UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Uso de técnicas de análise de dados e visão computacional na deteção de actividades suspeitas durante a realização de exames de admissão

Caso de estudo: Estudantes da Faculdade de Engenharia da UEM

Autor

MANUEL, Edmildo Amilde José

Supervisor

Dr. Alfredo Covele

Maputo, junho de 2025

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Uso de técnicas de análise de dados e visão computacional na deteção de actividades suspeitas durante a realização de exames de admissão

Caso de estudo: Estudantes da Faculdade de Engenharia da UEM

Autor

MANUEL, Edmildo Amilde José

Supervisor

Dr. Alfredo Covele

Maputo, junho de 2025

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, ___ de junho de 2025

O Autor

_____

(Edmildo Amilde José Manuel)

Dedicatória

Aos meus pais, José Manuel Bassiane e Glória Alberto Nhanombe, por todo o amor, apoio e sacrifícios ao longo desta jornada.

Agradecimentos

Primeiramente, agradeço a Deus, o autor da vida, pela força, sabedoria e saúde concedidas ao longo desta jornada académica. Foi a Sua graça que me sustentou nos momentos mais difíceis e me guiou até à conclusão deste trabalho.

Expresso minha profunda gratidão aos meus queridos pais, José Manuel Bassiane e Glória Alberto Nhanombe, pelo amor incondicional, apoio constante e por sempre acreditarem no meu potencial. Os sacrifícios entregues, obrigações e ensinamentos foram fundamentais para que eu chegasse até aqui.

Ao meu supervisor, Dr. Alfredo Covele, deixo o meu sincero agradecimento pela orientação precisa, paciência, incentivo e por compartilhar comigo o seu conhecimento ao longo deste percurso. A sua contribuição foi essencial para o desenvolvimento deste trabalho.

Agradeço igualmente à Embaixada de Portugal pelo apoio financeiro concedido através da bolsa de estudos, que foi determinante para a continuidade e conclusão da minha formação superior. Esta oportunidade teve um impacto significativo na concretização deste sonho académico.

Agradeço também aos meus colegas, pelo companheirismo, partilha de ideias, apoio moral e espírito de colaboração. Cada conversa, estudo em grupo e momento de superação juntos fizeram toda a diferença na minha formação e crescimento pessoal e académico.

Epígrafe

"It always seems impossible until it's done."

"Sempre parece impossível até que seja feito."

Nelson Mandela

Resumo

Este trabalho teve como objectivo o uso de técnicas de análise de dados e visão computacional na deteção de actividades suspeitas durante a realização de exames de admissão na Universidade Eduardo Mondlane. O estudo focou na Faculdade de Engenharia da UEM, com o propósito de desenvolver um sistema capaz de identificar comportamentos fraudulentos. Através da pesquisa bibliográfica, inicialmente, foram apresentados os conceitos fundamentais de visão computacional, processamento de imagens e Aprendizagem de máquina, que são a base para a deteção de actividades suspeitas usando técnicas de visão computacional. Em seguida, foram detalhadas as etapas, abordagens e algoritmos utilizados para a análise de dados de vídeo e imagem. No caso de estudo, foi criado um protótipo de sistema que utiliza visão computacional e análise de dados para automatizar o processo de identificação de comportamentos não permitidos em exames de admissão. No sistema desenvolvido, destaca-se a utilização de algoritmos de Aprendizagem de máquina para classificação de padrões de comportamento e deteção de anomalias, como o uso de dispositivos eletrónicos ou comunicação entre candidatos. No âmbito de realização de testes, foram analisados vídeos e imagens capturadas manualmente com vista a simular o ambiente de realização de exames de admissão, e o sistema teve uma taxa de aproveitamento relevante na identificação de actividades suspeitas, classificando corretamente uma alta percentagem de casos. Assim, concluiu-se que a implementação de um sistema que utiliza visão computacional é uma solução para minimizar as ocorrências de fraudes durantes os exames de admissão.

Palavras-chave: Visão Computacional. Deteção de Actividades Suspeitas. Exames de Admissão. Monitoramento.

