VisionApp: Reconhecimento Facial em Dispositivos Móveis para Segurança Pública

1st Beatriz Barreto Marreiros Barbosa
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
beatriz.barbosa@somosicev.com

2nd Anderson Araújo do Vale
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
anderson.vale@somosicev.com

3th Leonardo Jussieu Sousa Lopes
Curso de Direito
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
leonardo.lopes@somosicev.com

4rd Lucas César Soares Pereira
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
lucas_cesar.pereira@somosicev.com

5th Gustavo Araújo do Vale
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
gustavo.vale@somosicev.com

6th Cristovam Paulo de Brito Rocha
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
cristovam.rocha@somosicev.com

7th Raimundo Pereira da Cunha Neto
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
raimundo.neto@somosicev.com

8th Ricardo de Andrade Lira Rabêlo
Ciência da Computação
Universidade Federal do Piauí, UFPI
Teresina, PI, Brasil
ricardoalr@ufpi.edu.br

9th Dimmy Karson Soares Magalhães
Curso de Engenharia de Software
iCEV – Instituto de Ensino Superior
Teresina, PI, Brasil
dimmy.magalhaes@somosicev.com

***Resumo*—Este trabalho apresenta o *VisionApp*, um aplicativo móvel de reconhecimento facial para apoio a abordagens policiais, integrado a uma API *FastAPI* com *PostgreSQL/pgvector* e *MinIO*. O protótipo, desenvolvido em Flutter, foi avaliado com 48 indivíduos sob diferentes condições de imagem, obtendo acurácia global de 66%, latências abaixo de 2 s e ausência de falsos positivos, embora com maior incidência de falsos negativos em mulheres e pessoas pele preta. Uma validação com a SSP-PI confirmou a viabilidade operacional e destacou a necessidade de dados locais para reduzir vieses. Também são discutidas implicações da LGPD no tratamento de biometria. Conclui-se que o *VisionApp* é promissor como ferramenta de apoio, demandando retreinamento contínuo e expansão da base de imagens.**

***Index Terms*—Reconhecimento facial, Segurança pública, Aplicativo móvel, Visão computacional, LGPD, Viés algorítmico**

I. Introdução

A visão computacional (VC) consolidou-se como uma das engrenagens da Quarta Revolução Industrial. O volume de inovações é visível: um estudo de prospecção tecnológica identificou mais de 17.000 patentes ativas apenas em reconhecimento facial, com crescimento exponencial após 2014, impulsionado pela evolução de sensores e GPUs [1].

A visão computacional tem sido amplamente empregada na segurança pública, especialmente em países desenvolvidos como China e Estados Unidos, que lideram o desenvolvimento e a implementação dessa tecnologia. Sistemas de reconhecimento facial, por exemplo, têm se mostrado eficazes na identificação de indivíduos com pendências judiciais. No Brasil, um caso notório ocorreu durante o Carnaval de Salvador em 2019, quando o uso dessa tecnologia auxiliou na detecção e prisão de pessoas procuradas pela justiça [1].

A revisão da literatura realizada indica que a maior parte das soluções baseadas em visão computacional está voltada para o uso em câmeras de vigilância fixas, aplicadas ao monitoramento e reconhecimento de suspeitos. No entanto, como destacado por [2], esse tipo de sistema apresenta limitações importantes em termos de adaptabilidade, cobertura e tempo de reação. Diante desse cenário, o presente estudo propõe uma abordagem alternativa, explorando a aplicação da visão computacional em dispositivos móveis no contexto da segurança pública.

Conforme descrito por [3], uma abordagem policial típica envolve a sinalização de parada, a solicitação dos documentos do indivíduo e a checagem de seus antecedentes no sistema prisional. Somente após essa verificação o abordado é liberado ou conduzido à delegacia. O aplicativo proposto neste estudo tem como objetivo principal otimizar esse processo, facilitando a consulta de antecedentes criminais de forma mais ágil e eficiente. Com isso, busca-se reduzir o tempo necessário para a verificação e permitir que os policiais concentrem sua atenção em atividades mais críticas, como a segurança da cena, a contenção de suspeitos ou o atendimento a outras ocorrências.

