuição de escores segue a escala discretizada apresentada a seguir:

$$E = \begin{cases} 1.0, & \text{se } P < 10^7 \\ 0.8, & \text{se } 10^7 \leq P < 5 \times 10^7 \\ 0.6, & \text{se } 5 \times 10^7 \leq P < 10^8 \\ 0.4, & \text{se } 10^8 \leq P < 3 \times 10^8 \\ 0.2, & \text{se } 3 \times 10^8 \leq P < 10^9 \\ 0.0, & \text{se } P \geq 10^9 \end{cases} \quad (3)$$

O Algoritmo 1 formaliza o cálculo do escore de confiabilidade global (*SCG*) a partir dos quatro pilares definidos no framework. Cada dimensão é incorporada de maneira padronizada, permitindo a integração com sistemas automatizados de avaliação. Com exceção do pilar de interpretabilidade, que ainda depende de uma classificação manual (ver Tabela 1), os demais pilares podem ser computados de forma objetiva a partir dos resultados experimentais.

Algoritmo 1 Cálculo do Escore de Confiabilidade Global (*SCG*)

Require:

D : conjunto de datasets não vistos
 $P_{\text{comp}}, P_{\text{perturb}}, P_{\text{adv}}$: AUC ou ACC obtidas nos testes de robustez
 P : número total de parâmetros do modelo
 I : escore qualitativo de interpretabilidade (ver Tabela 1)

Ensure: Escore de confiabilidade global $SCG \in [0, 1]$

```

1: function CALCULARTRANSFERIBILIDADE( $D$ )
2:   return  $T = \frac{1}{|D|} \sum_{i=1}^{|D|} \text{Score}_{\text{cross}}(i)$  ▷ Equação 1
3: end function

4: function CALCULARROBUSTEZ( $P_{\text{comp}}, P_{\text{perturb}}, P_{\text{adv}}$ )
5:   return  $R = \frac{1}{3} \left( \frac{1}{C} \sum_{i=1}^C \text{Score}_{\text{comp}}(i) + \frac{1}{P} \sum_{j=1}^P \text{Score}_{\text{perturb}}(j) + \frac{1}{A} \sum_{k=1}^A \text{Score}_{\text{adv}}(k) \right)$  ▷ Equação 2
6: end function

7: function CALCULAREFICIÊNCIA( $P$ )
8:   return  $E$  conforme a escala definida na Equação 3
9: end function

10: function CALCULARCONFIABILIDADE( $D, P_{\text{comp}}, P_{\text{perturb}}, P_{\text{adv}}, I, P$ )
11:    $T \leftarrow \text{CALCULARTRANSFERIBILIDADE}(D)$ 
12:    $R \leftarrow \text{CALCULARROBUSTEZ}(P_{\text{comp}}, P_{\text{perturb}}, P_{\text{adv}})$ 
13:    $E \leftarrow \text{CALCULAREFICIÊNCIA}(P)$ 
14:    $SCG \leftarrow \frac{1}{4}(T + R + I + E)$ 
15:   return  $SCG$ 
16: end function

```

7. Estudo de Casos: Avaliação de Métodos do Estado da Arte

Com base no framework proposto, analisamos cinco métodos recentes de detecção de deepfakes à luz dos pilares de confiabilidade. A seleção considerou: (i) o desempenho reportado em cenários *cross-dataset*, como indicador da capacidade de generalização; e (ii) a avaliação sob condições degradadas, como compressão e ruído, evidenciando testes mínimos de robustez.

Para cada método, extraímos os valores de desempenho reportados em cenários *cross-dataset* e sob perturbações (compressão, ruído e ataques adversariais), priorizando AUC ou ACC, conforme a disponibilidade. Quando múltiplos testes estavam presentes, utilizamos a média aritmética, assegurando a comparabilidade. A partir disso, calculamos os escores de transferibilidade (T) e robustez (R) conforme as Equações 1 e 2.

O valor de interpretabilidade (I) foi atribuído manualmente com base na presença, natureza e integração das explicações fornecidas, seguindo os critérios da Tabela 1.