Abstract

This work aimed to use data analysis and computer vision techniques to detect suspicious activities during admission exams at Eduardo Mondlane University. The study focused on the Faculty of Engineering at UEM, with the purpose of developing a system capable of identifying fraudulent behaviors. Through a literature review, the fundamental concepts of computer vision, image processing, and machine learning, which form the basis for detecting suspicious activities using computer vision techniques, were initially presented. Subsequently, the steps, approaches, and algorithms used for video and image data analysis were detailed. In the case study, a prototype system was created that uses computer vision and data analysis to automate the process of identifying unauthorized behaviors in admission exams. In the developed system, the use of machine learning algorithms for classifying behavior patterns and detecting anomalies, such as the use of electronic devices or communication between candidates, is highlighted. For testing purposes, videos and images manually captured to simulate the admission exam environment were analyzed, and the system achieved a relevant success rate in identifying suspicious activities, correctly classifying a high percentage of cases. Thus, it was concluded that the implementation of a system using computer vision is a solution to minimize the occurrence of fraud during admission exams.

Keywords: *Computer Vision. Suspicious Activity Detection. Admission Exams. Monitoring.*

Índice

Anexos

Índice de figuras

Lista de Abreviaturas

UEM – Universidade Eduardo Mondlane

IA – Inteligência Artificial

AM – Aprendizagem de Máquina

YOLO - You Only Look Onc

CPU - Central Processing Unit (Unidade de Processamento Central)

GPU - Graphics Processing Unit (Unidade de Processamento Gráfico)

UML - Unified Modeling Language

COCO - Common Objects in Context

Glossário de termos

Cábula - Cábula (conhecida no Brasil e Angola como cola, copiar ou, em algumas regiões, pesca, fila) é um termo que define fraude em testes de conhecimento. Refere-se a anotações disfarçadas contendo resumos, utilizadas para colar durante um teste, exame ou prova, ou ao ato de copiar respostas de outras pessoas, com ou sem o consentimento delas

Cabulador – indivíduo que faz o uso de cábula.

Outsider – estudante ou qualquer individuo do lado de fora do exame que fornece respostas aos que se encontram a fazer o exame.

Histogramas - O histograma descreve graficamente a distribuição de frequências das intensidades luminosas. É uma ferramenta muito popular e normalmente utilizada para representar a quantidade que cada intensidade de cor se repete na imagem.

***Dataset* -** é uma coleção estruturada de dados organizados e armazenados juntos para análise ou processamento.

Framework - é um conjunto de bibliotecas, que abordam funcionalidades, e estruturas, para o desenvolvimento de aplicações, a fim de fornecer soluções para um mesmo domínio de problema, permitindo a reutilização do seu código.

1. Capítulo I - Introdução

Neste capítulo é apresentada a introdução detalhada do trabalho, desde o contexto da pesquisa, a formulação do problema que se pretende resolver com a pesquisa, a justificativa da escolha do tema, a apresentação do caso de estudo até os objectivos que se pretendem alcançar com a pesquisa.

1.1. Contextualização

Desde sempre, o ser humano procurou encontrar formas de supervisionar as suas actividades para garantir que elas sejam executadas de acordo com as regras estabelecidas com vista a alcançar determinados objectivos. No ramo da educação não é diferente, para que se tenha um processo de ensino e Aprendizagem de qualidade é necessário que os estudantes sejam submetidos a um processo de avaliação que vai testar os conhecimentos obtidos pelos mesmos e determinar o grau de conhecimento que cada estudante tem sobre a matéria. Porque a aprovação no processo avaliativo exige o conhecimento da matéria pelo lado do estudante e porque nem todos os estudantes são esforçados o suficiente para chegar ao dia da avaliação preparados, são verificadas várias tentativas de fraudes com vista a obter aprovação no exame.

Sendo também um processo avaliativo, o processo de exame de admissão não é isento da prática de fraudes, por esta razão que temos profissionais da UEM fazendo a vigilância dos estudantes durante o exame ou até o uso de detetores de metais em casos mais extremos. Porém, os estudantes sempre se inovam e encontram meios de cometer fraudes sem serem detetados. O uso de folhas de cábulas menores, Telemóveis ou relógios digitais em sapatos, matéria escrita em partes do corpo, são algumas das formas que os estudantes usam para enganar os meios de vigilância aplicados actualmente.

1.2. Formulação do problema

Em Moçambique, a educação é vista como um meio indispensável na preparação do capital humano para o combate à pobreza, a promoção do desenvolvimento socioeconómico e o bem-estar do cidadão. No quadro da Agenda 2030, dos Objectivos de Desenvolvimento Sustentável, das Nações Unidas, sustentada por programas quinquenais e planos estratégicos

educacionais, Moçambique estabelece como prioridade a escolarização de toda a sua população. É neste quadro que o país procura assegurar o ensino de qualidade para todos os cidadãos. Este é um objectivo fundamental, cuja avaliação é crucial. A Universidade Eduardo Mondlane faz o uso do processo avaliativo perante exames de admissão para seleção dos estudantes a ingressarem na instituição, estudantes que terão acesso à educação de qualidade fornecida pela Universidade. Entretanto, um dos fatores que reduz a qualidade de educação é a crescente taxa de fraudes que ocorrem durante o processo de avaliação, levando a Universidade a recomeçar os exames, como é o caso da Universidade Lúrio no caso apresentado na imagem abaixo.