A justificativa e relevância prática deste trabalho reside na proposta de uma solução tecnológica móvel que amplia a autonomia operacional dos agentes de segurança pública em campo, proporcionando maior agilidade, mobilidade e praticidade na consulta de antecedentes criminais diretamente no dispositivo móvel. Ao permitir consultas mais rápidas e

precisas sobre antecedentes criminais, o aplicativo desenvolvido contribui diretamente para a eficiência das abordagens policiais, reduzindo o tempo de exposição ao risco e otimizando a tomada de decisão. Do ponto de vista legal, a conformidade com a Lei Geral de Proteção de Dados (LGPD) [25] é uma prioridade na arquitetura do sistema, assegurando o tratamento responsável de dados pessoais sensíveis por meio de técnicas como criptografia, autenticação e registro seguro de acessos. Nesse sentido, o projeto se destaca por integrar inovação tecnológica, mobilidade operacional, facilidade de uso e responsabilidade legal, oferecendo uma alternativa viável e ética ao uso tradicional de sistemas fixos de vigilância.

As principais contribuições científicas deste trabalho são: (i) a proposição e implementação de um protótipo funcional de reconhecimento facial móvel para consultas de antecedentes criminais em campo; (ii) a condução de um estudo científico validado pela Secretaria de Segurança Pública do Piauí, que comprova a viabilidade operacional da abordagem; e (iii) a análise das implicações da LGPD [25] no tratamento de dados biométricos sensíveis em segurança pública.

Este trabalho está organizado da seguinte forma: a Seção II apresenta a revisão bibliográfica, a Seção III descreve o desenvolvimento do protótipo funcional, a Seção IV apresenta a validação com a Secretaria de Segurança Pública do Piauí, a Seção V discute as implicações da LGPD [25] no contexto do aplicativo e, por fim, a Seção VI expõe as conclusões e propõe trabalhos futuros.

II. Trabalhos Relacionados

Conforme discutido na introdução deste trabalho, a visão computacional, especialmente por meio do reconhecimento facial, já está em uso em diversas partes do mundo, inclusive no Brasil. Especificamente no contexto brasileiro, um mapeamento apresentado em [4] revelou que o reconhecimento facial é a terceira tecnologia mais adotada pelas 27 unidades federativas no âmbito da segurança pública, sendo superado apenas pelo uso de drones e de sistemas de reconhecimento óptico de caracteres (OCR).

Ainda de acordo com o mapeamento apresentado em [4], são descritas as diferentes formas de uso da tecnologia de reconhecimento facial nos estados brasileiros. Observa-se que, na maioria dos casos, essa tecnologia está integrada a câmeras de segurança fixas instaladas em pontos estratégicos das cidades. Um exemplo disso é o estado do Acre, que lançou o plano municipal "Rio Branco Mais Segura" em fevereiro de 2022. O projeto prevê a instalação de 430 câmeras de videomonitoramento na capital, das quais 18 contam com tecnologia de reconhecimento facial, conforme apresentado em [5] e citado por [4].

Entre os estados analisados em [4], o Amazonas é o único que, até o momento do levantamento, utilizava a tecnologia de reconhecimento facial embarcada em dispositivos móveis. Trata-se do aplicativo Copmam (Comando Operacional da Polícia Militar do Amazonas), desenvolvido sob demanda do Comandante-Geral da corporação, Ayrton Norte, e destinado exclusivamente ao uso das forças de segurança pública [6]. O aplicativo permite a identificação de foragidos diretamente pelo celular dos policiais em serviço, proposta semelhante à abordada neste trabalho. Ainda segundo [4], o Copmam encontrava-se em fase de testes em 2020, e não foram localizadas informações mais recentes que confirmem sua adoção oficial ou a continuidade de seu uso nas operações policiais.

Ainda no contexto brasileiro, em janeiro de 2025, a Polícia Civil do Estado do Rio de Janeiro anunciou o lançamento do aplicativo iPol [7], com o objetivo de facilitar a identificação de suspeitos e a consulta de informações veiculares. A ferramenta permite o retorno rápido de dados relacionados a roubo, furto e outros crimes vinculados a automóveis. O iPol foi desenvolvido pelo Departamento Geral de Tecnologia da Informação e Telecomunicações (DGTIT) e está totalmente integrado ao Sistema Integrado da Polícia Civil (Sipol), ampliando a capacidade investigativa e operacional das equipes em campo.

Em novembro de 2024, o governador do Piauí, Rafael Fonteles, anunciou o desenvolvimento do sistema Face PI, que utilizará reconhecimento facial e uma base de dados com aproximadamente 800 mil rostos de cidadãos piauienses para auxiliar na resolução de crimes [8]. O projeto ainda se encontra em fase de estudos, uma vez que, conforme declarado, "existe um limite entre o combate à criminalidade e o direito à privacidade" [8]. O algoritmo utilizado no sistema foi desenvolvido pelo próprio Núcleo de Estudos Avançados em Segurança Pública do Piauí (DataSSP), que também realizou treinamentos com dados biométricos locais com o objetivo de aprimorar a performance do modelo.