A eficiência computacional (E) foi estimada com base no número de parâmetros (P). Quando não informado, P foi inferido a partir do modelo base utilizado na arquitetura (por exemplo, DINoV2 e PaliGemma2).

Com todos os pilares quantificados, o escore de confiabilidade global (SCG) foi calculado conforme o Algoritmo 1, permitindo uma avaliação mais padronizada diante da heterogeneidade dos protocolos originais.

O FrePGAN [Jeong et al., 2022] é um método voltado à detecção de deepfakes gerados por GANs, com foco na mitigação de *overfitting* por meio da aplicação de mapas de perturbação no domínio da frequência. Apresenta boa transferibilidade, com desempenho estável em múltiplos domínios, alcançando uma acurácia média de 0,76 em conjuntos de dados não vistos. Também exibe robustez frente a compressão e ruído, mas não foi avaliado contra ataques adversariais, limitando sua análise completa. A interpretabilidade é considerada baixa, uma vez que não oferece explicações claras além dos mapas especiais. Quanto à eficiência computacional, o uso da arquitetura ResNet-50 combinada a um gerador adicional sugere um custo moderado.

O SCLoRA [Kong et al., 2023] utiliza uma arquitetura ViT combinada com LoRA e a função *Single-Center Loss* para promover a separação entre classes. Apresentou transferibilidade intermediária, com AUC média de 0,72, superando modelos baseados exclusivamente em ViTs. Em termos de robustez, demonstrou desempenho consistente sob diferentes níveis de compressão (fatores c23 e c40), que simulam perdas de qualidade típicas de vídeos em redes sociais – sendo c23 associado a compressão moderada e c40 a compressão severa, segundo o padrão do conjunto de dados FaceForensics++ [Rössler et al., 2019]. Por outro lado, o modelo não foi submetido a avaliações contra ataques adversariais, o que limita a análise de sua resiliência em cenários mais hostis. Assim como o método anterior, carece de interpretabilidade estruturada, operando como um modelo caixa-preta. Apesar do uso eficiente do LoRA, o backbone com 86M de parâmetros resulta em um custo computacional elevado durante a inferência.

O OSDFD [Kong et al., 2024] combina uma arquitetura ViT com módulos eficientes (Adapter + LoRA) e técnicas de mistura de estilos de falsificação para promover maior capacidade de generalização. Alcançou AUC média de 0,82 em seis conjuntos de dados não vistos, destacando-se em termos de transferibilidade. Quanto à robustez, apresentou bons resultados sob diferentes níveis de compressão e perturbações, embora não tenha sido avaliado frente a ataques adversariais. Sua explicabilidade é limitada, baseada apenas no Grad-CAM [Selvaraju et al., 2017], que destaca as regiões da imagem mais relevantes para a decisão do modelo, e no t-SNE [van der Maaten e Hinton, 2008], utilizado para projetar representações internas em duas dimensões, facilitando a visualização da separação entre classes. O modelo é relativamente leve no treinamento, com 1,34M de parâmetros ajustáveis, mas sua dependência de um backbone com 83M de parâmetros pode impactar negativamente o desempenho na fase de inferência.

O CFM [Luo et al., 2024] adota *triplet learning* e mineração de amostras críticas para fomentar representações discriminativas e agnósticas ao domínio. Alcançou alta transferibilidade, com AUC média de 0,84, e demonstrou robustez notável, apresentando uma queda média de apenas 3,71% em sete tipos de perturbações visuais. Sua explicabilidade, assim como nos métodos anteriores, é limitada ao uso de Grad-CAM. Em termos de

eficiência, a utilização de dois *encoders* e amostragem por *triplets* tende a elevar o custo computacional; no entanto, o uso do backbone EfficientNet-B4, com aproximadamente 19M de parâmetros, contribui para manter uma eficiência moderada.

