CONTROLE DO HORÁRIO DE SAÍDA DE ESTUDANTES DA EDUCAÇÃO INFANTIL COM RECONHECIMENTO FACIAL

Adryan Luccas Garcez Santana, Arthur Gabriel Gerônimo Fortes, Ryan Gabriel Saes de Sousa, Bruno Michel Pera (Orientador)

Universidade do Vale do Paraíba – UNIVAP Centro, Praça Cândido Dias Castejón, 116, Centro – 12245-720 – São José dos Campos-SP, Brasil, adryangarcez03@gmail.com, arthurgfortes98@gmail.com, saesryan08@gmail.com, brunomichel00@gmail.com.

Resumo

Este trabalho apresenta o desenvolvimento de um aplicativo móvel para apoiar o controle da saída de estudantes da educação infantil por meio do reconhecimento facial de responsáveis previamente autorizados. A pesquisa, de natureza aplicada, combinou revisão bibliográfica e desenvolvimento de protótipo no Android Studio, com Kotlin, OpenCV, Haar Cascade, LBPH e Firebase. O sistema organiza o cadastro de crianças e responsáveis, associa vínculos de autorização, detecta a face capturada na portaria e registra cada tentativa de retirada. A avaliação realizada foi funcional, restrita ao encadeamento das telas, à persistência dos dados e à execução do fluxo de detecção e consulta. Não foram conduzidos ensaios de acurácia, taxas de falso aceite ou falsa rejeição, nem validação com amostra representativa em ambiente escolar. Assim, os resultados demonstram o funcionamento do protótipo, mas não comprovam eficácia biométrica para uso real, que depende de validação experimental, proteção de dados, supervisão humana e mecanismos contra fraude.

Palavras-chave: Reconhecimento facial. Visão computacional. Biometria. Segurança escolar. Proteção de dados.

Área do Conhecimento: Ciências Exatas e da Terra – Ciência da Computação.

Introdução

O controle da retirada de crianças exige que a escola identifique corretamente a pessoa autorizada e registre o evento de forma rastreável. Procedimentos baseados apenas em conferência visual podem apresentar demora, inconsistências e dificuldade de auditoria. Estudos recentes sobre controle de saída em unidades de educação infantil mostram que a combinação de identificação e registro digital pode apoiar a segurança do processo e reduzir a dependência de verificações exclusivamente manuais (Liberato et al., 2023).

O reconhecimento facial é uma modalidade biométrica baseada na aquisição da imagem, detecção da face, extração de características e comparação com referências previamente cadastradas. Seu desempenho pode variar com iluminação, pose, expressão, resolução da câmera e características da população avaliada, motivo pelo qual a demonstração de um fluxo funcional não deve ser confundida com validação biométrica (Kortli et al., 2020; Wang; Deng, 2021).

Além do desempenho técnico, sistemas biométricos exigem atenção a vieses demográficos, privacidade e segurança das informações. A literatura aponta que algoritmos biométricos podem apresentar diferenças de desempenho entre grupos e que dados faciais exigem governança específica (Drozdowski et al., 2020; Sarabdeen, 2022). No Brasil, dado biométrico vinculado a uma pessoa natural é classificado como dado pessoal sensível pela Lei Geral de Proteção de Dados Pessoais - LGPD (Brasil, 2018). Também devem ser considerados ataques de apresentação, como uso de fotografias, vídeos ou máscaras, cuja mitigação demanda mecanismos próprios de detecção (Sharma; Selwal, 2023).

Nesse contexto, o objetivo deste trabalho foi desenvolver um protótipo móvel em Kotlin para apoiar o controle do horário de saída de estudantes da educação infantil, detectando e reconhecendo responsáveis previamente cadastrados, verificando o vínculo de autorização com a criança e registrando as tentativas de retirada. O estudo concentra-se na construção e demonstração funcional da solução, sem pretender comprovar, nesta etapa, sua eficácia biométrica em condições reais de uso.