No contexto internacional, a revisão bibliográfica identificou três soluções com propostas semelhantes à deste trabalho. Um artigo publicado na revista *Discover* [9] menciona o projeto iCop, que visa transformar o iPhone em um "dispositivo de combate ao crime", utilizando reconhecimento facial e de íris para identificar criminosos. A mesma publicação também cita o sistema MORIS (*Mobile Offender Recognition and Identification System*), já em uso, que opera com tecnologia de reconhecimento facial para auxiliar agentes de segurança na identificação de indivíduos em campo.

O artigo apresentado em [10] propõe um sistema de reconhecimento facial integrado a um aplicativo móvel para identificação de criminosos, como alternativa aos métodos tradicionais, considerados lentos e imprecisos. A solução combina algoritmos avançados de reconhecimento facial, banco de dados criminal sincronizado e uma interface amigável, permitindo comparações em tempo real com alta precisão. O sistema ainda contempla protocolos de segurança para proteção dos dados e diretrizes éticas de uso. Os autores destacam o potencial da ferramenta para aumentar a agilidade e a eficácia das operações policiais.

A Tabela I apresenta uma comparação entre os aplicativos identificados na revisão da literatura e o aplicativo proposto neste estudo o *VisionApp*, considerando critérios como validação com usuários finais, uso exclusivo por forças de segurança, preocupação com proteção de dados (incluindo conformidade com a LGPD), uso de criptografia, presença

de estudos científicos associados e realização de testes de performance documentados.

Tabela I
COMPARAÇÃO ENTRE SOLUÇÕES EXISTENTES E O APLICATIVO PROPOSTO. FONTE: ELABORADO PELOS AUTORES.

Aplicativo	Critérios de Comparação					
	I	II	III	IV	V	VI
Copmam [6]	X	X				
Face PI [8]	X	X	X	X		
iPol [7]	X	X				
MORIS [9]	X	X				
iCop [9]						
Crime Identification App [10]			X	X	X	
VisionApp	X	X	X	X	X	X

I: Validado pelo usuário final - II: Uso exclusivo por forças de segurança III: Proteção de dados / LGPD - IV: Criptografia de dados V: Estudo científico associado - VI: Testes de performance no artigo

A análise da Tabela I evidencia que poucas soluções divulgam documentação científica ou métricas quantitativas. Copmam, iPol, MORIS e iCop foram aplicados em campo, mas sem estudos formais de acurácia ou latência, enquanto o Face PI permanece em fase de testes. O Crime Identification App [10] é uma das raras propostas com métricas explícitas, alcançando mais de 90% em cenários controlados. Nesse contexto, o VisionApp se diferencia ao apresentar validação prática com usuários, métricas transparentes em condições realistas e discussão legal alinhada à LGPD, contribuindo de forma original frente às soluções correlatas.

III. METODOLOGIA

Esta seção descreve em detalhes as ferramentas e procedimentos adotados no desenvolvimento do VisionApp, dividida em: (A) Ferramentas Utilizadas e (B) Arquitetura Geral do Sistema.

A. Ferramentas Utilizadas

Para o aplicativo móvel, adotou-se *Flutter* [11] (com *Dart*) e *Android Studio*, pois permitem desenvolvimento multiplataforma a partir de um único código-fonte e oferecem suporte nativo a compilação, emulação e depuração em dispositivos *Android* [12]. A autenticação e o gerenciamento de usuários ficaram a cargo do *Firebase Authentication* [13], escolhido por sua integração direta com *Flutter* e pelos mecanismos de segurança e troca de *tokens* que já vêm configurados na plataforma. Testes iniciais foram realizados tanto em emuladores quanto em aparelhos físicos, garantindo interoperabilidade em diferentes versões de *Android*.

Para a *API*, a base é *Python*, por sua sintaxe enxuta, comunidade ativa e vasta disponibilidade de bibliotecas para reconhecimento facial e segurança [14]. O *framework FastAPI* foi selecionado devido à facilidade de definir *endpoints* assíncronos, validação automática de tipos (via *Pydantic*) e documentação automática dos recursos [15]. Em produção, o servidor *Uvicorn* (integrado ao *Gunicorn* para múltiplos *workers*) foi empregado para assegurar baixo tempo de resposta e escalabilidade horizontal.

No módulo de reconhecimento facial, recorremos às bibliotecas *dlib* [20] e *face-recognition* [21] por oferecerem algoritmos de extração de vetores de representação com alta acurácia e funções simples para comparações de rostos. Para pré-processamento de imagens—detecção e alinhamento de faces utilizou-se *OpenCV*, escolhido por sua robustez nas funções de visão computacional. A manipulação básica de formatos e redimensionamento ficou a cargo do *Pillow*, por sua leveza e compatibilidade com *Python*.