O *TruthLens* [Kundu et al., 2025] se destaca por adotar uma abordagem multimodal, combinando o modelo visual DINOv2 com o LLM PaliGemma2 para gerar explicações em linguagem natural. Alcançou acurácia média de 0,94 em três conjuntos de dados não vistos, evidenciando alto desempenho em termos de transferibilidade. No entanto, sua avaliação de robustez foi limitada a cenários com compressão. É o único método analisado com explicabilidade integrada, validada por métricas de linguagem como BLEU e ROUGE. Quanto à eficiência, o uso combinado de dois modelos fundacionais de grande porte impõe elevada complexidade computacional, o que pode limitar sua aplicação em tempo real ou em sistemas de larga escala.

A Tabela 2 apresenta os valores de robustez R calculados para cada método, conforme a Equação 2. A métrica considera as médias de AUC ou acurácia dos detectores sob três tipos de perturbações: compressão ($Score_{comp}$), ruído ($Score_{perturb}$) e ataques adversariais ($Score_{adv}$). Nos casos em que os testes não foram realizados, o valor 0 foi adotado.

Tabela 2. Comparação dos métodos quanto aos fatores de robustez.

Método	Métrica	$Score_{comp}$	$Score_{perturb}$	$Score_{adv}$	R
SCLoRA	AUC	0,70	0,0	0,0	0,23
OSDFD	AUC	0,79	0,87	0,0	0,55
CFM	AUC	0,93	0,80	0,0	0,58
FrePGAN	Acurácia	0,99	0,97	0,0	0,65
TruthLens	Acurácia	0,94	0,0	0,0	0,31

A Tabela 3 consolida os escores de confiabilidade global (SCG), calculados conforme o Algoritmo 1, bem como os valores individuais obtidos por cada método nos quatro pilares que compõem o framework: transferibilidade (T), robustez (R), interpretabilidade (I) e eficiência computacional (E).

Tabela 3. Comparação dos métodos em relação aos pilares de confiabilidade.

Método	Métrica	T	R	I	E	SCG
OSDFD	AUC	0,82	0,55	0,50	0,62	0,62
SCLoRA	AUC	0,72	0,23	0,20	0,60	0,44
CFM	AUC	0,84	0,58	0,50	0,80	0,68
FrePGAN	Acurácia	0,76	0,65	0,30	0,58	0,57
TruthLens	Acurácia	0,94	0,31	1,00	0,00	0,56

7.1. Discussão

A análise comparativa dos cinco métodos avaliados revela avanços significativos na detecção de deepfakes, mas também expõe fragilidades estruturais recorrentes, especialmente à luz dos quatro pilares de confiabilidade. Apesar da *transferibilidade* ter se tornado um foco crescente em abordagens recentes, com modelos como TruthLens e CFM alcançando acurácia média superior a 88% em conjuntos de dados não vistos, observa-se uma persistente dependência de características específicas dos dados de treinamento, o que ainda limita a generalização plena desses métodos em cenários abertos.

No que diz respeito à *robustez*, a maioria dos métodos avaliou seu desempenho frente a perturbações como compressão e ruído; no entanto, nenhum dos cinco métodos contemplou testes contra ataques adversariais – uma lacuna crítica apontada por Abdullah et al. [2024], sobretudo em contextos de segurança. Mesmo modelos com bom desempenho sob perturbações convencionais, como o FrePGAN e o CFM, ainda demonstram vulnerabilidade potencial diante desse tipo de ameaça.

O pilar da *interpretabilidade* apresenta disparidades ainda mais acentuadas. Dentro os métodos avaliados, apenas o TruthLens incorpora um mecanismo explicativo integrado ao processo decisório, fornecendo descrições textuais que justificam a detecção. Os demais métodos, quando oferecem alguma forma de explication, limitam-se a visualizações básicas com técnicas como Grad-CAM ou t-SNE, sem uma análise interpretativa mais profunda. Essa ausência de mecanismos explicativos pode comprometer a adoção de detectores em contextos forenses e jurídicos, nos quais as decisões precisam ser justificáveis e passíveis de auditoria [Wang et al., 2024a].