Metodologia

A pesquisa é de natureza aplicada e foi conduzida como estudo de desenvolvimento tecnológico. Inicialmente, foram levantados requisitos relacionados ao cadastro de usuários, crianças, responsáveis, vínculos de autorização e registros de retirada. Em seguida, foram modelados os fluxos do sistema e a estrutura NoSQL. O protótipo foi implementado no Android Studio com Kotlin; o OpenCV foi empregado

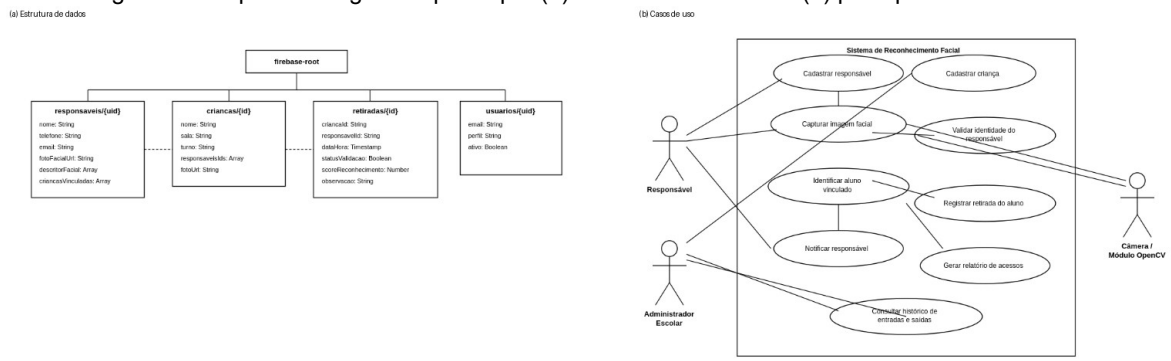
no processamento de imagens, e o Firebase Realtime Database, na persistência e sincronização dos dados (Google, 2026; JetBrains, 2026; OpenCV, 2026).

O fluxo operacional foi dividido em cadastro e validação. No cadastro, o operador informa os dados do responsável e da criança, registra o vínculo e adiciona amostras faciais. Na validação, a câmera captura a imagem, a rotina Haar Cascade localiza a região facial e o LBPH compara o descritor obtido com os padrões cadastrados. O LBPH trabalha com imagens em tons de cinza e retorna uma medida de distância associada à comparação; no OpenCV, a API permite configurar raio, número de vizinhos, grade horizontal, grade vertical e limiar de rejeição. A documentação da biblioteca apresenta, como valores padrão da API, radius=1, neighbors=8 e grade 8 x 8, enquanto o threshold deve ser explicitamente controlado quando se deseja rejeitar correspondências acima de determinada distância (OpenCV, 2026).

Na versão funcional documentada neste trabalho, o limiar de decisão permaneceu configurável e não foi calibrado por meio de um ensaio biométrico. Da mesma forma, não houve desenho experimental com quantidade fixa de amostras faciais por responsável nem padronização formal de iluminação, distância, pose, câmera e separação entre conjuntos de treinamento e teste. Por essa razão, tais elementos não são apresentados como parâmetros de desempenho. Para uma reprodução experimental futura, o protocolo deverá registrar esses itens, bem como a versão da biblioteca, os parâmetros efetivamente usados no LBPH e no detector Haar, e critérios objetivos de falso aceite e falsa rejeição.

Toda tentativa de retirada gera registro com data, horário, identificadores, estado da validação e índice retornado pelo reconhecimento. A decisão final permanece sob responsabilidade do funcionário da escola. A base foi organizada nos nós responsáveis, crianças, retiradas e usuários: os dois primeiros armazenam identificação e vínculos de autorização; o terceiro forma o histórico de auditoria; e o quarto controla perfis de operadores. A avaliação desta etapa foi exclusivamente funcional, verificando cadastro, persistência, navegação, detecção facial, consulta do vínculo e geração de registros; não foram realizados ensaios biométricos com amostra populacional nem validação em ambiente escolar.

Figura 1 – Arquitetura lógica do protótipo: (a) dados no Firebase e (b) principais casos de uso.



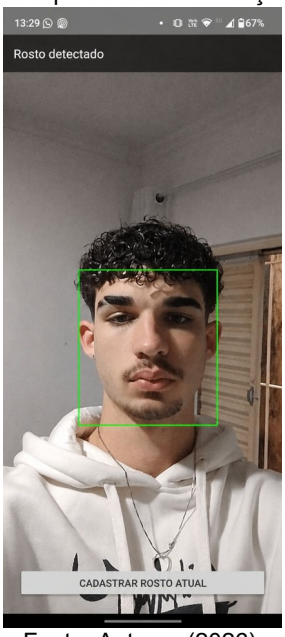
Fonte: Autores (2026).