Todas as comunicações entre *app* e servidor ocorrem sobre *TLS*, em conformidade com recomendações de segurança para proteger dados sensíveis em trânsito [16]. A autenticação da *API* se apoia em *tokens JWT* (*python-jose* e *PyJWT*), adotados por permitir autenticação sem estado e fácil validação em cada requisição [17]. As senhas de usuários são armazenadas mediante aplicação de função de *hash* (*bcrypt*) antes de serem persistidas, seguindo boas práticas de segurança para armazenamento de credenciais [18].

Para persistência de dados relacionais, escolheu-se *PostgreSQL* em razão de sua estabilidade, maturidade e suporte à extensão *pgvector*, essencial para armazenamento e busca de vetores de representação faciais como vetores de alta dimensão [19]. O *SQLAlchemy* foi empregado como *ORM* para simplificar o mapeamento objeto-relacional, e o *driver psycopg2-binary* para viabilizar a conexão com o banco em tempo de execução. Por fim, o *MinIO* (compatível com *API S3*) foi integrado para gerenciamento de objetos (como imagens armazenadas), evitando dependências de provedores de nuvem externos e permitindo controle total do armazenamento [22].

B. Arquitetura Geral do Sistema

O VisionApp adota uma arquitetura cliente-servidor em três camadas: (i) o Aplicativo Móvel, que captura CPF e imagem facial, autentica o usuário via *Firebase Authentication* e envia o JWT e o vetor de representação para a API; (ii) o serviço terceirizado de autenticação, que valida credenciais e emite tokens JWT sem estado; e (iii) a API, implementada em *FastAPI*, cujo ponto de entrada em *main.py* valida o JWT, pré-processa a imagem com *OpenCV*, extrai o vetor de representação facial com *face-recognition/dlib* e consulta o *PostgreSQL* para retornar a ficha criminal. O código da API está organizado em módulos: *functions/* (lógica de negócio), *crud/* (módulo responsável pelas operações CRUD — *create, read, update, delete* — que representam as ações fundamentais de inserção, consulta, atualização e exclusão de registros em tabelas como "Usuarios" e "Criminosos"), *requests/* (integrações externas, como Firebase e comparação de vetores de representação) e *config/* (conexão ao banco e modelos do *SQLAlchemy*). O serviço *MinIO* gerencia o armazenamento de imagens brutas, liberando o *PostgreSQL* para dados estruturados. Todas as comunicações ocorrem sobre *TLS*, com senhas e vetores de representação cifrados, garantindo confiabilidade, conformidade com a *LGPD* e escalabilidade horizontal.

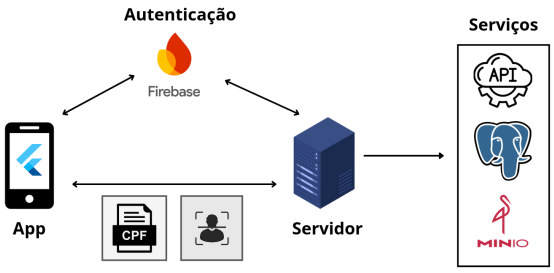

Figura 1. Arquitetura geral do VisionApp: o aplicativo móvel (Flutter) autentica o usuário via Firebase e envia CPF, imagem facial e token JWT para a API em FastAPI. O servidor realiza o pré-processamento da imagem, valida a autenticação, executa o reconhecimento facial e integra os resultados ao banco de dados (PostgreSQL) e ao armazenamento de imagens (MinIO). Fonte: Elaborado pelos autores.

IV. Resultados

O principal objetivo desta etapa foi avaliar a precisão do algoritmo de reconhecimento facial em diferentes condições de imagem. Utilizaram-se fotos de 48 indivíduos (24 homens e 24 mulheres), cada um com 9 variações de imagem: três com boa qualidade e seguindo os critérios definidos, três em resolução 480p e três com alterações intensas de iluminação. Para garantir condições adequadas ao pré-processamento e ao reconhecimento facial, definimos critérios rígidos para cada imagem: o rosto do indivíduo deve estar reto e centralizado, a expressão deve ser neutra, nenhum acessório deve obstruir pontos faciais e a resolução mínima de cada imagem deve ser de 480p para assegurar detalhes suficientes na extração de características. Inicialmente, usamos o *LFW Dataset* por ser uma base pública consagrada [24], mas constatamos que muitas imagens não atendiam à padronização exigida. Assim, foi necessário complementar esse acervo coletando imagens de bases públicas disponíveis na internet.