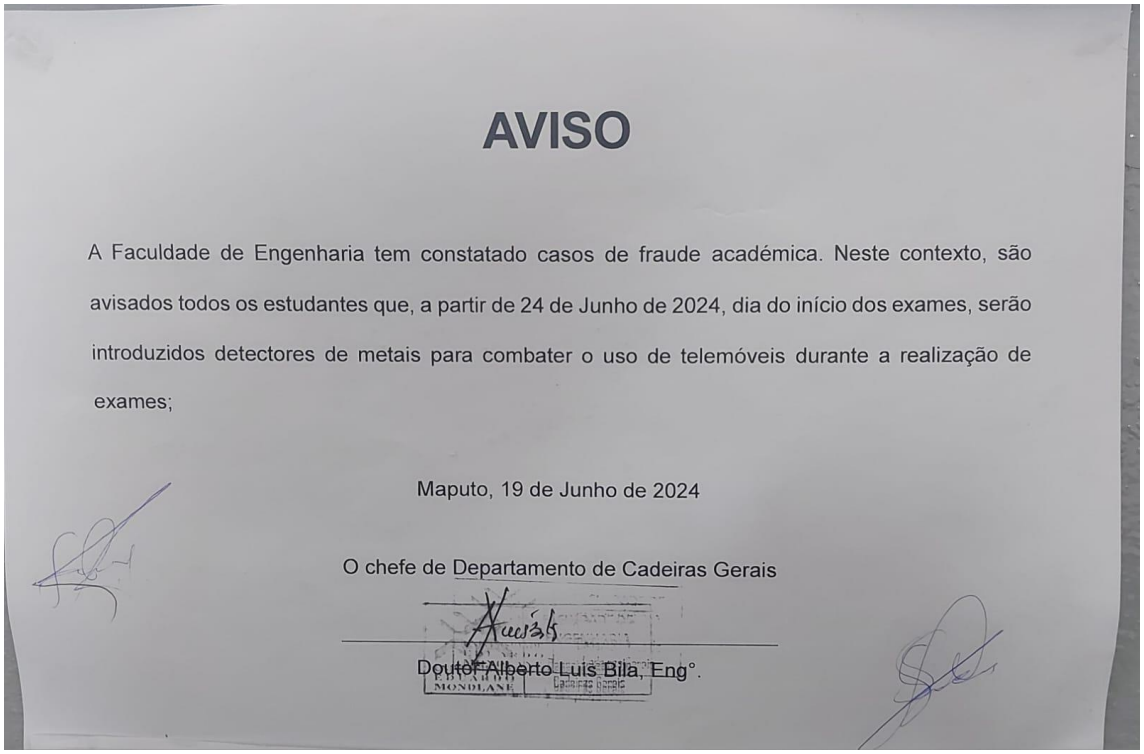
Figura 1. Registos de Fraudes nos exames de admissão da Universidade Lúrio
Fonte: https://web.facebook.com/share/p/1Asgu3ZXXP/

A fraude académica cometida por alunos é um problema de ordem institucional e social. Ela compromete a solidez de estruturas básicas da sociedade, tais

como a confiança nas instituições e a confiança interpessoal. Entre outros determinantes culturais e até mesmo antropológicos, a incapacidade de as instituições de ensino superior responderem eficazmente ao aumento do número de alunos que as frequentam pode estar na origem da tendência mundial para aumento das práticas de fraude. Esta massificação do acesso ao ensino superior não parece ter sido acompanhada por políticas públicas e institucionais adequadas à manutenção da qualidade do ensino e da aprendizagem (Almeida, Seixas, Gama, & Peixoto, 2015).

Muitas vezes a quantidade de alunos na sala de exame é tão grande que até mesmo dois docentes não são suficientes para controlar uma turma inteira durante o exame, ou os estudantes têm métodos bastante inovadores que os docentes são incapazes de detetar, culminando assim com a admissão de estudantes não capacitados na universidade.