Com relação à *eficiência computacional*, observa-se um trade-off recorrente: modelos altamente explicáveis (como o TruthLens) ou com forte capacidade de generalização (como o OSDFD) apresentam elevado custo de inferência, em razão do uso de arquiteturas fundacionais ou transformers de grande porte. Entre os métodos avaliados, apenas o CFM demonstra um equilíbrio razoável entre desempenho, robustez e eficiência, adotando um backbone intermediário com aproximadamente 19M de parâmetros.

Embora este trabalho forneça um panorama abrangente, reconhece-se que a comparação entre os métodos pode ser influenciada pela diversidade dos datasets utilizados nos experimentos originais e pela variação no número e tipo de testes de robustez realizados. Essa limitação evidencia a necessidade de métricas padronizadas para avaliação da confiabilidade, que vão além de indicadores tradicionais como acurácia ou AUC, mas que incorporem uma visão mais ampla e multidimensional da confiabilidade dos modelos.

8. Conclusões

Este trabalho apresentou uma análise crítica da confiabilidade de detectores de deepfakes, propondo um framework de avaliação baseado em quatro pilares fundamentais: transferibilidade, robustez, interpretabilidade e eficiência computacional. A aplicação desse framework a cinco métodos do estado da arte permitiu identificar avanços relevantes, especialmente na capacidade de generalização para dados não vistos e na mitigação de artefatos de geração específicos. Ainda assim, persistem limitações estruturais que comprometem a adoção confiável desses detectores em cenários reais.

Entre os principais desafios identificados está a carência de testes contra ataques adversariais, o que fragiliza a robustez dos modelos diante de ameaças propositalmente elaboradas para “enganá-los”. A interpretabilidade também permanece como um gargalo considerável, com apenas um dos métodos avaliados oferecendo explicações integradas em linguagem natural. Quanto à eficiência computacional, observou-se um trade-off entre complexidade e desempenho, que pode limitar a aplicabilidade dos modelos em tempo real ou em dispositivos com restrições de hardware.

Como próximos passos, propõe-se a ampliação do número de modelos analisados, com a reprodução dos experimentos em um ambiente padronizado, utilizando os mesmos

conjuntos de dados, protocolos de teste e métricas de avaliação. Acreditamos que essa padronização permitirá comparações mais justas entre os métodos e favorecerá o desenvolvimento de detectores realmente confiáveis, transparentes e acessíveis.

Agradecimentos

Este trabalho foi financiado com recursos do Programa de Excelência Acadêmica (PROEX) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) – Brasil. Agradecemos o apoio institucional, essencial tanto para a participação no evento quanto para o desenvolvimento desta pesquisa.

Referências

- Abdullah, S. M., Cheruvu, A., Kanchi, S., Chung, T., Gao, P., Jadliwala, M. O., e Viswanath, B. (2024). Deepfake detection: Challenges in the age of custom generative models and adversarial attacks. <https://paperswithcode.com/research/deepfake-detection-evolving-challenges>. Papers with Code.
- Bammey, Q. (2024). Synthbuster: Towards detection of diffusion model generated images. *IEEE Open Journal of Signal Processing*, 5:1–9.
- Bishop, C. M. e Bishop, H. (2024). *Deep Learning: Foundations and Concepts*. Springer Nature.
- Caporusso, N. (2021). Deepfakes for the good: A beneficial application of contentious artificial intelligence technology. In *International Conference on Applied Human Factors and Ergonomics*, pages 235–241.
- Chen, R. et al. (2020). SimSwap: An efficient framework for high fidelity face swapping. In *ACM International Conference on Multimedia*, page 2003–2011.
- Deepfakes (2017). Deepfakes. <https://github.com/deepfakes/>. Accessed: 2025-03-07.
- Diniz, M. M. e Rocha, A. (2024). Open-set deepfake detection to fight the unknown. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 13091–13095.
- dos Santos, M., Laroca, R., Ribeiro, R. O., Neves, J., e Menotti, D. (2024). Multi-feature aggregation in diffusion models for enhanced face super-resolution. In *Conference on Graphics, Patterns and Images (SIBGRAPI)*, pages 1–6.
- Ezeakunne, U., Eze, C., e Liu, X. (2024). Data-driven fairness generalization for deepfake detection. In *Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP)*. To appear.
- Giudice, O., Guarnera, L., e Battiato, S. (2021). Fighting deepfakes by detecting GAN DCT anomalies. *Journal of Imaging*, 7(8).
- Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., e Bengio, Y. (2014). Generative adversarial nets. In *International Conference on Neural Information Processing Systems (NeurIPS)*, page 2672–2680.
- Google, D. (2025). Synthid — deepmind’s tool for watermarking and identifying ai-generated content. Accessed: 2025-07-25.
- Hernandez-Ortega, J., Tolosana, R., Fierrez, J., e Morales, A. (2022). Deepfakes detection based on heart rate estimation: Single-and multi-frame. In *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*, pages 255–273. Springer International Publishing.