A. Desempenho Geral e Limitações

Observou-se desempenho reduzido quando havia variações extremas entre a imagem de referência e a de consulta, tais como diferença de idade significativa, oclusões (barba ou acessórios) e baixa iluminação, que dificultam a extração precisa dos vetores de representação faciais. Imagens borradas ou desfocadas resultaram em "Rosto não detectado na imagem". Alterações como barba densa ou rugas profundas também reduziram a acurácia.

A comparação de similaridade baseou-se na distância euclidiana entre vetores: distâncias menores que 0,4 foram classificadas como "Confiante"; entre 0,4 e 0,5 como "Ambíguo"; acima de 0,5 como "Nenhuma similaridade forte". O motivo da escolha dessa tolerância é que, nas primeiras leituras realizadas durante os testes iniciais, as distâncias euclidianas entre rostos semelhantes se concentraram nessas faixas.

B. Taxa de Sucesso e Tempo de Requisição

A Tabela II mostra a taxa de sucesso nas requisições e o tempo médio de processamento para cada intervalo de requisição (1s, 2s e 5s), considerando os dados consolidados de homens e mulheres:

Tabela II
Taxa de Sucesso e Tempo Médio por Requisição – Geral. Fonte: Elaborado pelos autores.

Intervalo	Taxa de Sucesso	Tempo Médio (s)
1 segundo	97,97%	1,629
2 segundos	97,97%	1,823
5 segundos	97,97%	1,864

A taxa de sucesso manteve-se alta (acima de 97%), sem variação significativa ao aumentar o intervalo entre requisições. No entanto, o tempo médio por requisição apresentou um leve aumento conforme o intervalo se tornava maior, o que é esperado devido ao tempo adicional de espera incorporado entre as requisições.

C. Classificações de Similaridade por Gênero e Tom de Pele

A Tabela III mostra que homens brancos e pardos mantiveram taxas "Confiante" próximas de 73-75%, enquanto homens de pele preta caíram para 47-50%, com aumento de respostas "Ambíguo" e rejeições. Entre mulheres, o desempenho geral foi inferior: brancas e pardas ficaram entre 45-51% de acerto, e de pele preta apresentaram apenas 40-42% de "Confiante" e até 19% de rejeição. Esses resultados revelam vieses interseccionais de gênero e raça, associados à sub-representação de certos grupos no treinamento. Em termos práticos, indicam maior risco de falsos negativos em populações vulneráveis, reforçando a necessidade de bases mais diversas e de técnicas de balanceamento que promovam equidade no desempenho do sistema.

Tabela III
Classificações de Similaridade por Gênero e Tom de Pele (%). Fonte: Elaborado pelos autores.

Gênero	Tom de Pele	Intervalo	Confiante	Ambíguo	Nenhuma Similaridade Forte
Homens	Pele Branca	1 s	75,25	23,38	1,38
		2 s	73,13	25,50	1,38
		5 s	73,00	24,25	2,75
	Pele Parda	1 s	75,25	23,38	1,38
		2 s	73,00	25,63	1,38
		5 s	75,25	23,38	1,38
	Pele Preta	1 s	48,50	44,75	6,75
		2 s	49,88	43,38	6,75
		5 s	47,25	44,50	8,25
Mulheres	Pele Branca	1 s	45,50	53,00	1,50
		2 s	44,75	53,88	1,38
		5 s	46,63	51,88	1,50
	Pele Parda	1 s	49,88	44,88	5,25
		2 s	51,13	42,13	6,75
		5 s	48,50	46,00	5,50
	Pele Preta	1 s	41,75	40,50	17,75
		2 s	40,38	40,50	19,13
		5 s	41,75	39,13	19,13

D. Análise de Falsos Positivos e Falsos Negativos

Para avaliar erros críticos, utilizou-se a Matriz de Confusão em 1.518 requisições de imagem: 1.296 de criminosos simulados e 222 de indivíduos não cadastrados. Entre os não cadastrados, havia 43 homens e 31 mulheres, com 3 imagens por pessoa (totalizando 129 requisições de homens inocentes e 93 de mulheres inocentes). A Tabela IV apresenta os resultados.

Tabela IV
MATRIZ DE CONFUSÃO GERAL. FONTE: ELABORADO PELOS AUTORES.