Resultados

O desenvolvimento resultou em um aplicativo móvel capaz de cadastrar crianças e responsáveis, associar autorizações, capturar a imagem facial, consultar o vínculo entre responsável e estudante e apresentar uma resposta ao operador. A integração com o Firebase centralizou as informações e os registros de retirada, enquanto o processamento local com OpenCV forneceu retorno visual durante a captura. Esses resultados confirmam o encadeamento funcional dos componentes previstos na arquitetura, mas não constituem uma medição de desempenho biométrico.

A interface de reconhecimento apresenta o retorno “Rosto detectado”, delimita a região facial por uma caixa e disponibiliza o comando de cadastro da amostra atual. Na etapa de retirada, a mesma cadeia de processamento é utilizada para localizar um cadastro e consultar a criança vinculada. A Figura 2 documenta essa demonstração funcional da detecção e do cadastro facial. A imagem não representa, isoladamente, evidência de acurácia do reconhecimento, pois não houve protocolo de teste com identidades múltiplas, repetições controladas ou condições variadas de captura.

Figura 2 – Tela do protótipo durante a detecção e o cadastro facial.



Fonte: Autores (2026).

Não foram calculadas métricas como acurácia, taxa de falso aceite, taxa de falsa rejeição, EER, matriz de confusão ou tempo de resposta em uma população representativa. Também não foi realizada validação de uso em ambiente escolar. Portanto, os resultados apresentados devem ser interpretados como verificação do funcionamento do protótipo e da integração entre interface, reconhecimento e banco de dados, sem extrapolação para eficácia, segurança biométrica ou desempenho operacional em implantação real.

Além do protótipo, estimou-se o esforço de desenvolvimento em 280 horas de programação e 6 horas de análise. Com os valores de referência adotados na monografia, o custo total estimado foi de R$ 2.457,38. A estimativa representa apenas mão de obra e não inclui dispositivos, conectividade, manutenção, treinamento, infraestrutura, testes biométricos ou custos de conformidade.

Tabela 1 – Estimativa de custo da mão de obra do protótipo.

Profissional	Valor/hora	Horas	Subtotal
Programador júnior	R$ 8,33	280	R$ 2.332,40
Analista de sistemas júnior	R$ 20,83	6	R$ 124,98
Total		**286**	**R$ 2.457,38**

Fonte: Elaborado pelos autores com base nos valores utilizados na monografia (2026).

Discussão

Os resultados indicam que a integração entre aplicativo, visão computacional e banco de dados é tecnicamente viável como prova de conceito para organizar o fluxo de retirada. A associação digital entre adulto e criança e a gravação do histórico aumentam a rastreabilidade e oferecem apoio ao inspetor. Essa finalidade é coerente com trabalhos recentes voltados ao controle de saída e de acesso em instituições de ensino, inclusive propostas que combinam biometria, RFID ou autenticação múltipla para reduzir falhas de identificação (Liberato et al., 2023; Liberato et al., 2024).

Entretanto, o funcionamento do protótipo não comprova desempenho biométrico suficiente para uso real. Variações de iluminação, posição do rosto, qualidade da câmera e aparência podem alterar as comparações, e a literatura destaca a necessidade de avaliar robustez em diferentes cenários, além de possíveis diferenças de desempenho entre grupos demográficos (Kortli et al., 2020; Drozdowski et al., 2020). Embora métodos modernos baseados em aprendizagem profunda tenham ampliado o desempenho do reconhecimento facial, eles também dependem de bases adequadas, protocolos de avaliação e recursos computacionais compatíveis (Wang; Deng, 2021). Assim, o LBPH utilizado no protótipo deve ser compreendido como opção de implementação da prova de conceito, e não como evidência de superioridade ou prontidão para implantação.

A adoção em ambiente escolar também exige controles de privacidade, finalidade, acesso, retenção e segurança dos dados biométricos, em consonância com a LGPD, além de procedimento manual alternativo e supervisão humana (Brasil, 2018; Sarabdeen, 2022). Outro ponto necessário é a proteção contra ataques de apresentação, já que fotografias ou vídeos podem explorar vulnerabilidades de sistemas faciais sem mecanismos de detecção de vivacidade (Sharma; Selwal, 2023). Dessa forma, uma etapa posterior deverá combinar testes biométricos controlados, avaliação de usabilidade, análise jurídica e mecanismos de anti-spoofing antes de qualquer uso operacional.