As fraudes académicas não só estão presentes na realização dos exames de admissão, assim como no meio académico, sendo cometidas durante a realização de avaliações comuns e exames nas demais faculdades da Universidade.



AVISO

A Faculdade de Engenharia tem constatado casos de fraude académica. Neste contexto, são avisados todos os estudantes que, a partir de 24 de Junho de 2024, dia do início dos exames, serão introduzidos detectores de metais para combater o uso de telemóveis durante a realização de exames;

Maputo, 19 de Junho de 2024

O chefe de Departamento de Cadeiras Gerais

Doutor Alberto Luís Bila, Eng°.

Figura 2. Aviso do uso de detetores de metal durante a realização dos exames na Faculdade de Engenharia. Fonte: Autor

Como pode se observar na imagem anterior, há uma grande preocupação por parte da Universidade para acabar com as fraudes no meio académico.

Para resolver os problemas acima citados, propõe-se o desenvolvimento de um sistema que terá como auxílio à visão computacional para a deteção e alerta em tempo real das actividades suspeitas durante o processo de avaliação dos estudantes, detetando movimentos suspeitos durante o teste, material que não deveria fazer parte da sala de exame como Telemóveis, a passagem de material entre os alunos durante a realização do teste e tantos outros aspetos que podem ser considerados fraudulentos durante a realização das avaliações

1.3. Justificativa

Com a introdução dos exames de admissão em 1991 pela UEM, a instituição sempre tem investido em meios para garantir com que o processo seja o mais livre de fraudes possível, porém nenhum dos meios se mostrou eficaz.

Não só em exames de admissão, mas durante a realização de exames normais nas diferentes faculdades da universidade são verificadas várias tentativas de fraudes, levando a faculdade a ter que usar detetores de metal em seus estudantes, como é o caso da faculdade de engenharia.

Com o objectivo de erradicar as tentativas de fraudes em salas de exames de admissão, o trabalho apontara as principais actividades fraudulentas que são cometidas na sala de exame de admissão assim como indicará as técnicas de análise de dados apropriadas para deteção das mesmas. Nesse contexto, o trabalho indicara como a inteligência artificial pode ser usada com vista a garantir um processo seletivo livre de fraudes.

1.4. Apresentação do caso de estudo

A Universidade Eduardo Mondlane (UEM) é uma instituição de ensino superior pública moçambicana, que tem a sua reitoria instalada na cidade de Maputo.

Com uma tradição que remonta ao período colonial, é a mais antiga e também referência entre as universidades do país. Foi fundada, em definitivo, em 1962, e depois da independência foi durante muito tempo a única responsável pela formação intelectual moçambicana.

Em 2016, a universidade foi classificada pela classificação Webometrics Ranking of World Universities como a melhor universidade dos PALOP, sendo, de longe, a melhor universidade do seu país. (uem.co.mz, n.d.)

1.4.1. A Faculdade de Engenharia

A Faculdade de Engenharia foi fundada em 1962 com uma estrutura de chefia centralizada, com cada curso associado a um Departamento específico. Logo após a Independência, os departamentos assumiram o estatuto de Faculdade com um corpo diretivo não centralizado, mas com uma coordenação inter-faculdade. Esta estrutura permaneceu até 1980, quando a estrutura foi de novo mudada para a situação de 1962. Em 1962 existiam 4 cursos, nomeadamente Engenharia Civil, Engenharia Electrotécnica, Engenharia Mecânica e Engenharia Química. (uem.co.mz, n.d.)

A escolha dos estudantes da Faculdade de Engenharia como caso de estudo neste trabalho justifica-se pelo facto de já terem experienciado o processo dos exames de admissão. Esta experiência prévia proporciona-lhes uma perspetiva valiosa e um conhecimento direto sobre as dinâmicas e potenciais desafios associados a esses exames, tornando-os um grupo relevante para a análise e deteção de atividades suspeitas.

1.5. Objectivos

1.5.1. Objectivo Geral

- Usar técnicas de análise de dados e visão computacional na deteção de actividades suspeitas durante a realização de exames de admissão.