Categoria	Homens	Mulheres	Total
Verdadeiro Positivo (VP)	450	329	779
Falso Negativo (FN)	198	319	517
Verdadeiro Negativo (VN)	129	93	222
Falso Positivo (FP)	0	0	0

O algoritmo não gerou falsos positivos (FP = 0), classificando corretamente todos os 222 indivíduos inocentes (VN = 222), o que indica robustez ética e evita acusar inocentes. No entanto, houve 517 falsos negativos (39,9% do total), sendo 198 em homens e 319 em mulheres. Esse viés, especialmente elevado no público feminino, corrobora resultados de estudos como "Gender Shades" de Buolamwini e Gebru (2018) [23]. A taxa geral de acerto do sistema foi de aproximadamente 66%, considerando os verdadeiros positivos e negativos.

E. Teste com Gêmeos

Para identificar possíveis confusões em rostos muito semelhantes, adicionaram-se dois gêmeos pardos ao banco de dados. Foram feitas 24 requisições (12 para cada gêmeo). Os resultados (Tabela V) mostram que o Gêmeo A recebeu 3 classificações "Confiante" e 9 "Ambíguo", enquanto o Gêmeo B teve 0 "Confiante" e 12 "Ambíguo". Nenhum caso de "Nenhuma similaridade forte" foi registrado, indicando que o algoritmo evitou falsos positivos, mas manteve alta ambiguidade em situações de alta semelhança facial.

Tabela V
RESULTADOS DO TESTE COM GÊMEOS. FONTE: ELABORADO PELOS AUTORES.

Classificação	Gêmeo A	Gêmeo B
Confiante	3	0
Ambíguo	9	12
Nenhuma Similaridade Forte	0	0

V. DISCUSSÃO

O bom desempenho do VisionApp em condições controladas deve-se, em grande parte, ao uso de vetores de representação faciais pela biblioteca *face-recognition* [21], à arquitetura modular baseada em *FastAPI* e *PostgreSQL* que garante baixa latência nas consultas [15], [19], e à coleta rigorosa de imagens — com critérios de centralização do rosto, iluminação uniforme e resolução mínima de 480p — que favoreceu a extração precisa dos vetores faciais. Essas escolhas metodológicas explicam a taxa de acerto de 66% observada em cenários ideais. Já em imagens de baixa qualidade ou ângulos não convencionais, a acurácia caiu, evidenciando a dependência da variabilidade das amostras de treinamento. Embora inferior a resultados acima de 90% reportados em condições controladas [10], o desempenho do VisionApp reflete de forma mais realista os desafios de campo. Aplicações como MORIS [9] e Copmam [6] não divulgaram métricas consolidadas, o que reforça a contribuição deste estudo ao apresentar resultados quantitativos e destacar a necessidade de retreinamento com dados locais para maior equidade.

Por outro lado, os elevados índices de falsos negativos — especialmente entre mulheres de pele preta — reforçam a necessidade de ampliar o conjunto de treinamento com dados locais (rostos brasileiros) e diversos, contemplando diferentes características regionais e demográficas, como sugerido em estudos de viés algorítmico [23]. Essas ações são fundamentais para reduzir erros críticos e garantir que o VisionApp se mantenha uma ferramenta auxiliar confiável no apoio à decisão policial. A validação prática com a SSP-PI confirmou a viabilidade de uso em campo e a adequação da proposta ao contexto de sistemas já adotados, como o Face PI [8].

Entretanto, a qualidade do treinamento do modelo impacta diretamente sua eficácia. Dados mal selecionados ou modelos desatualizados podem gerar indicações errôneas, com risco de cerceamento da liberdade de cidadãos inocentes. Por isso, recomendam-se validação contínua dos conjuntos de treinamento e auditoria periódica. Do ponto de vista ético, esse cuidado é essencial para mitigar vieses estruturais, do ponto de vista legal, o tratamento de dados biométricos é regulado pela LGPD (Lei n. 13.709/2018) [25], que classifica tais informações como sensíveis e exige medidas proporcionais de proteção. A ausência de métricas públicas em soluções internacionais [6], [9] contrasta com a transparência aqui adotada, que permite discutir não apenas resultados técnicos, mas também implicações legais e éticas do uso da tecnologia.

Outro ponto crítico diz respeito à robustez frente a imagens de qualidade reduzida. Embora a avaliação inicial tenha contemplado diferentes níveis de resolução, iluminação e ângulo, observou-se queda significativa na acurácia sob condições adversas. Por isso, recomenda-se ampliar o conjunto de treinamento com imagens capturadas em campo, aplicar técnicas de *data augmentation* e realizar retreinamento periódico com novos dados coletados em operação. Além disso, é importante reconhecer limitações adicionais dos testes conduzidos: o impacto de disfarces comuns (como barba, mudanças de penteado ou acessórios, a exemplo de óculos e bonés) não foi avaliado de forma sistemática, apesar de seu potencial para reduzir a acurácia, a ambiguidade em casos de gêmeos idênticos e as disparidades por cor da pele evidenciam fragilidades que comprometem a equidade do sistema, e o tamanho reduzido e pouco diverso do conjunto de treinamento limita a generalização do modelo. Esses fatores indicam que o VisionApp, embora promissor, deve ser continuamente refinado para enfrentar cenários realistas e garantir maior confiabilidade operacional.