- Ho, J., Jain, A., e Abbeel, P. (2020). Denoising diffusion probabilistic models. In *International Conference on Neural Information Processing Systems*.
- Jeong, Y., Kim, D., Ro, Y., e Choi, J. (2022). FrePGAN: Robust deepfake detection using frequency-level perturbations. In *AAAI Conference on Artificial Intelligence*, pages 1060–1068.
- Karras, T., Laine, S., e Aila, T. (2021). A style-based generator architecture for generative adversarial networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(12):4217–4228.
- Kato, G., Fukuhara, Y., Isogawa, M., Tsunashima, H., Kataoka, H., e Morishima, S. (2023). Scapegoat generation for privacy protection from deepfake. arXiv:2303.02930. Available at <https://arxiv.org/abs/2303.02930>.
- Kim, K., Kim, Y., Cho, S., Seo, J., Nam, J., Lee, K., Kim, S., e Lee, K. (2025). DiffFace: Diffusion-based face swapping with facial guidance. *Pattern Recognition*, 163:111451.
- Kong, C., Li, H., e Wang, S. (2023). Enhancing general face forgery detection via vision transformer with low-rank adaptation. In *IEEE International Conference on Multimedia Information Processing and Retrieval (MIPR)*, pages 102–107.
- Kong, C., Luo, A., Bao, P., Li, H., Wan, R., Zheng, Z., Rocha, A., e Kot, A. C. (2024). Open-set deepfake detection: A parameter-efficient adaptation method with forgery style mixture. *arXiv preprint 2408.12791*.
- Kundu, R. et al. (2025). TruthLens: Explainable deepfake detection for face manipulated and fully synthetic data. *arXiv preprint arXiv:2503.15867*.
- Li, L., Bao, J., Yang, H., Chen, D., e Wen, F. (2019). Faceshifter: Towards high fidelity and occlusion aware face swapping. *arXiv preprint arXiv:1912.13457*.
- Li, Y., Chang, M.-C., e Lyu, S. (2018). In Ictu Oculi: Exposing AI created fake videos by detecting eye blinking. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–7.
- Li, Y. e Lyu, S. (2019). Exposing deepfake videos by detecting face warping artifacts. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*.
- Luo, A., Kong, C., Huang, J., Hu, Y., Kang, X., e Kot, A. C. (2024). Beyond the prior forgery knowledge: Mining critical clues for general face forgery detection. *IEEE Transactions on Information Forensics and Security*, 19:1168–1182.
- Melappalayam, R. (2024). Data-driven compliance: A new frontier for anti-bribery and anti-corruption risk programs. *Fraud Magazine*. Available at <https://www.acfe.com/fraud-magazine?id=4295023572>.
- Moura, C. S. F. T. (2021). Detecção de deepfakes a partir de técnicas de visão computacional e aprendizado de máquina. Master's thesis, Universidade Estadual de Campinas.
- Murphy, G., Ching, D., Twomey, J., e Linehan, C. (2023). Face/Off: Changing the face of movies with deepfakes. *PLoS ONE*, 18(7):e0287503.
- Pedulla, N. R. L. (2022). Interpretabilidade de modelos de aprendizagem de máquina no mercado de seguros. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro de Informática, Universidade Federal de Pernambuco.
- Pei, G. et al. (2024). Deepfake generation and detection: A benchmark and survey. *arXiv preprint arXiv:2403.17881*.
- Pontorno, O. et al. (2024). On the exploitation of DCT-traces in the generative-AI domain. In *IEEE International Conference on Image Processing (ICIP)*, pages 3806–3812.
- Roe, J., Perkins, M., e Furze, L. (2024). Deepfakes and higher education: A research agenda and scoping review of synthetic media. *Journal of University Teaching and Learning Practice*, 21(10):1–22.