Conclusão

O objetivo de desenvolver um protótipo móvel para apoiar o controle do horário de saída escolar por reconhecimento facial foi alcançado. A solução integra cadastro de crianças e responsáveis, captura e detecção facial, comparação por LBPH, consulta do vínculo de autorização e histórico de retiradas. Kotlin, OpenCV e Firebase mostraram-se adequados à construção da prova de conceito e permitiram integrar interface, processamento de imagens e persistência de dados.

A principal contribuição do estudo é demonstrar uma arquitetura funcional e rastreável para apoiar a conferência realizada pela escola. Contudo, não foram medidos acurácia, falso aceite, falsa rejeição, tempo de resposta ou desempenho em uma amostra representativa; por isso, o trabalho não comprova eficácia do reconhecimento facial para uso em ambiente escolar. Como continuidade, recomendam-se a definição e documentação completa dos parâmetros de captura e do LBPH, testes com diferentes condições e grupos de usuários, métricas biométricas, validação de usabilidade, detecção de apresentação fraudulenta, análise de segurança e adequação integral às regras de proteção de dados.

Referências

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 out. 2026.

DROZDOWSKI, P.; RATHGEB, C.; DANTCHEVA, A.; DAMER, N.; BUSCH, C. Demographic bias in biometrics: a survey on an emerging challenge. **IEEE Transactions on Technology and Society**, v. 1, n. 2, p. 89-103, 2020. DOI: 10.1109/TTS.2020.2992344.

GONZALEZ, R. C.; WOODS, R. E. **Processamento digital de imagens.** 3. ed. São Paulo: Pearson Prentice Hall, 2010.

GOOGLE. **Firebase Realtime Database.** Disponível em: https://firebase.google.com/docs/database. Acesso em: 4 ago. 2026.

JETBRAINS. **Kotlin documentation.** Disponível em: https://kotlinlang.org/docs/home.html. Acesso em: 4 ago. 2026.

KORTLI, Y.; JRIDI, M.; AL FALOU, A.; ATRI, M. Face recognition systems: a survey. **Sensors**, v. 20, n. 2, art. 342, 2020. DOI: 10.3390/s20020342.

LIBERATO, A. B.; OLIVEIRA, K. S.; GURGEL, S.; NARDI, J. C.; TEIXEIRA, G. F.; CAVALARI JÚNIOR, O.; MEIRELES, E. A system for access control in students' leaving times at childhood education units. **Concilium**, v. 23, n. 15, p. 657-677, 2023. DOI: 10.53660/CLM-1758-23L07.

LIBERATO, A. B.; TEIXEIRA, G. F.; MOREIRA, A. X.; BONJARDIM, L. C.; LIBERATO, G. M. Innovation in security: a proposal for access control with dual authentication through facial recognition and radiofrequency. **Concilium**, v. 24, n. 4, p. 302-317, 2024. DOI: 10.53660/CLM-2934-24D14.

OPENCV. **OpenCV documentation: LBPHFaceRecognizer and CascadeClassifier.** Disponível em: https://docs.opencv.org/. Acesso em: 5 out. 2026.

SANTANA, A. L. G.; FORTES, A. G. G.; SOUSA, R. G. S. **Controle no horário de saída escolar dos estudantes no ensino infantil com inteligência artificial.** Trabalho de Conclusão de Curso (Técnico em Informática) – Colégio Técnico Antônio Teixeira Fernandes, Universidade do Vale do Paraíba, São José dos Campos, 2026.

SARABDEEN, J. Protection of the rights of the individual when using facial recognition technology. **Heliyon**, v. 8, n. 3, e09086, 2022. DOI: 10.1016/j.heliyon.2022.e09086.

SHARMA, D.; SELWAL, A. A survey on face presentation attack detection mechanisms: hitherto and future perspectives. **Multimedia Systems**, v. 29, n. 3, p. 1527-1577, 2023. DOI: 10.1007/s00530-023-01070-5.

WANG, M.; DENG, W. Deep face recognition: a survey. **Neurocomputing**, v. 429, p. 215-244, 2021. DOI: 10.1016/j.neucom.2020.10.081.

Agradecimentos

Os autores agradecem às famílias, aos professores e ao Colégio Técnico Antônio Teixeira Fernandes – UNIVAP Centro pelo apoio ao desenvolvimento do projeto.