Como recomendação de uso, o aplicativo deve apoiar, e não substituir, a decisão do policial. Em vez de apontar um único correspondente, a solução deve retornar as 3–5 faces mais semelhantes, reduzindo a chance de identificação equivocada e reforçando a necessidade de conferência manual do CPF e dos documentos do abordado. Esse alinhamento é fundamental para equilibrar eficiência operacional e proteção de direitos fundamentais, evitando que o VisionApp reproduza os riscos já criticados em outros sistemas.

Por fim, embora este trabalho tenha focado na Polícia do Piauí, a abordagem pode ser adaptada a outras forças de segurança, desde que os modelos sejam treinados com dados locais e observem as particularidades legais de cada jurisdição.

VI. Conclusões

Este trabalho apresentou o VisionApp, um aplicativo móvel de reconhecimento facial que integra captura e pré-processamento de imagens, extração de vetores de representação e consulta a banco de dados criminal via API. As principais contribuições foram: (i) a implementação de um protótipo funcional em Flutter e FastAPI, com PostgreSQL e MinIO; (ii) a validação prática junto à Secretaria de Segurança Pública do Piauí; (iii) a análise de viés algorítmico e limitações de robustez; e (iv) a discussão dos impactos da LGPD no uso de dados biométricos.

Entre as limitações destacam-se o curto período de testes, a predominância de imagens de alta qualidade e a reduzida diversidade do conjunto de treinamento. Trabalhos futuros incluem ampliar a base de imagens com dados reais de campo, aplicar técnicas de *data augmentation* e estender a avaliação a outras forças de segurança.

Ressalta-se a importância de conformidade contínua com a LGPD, por meio de anonimização, registros de acesso e auditorias, de forma a equilibrar eficiência operacional e proteção de direitos fundamentais.

Em síntese, o VisionApp mostra-se promissor para modernizar abordagens policiais com maior agilidade e mobilidade, mas seu uso responsável requer supervisão humana, investimento em qualidade de dados e adequação legal, para que contribua à segurança pública sem comprometer garantias constitucionais.

Referências

[1] V. S. Conceição, E. M. Nunes, and A. M. Rocha, "O Reconhecimento Facial como uma das Vertentes da Inteligência Artificial (IA): um estudo de prospecção tecnológica," *Cadernos de Prospecção*, vol. 13, no. 3, pp. 745–758, Jun. 2020, doi: 10.9771/cp.v13i3.32818.

[2] F. P. Carmone, "Enhance Security with Robots and Artificial Intelligence," M.S. thesis, Dept. of Computer Engineering, Politecnico di Torino, Turin, Italy, Apr. 2025.

[3] J. G. da Mata, "Capítulo 2. Face a Face – Missões e Razões dos Enquadros, Parte 1: O Enquadro como Sintoma," *A Política do Enquadro*, Jusbrasil, 2021. [Online]. Available: https://www.jusbrasil.com.br/doutrina/secao/capitulo-2-face-a-face-missoes-e-razoes-dos-enquadros-parte-1-o-enquadro-como-sintoma-a-politica-do-enquadro/1333799498. Accessed: May 5,2025.

[4] T. Bottino, D. Vargas, and F. P. Fraga, Eds., *Segurança pública na era do Big Data: mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade*. Rio de Janeiro, Brasil: FGV Direito Rio, 2023. ISBN 978-65-86060-48-5. [Online]. Available: https://direitorio.fgv.br/publicacao/seguranca-publica-na-era-do-big-data. Accessed: May 5, 2025.

[5] J. Brasil, "Câmeras com tecnologia de reconhecimento facial vão ser instaladas em Rio Branco," *G1 Acre*, 14 Feb. 2022. [Online]. Available: https://g1.globo.com/ac/acre/noticia/2022/02/14/cameras-com-tecnologia-de-reconhecimento-facial-vao-ser-instaladas-em-rio-branco.ghtml. Accessed: Aug. 6, 2022.

[6] Secretaria de Segurança Pública do Estado do Amazonas (SSP-AM), "PM do Amazonas desenvolve tecnologia de reconhecimento facial," 17 Nov. 2020. [Online]. Available: https://www.ssp.am.gov.br/pm-do-amazonas-desenvolve-tecnologia-de-reconhecimento-facial/. Accessed: May 8, 2025.