- Ruiz, N., Bargal, S. A., e Sclaroff, S. (2020). Disrupting deepfakes: Adversarial attacks against conditional image translation networks and facial manipulation systems. In *European Conference on Computer Vision (ECCV)*, pages 236–251.
- Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., e Niessner, M. (2019). Faceforensics++: Learning to detect manipulated facial images. In *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 1–11.
- Schroff, F., Kalenichenko, D., e Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 815–823.
- Selvaraju, R. R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., e Batra, D. (2017). Grad-CAM: Visual explanations from deep networks via gradient-based localization. In *IEEE International Conference on Computer Vision (ICCV)*, pages 618–626.
- Sharma, S. (2024). South korean woman loses £40k in elon musk romance scam involving deepfake video. *The Independent*. Available at <https://www.independent.co.uk/asia/east-asia/elon-musk-romance-scams-dupes-south-korean-b2533764.html>.
- Shen, H. et al. (2025). Efficient diffusion models: A survey. *arXiv preprint arXiv:2502.06805*.
- Suwajanakorn, S., Seitz, S. M., e Kemelmacher-Shlizerman, I. (2017). Synthesizing Obama: Learning lip sync from audio. *ACM Transactions on Graphics*, 36(4):1–13.
- Tan, C., Zhao, Y., Wei, S., Gu, G., Liu, P., e Wei, Y. (2024). Frequency-aware deepfake detection: improving generalizability through frequency space domain learning. In *AAAI Conference on Artificial Intelligence*, pages 5052–5060.
- Tan, M. e Le, Q. (2019). EfficientNet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning*, pages 6105–6114.
- Tariq, S., Lee, S., e Woo, S. S. (2021). One detector to rule them all: Towards a general deepfake attack detection framework. In *The Web Conference (WWW)*, page 3625–3637.
- Trinh, L., Tsang, M., Rambhatla, S., e Liu, Y. (2021). Interpretable and trustworthy deepfake detection via dynamic prototypes. In *2021 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pages 1972–1982.
- van der Maaten, L. e Hinton, G. (2008). Visualizing data using t-SNE. *Journal of Machine Learning Research*, 9:2579–2605.
- Wang, T., Liao, X., Chow, K. P., Lin, X., e Wang, Y. (2024a). Deepfake detection: A comprehensive survey from the reliability perspective. *ACM Comput. Surv.*, 57(3).
- Wang, Y. et al. (2024b). Computation-efficient deep learning for computer vision: A survey. *Cybernetics and Intelligence*, pages 1–24.
- Xie, Y., Xu, H., Song, G., Wang, C., Shi, Y., e Luo, L. (2024). X-Portrait: Expressive portrait animation with hierarchical motion attention. In *SIGGRAPH 2024*.
- Zhao, W., Rao, Y., Shi, W., Liu, Z., Zhou, J., e Lu, J. (2023). DiffSwap: High-fidelity and controllable face swapping via 3D-aware masked diffusion. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 8568–8577.
- Zhou, Y. e Lim, S.-N. (2021). Joint audio-visual deepfake detection. In *IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 14780–14789.
- Zi, B., Chang, M., Chen, J., Ma, X., e Jiang, Y.-G. (2020). Wilddeepfake: A challenging real-world dataset for deepfake detection. In *Proceedings of the 28th ACM International Conference on Multimedia*, pages 2382–2390.