[7] Tempo Real RJ, "Polícia do Rio agora tem o reconhecimento facial na palma da mão," 28 Jan. 2025. [Online]. Available: https://temporealrj.com/policia-do-rio-agora-tem-o-reconhecimento-facial-na-palma-da-mao/. Accessed: May 8, 2025.

[8] L. Arrais, "Governo do Piauí desenvolve tecnologia de reconhecimento facial para solucionar crimes," *Portal do Governo do Piauí*, 6 Nov. 2024. [Online]. Available: https://www.pi.gov.br/noticia/governo-do-piaui-desenvolve-tecnologia-de-reconhecimento-facial-para-solucionar-crimes. Accessed: May 8, 2025.

[9] J. Calamia, "iCop: Police to Use Facial Recognition App to Nab Criminals," *Discover Magazine – Discoblog*, 16 Jun. 2010. [Online]. Available: https://www.discovermagazine.com/technology/icop-police-to-use-facial-recognition-app-to-nab-criminals. Accessed: May 8, 2025.

[10] K. Kumar and K. Sharath, "Crime Identification Using Face Matching Based on Mobile Application," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 4, no. 2, pp. 122–125, Jul. 2024, doi: 10.48175/568. [Online]. Available: https://www.ijarsct.co.in.

[11] Flutter. *Flutter – Build apps for any screen*. Disponível em: https://flutter.dev. Acesso em: 31 maio 2025.

[12] Android Developers. *Android Studio – Android Developers*, 2025. Disponível em: https://developer.android.com/studio. Acesso em: 31 maio 2025.

[13] Google. *Firebase Authentication Documentation*, 2024. Disponível em: https://firebase.google.com/docs/auth. Acesso em: 27 maio 2025.

[14] M. N. C. Menezes, *Introdução à Programação com Python: Algoritmos e Lógica de Programação para Iniciantes*, 3. ed. São Paulo: Novatec, 2019. ISBN 978-85-7522-718-3.

[15] S. Ramírez, *FastAPI*. Disponível em: https://fastapi.tiangolo.com. Acesso em: 28 maio 2025.

[16] A. S. Tanenbaum e M. Van Steen, *Distributed Systems: Principles and Paradigms*, 4. ed. Version 4.01. [S.l.]: Maarten van Steen, 2023. ISBN 978-90-815406-3-6. Disponível em: https://www.distributed-systems.net/index.php/books/ds4/. Acesso em: 27 maio 2025.

[17] M. B. Jones, J. Bradley e N. Sakimura, "JSON Web Token (JWT)," *RFC 7519*, Internet Engineering Task Force, 2015. Disponível em: https://tools.ietf.org/html/rfc7519. Acesso em: 28 maio 2025.

[18] V. Santos, "Encriptando senhas em Python com bcrypt," *Medium*, 29 jun. 2020. Disponível em: https://medium.com/py-bcrypt/encriptando-senhas-em-python-com-bcrypt-25e46b5c8166. Acesso em: 31 maio 2025.

[19] M. Stonebraker e L. A. Rowe, "The Design of POSTGRES," *ACM SIGMOD Record*, vol. 15, no. 2, pp. 340–355, jun. 1986. Disponível em: https://dl.acm.org/doi/10.1145/16856.16888. Acesso em: 27 maio 2025.

[20] D. E. King, "Dlib C++ Library Documentation," 2025. [Online]. Available: http://dlib.net. Acesso em: 29 maio 2025.

[21] A. Geitgey, "face-recognition: Simple face recognition library for Python," 2025. [Online]. Available: https://github.com/ageitgey/face_recognition. Acesso em: 29 maio 2025.

[22] MinIO, "MinIO – High Performance Object Storage," 2024. [Online]. Available: https://min.io. Acesso em: 30 maio 2025.

[23] J. Buolamwini and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, vol. 81, 2018. [Online]. Available: https://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 5 jun. 2025.

[24] J. Li, "LFW Dataset," Kaggle, 2025. [Online]. Available: https://www.kaggle.com/datasets/jessicali9530/lfw-dataset/data. Accessed: Jun. 5, 2025.

[25] Brasil, "Lei Geral de Proteção de Dados Pessoais (LGPD)," Lei n. 13.709, de 14 de agosto de 2018. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 junho 2025.

[26] E. C. Almeida, "Os Grandes Irmãos: O Uso de Tecnologias de Reconhecimento Facial para Persecução Penal," *Revista Brasileira de Segurança Pública*, vol. X, no. Y, pp. 123–145, 2021. [Online]. Available: https://exemplo.com/almeida_reconhecimento_facial. Acesso em: 21 junho 2025.