1.5.2. Objectivos Específicos

- Identificar as principais actividades fraudulentas cometidas pelos estudantes durante os exames de admissão;
- Comparar as técnicas de análise de dados que podem ser usadas que podem ser usadas para o desenvolvimento da pesquisa;
- Desenvolver um protótipo de sistema que permita a visualização, em tempo real, das actividades suspeitas na sala do exame

1.6. Metodologia

1.6.1. Classificação da pesquisa

a) O presente trabalho tem uma natureza **aplicada** que segundo (Gil, 2008) tem como característica fundamental o interesse na aplicação, utilização e consequências práticas dos conhecimentos.

b) A pesquisa tem uma abordagem qualitativa e quantitativa:

- Para (Mussi, Mussi, Assunção, & Nunes, 2019), a **pesquisa quantitativa** pretende e permite a determinação de indicadores e tendências presentes na realidade, ou seja, dados representativos e objectivos, opondo-se à ciência aristotélica, com a desconfiança sistemática das evidências e experiência imediata.
- Segundo (Mussi, Mussi, Assunção, & Nunes, 2019), a **pesquisa qualitativa** nos permite enveredar por situações que os números muitas vezes não conseguem responder. Um desses fatores pode ser utilizado através do uso da memória como fonte de pesquisa.

c) Quanto aos objectivos, a pesquisa é de carácter **exploratório**, que, segundo (Gil, 2008), pesquisas exploratórias são desenvolvidas com o objectivo de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato. Este tipo de pesquisa é realizado especialmente quando o tema escolhido é pouco explorado e torna-se difícil sobre ele formular hipóteses precisas e operacionalizáveis.

d) Quanto ao procedimento, a pesquisa é um **estudo de caso**, que se caracteriza pela investigação aprofundada de um aspeto dentro de um contexto real e específico.

1.6.2. Técnicas de coleta de dados

a) Pesquisa bibliográfica

Para (Gil, 2008), a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos.

b) Questionário

(Gil, 2008) define questionário como a técnica de investigação composta por um conjunto de questões que são submetidas a pessoas com o

propósito de obter informações sobre conhecimentos, crenças, sentimentos, valores, interesses, expectativas, aspirações, temores, comportamento presente ou passado.

1.6.3. População alvo

a) Candidatos aos Exames de Admissão

São os principais envolvidos, pois a fraude pode prejudicar candidatos honestos e comprometer a justiça durante o processo seletivo.

b) Vigilantes de exames de admissão

Profissionais que actuam na fiscalização e que podem se beneficiar da ferramenta para deteção de fraudes.

c) Direção da Universidade Eduardo Mondlane

Responsáveis por garantir a integridade, transparência e eficiência do processo de seleção;

d) Instituições Académicas em Geral

Universidades e centros de formação que enfrentam desafios semelhantes;

e) Pesquisadores e Estudantes da Área de Inteligência Artificial e Visão Computacional

Interessados nos resultados técnicos e científicos do trabalho, podendo aprimorar ou ampliar a proposta de solução.

1.7. Estrutura do trabalho

Capítulo 1 - Introdução

Apresenta o contexto da pesquisa, a formulação do problema, a justificativa da escolha do tema, os objectivos da pesquisa, a metodologia aplicada e o caso de estudo.

Capítulo 2 - Revisão da Literatura

Explora os conceitos teóricos que embasam o trabalho, incluindo fraude académica, inteligência artificial, Aprendizagem de máquina e visão computacional, com foco em ferramentas como o modelo YOLO e a biblioteca OpenCV, além de detalhar as principais técnicas de fraude em exames.

Capítulo 3 - Desenvolvimento do Protótipo

Descreve a metodologia de desenvolvimento utilizada, detalhando as fases de compreensão do problema, coleta e preparação de dados, modelagem, testes e implementação do sistema, incluindo os requisitos funcionais e não funcionais, bem como os resultados obtidos em simulações na sala acima citada.

Capítulo 4 - Considerações Finais

É sintetizado como explicações da pesquisa, discutindo a eficácia do sistema proposto, suas limitações, sugestões para melhorias futuras, além de destacar a relevância da solução para a integridade académica.

2. Capítulo II - Revisão da Literatura

2.1. Conceitos de Fraude académica

2.1.1. A avaliação e a prática da fraude

Segundo Pozo 2008 citado por (Barbosa J. Á., 2017), ensinar e aprender são dois verbos que deveriam ser conjugados juntos, mas isso nem sempre acontece no processo pedagógico. Existe, portanto, aprendizagem sem ensino e ensino sem aprendizagem. Este necessário ajuste entre o que se ensina e o que se aprende tornou-se um dos desafios da profissionalidade docente e envolve dilemas que podem comprometer a docência universitária. Desta forma, é essencial reconhecer a avaliação das aprendizagens como uma prática que facilita o alinhamento entre o que é ensinado e o que é aprendido, servindo como um meio de reflexão tanto para alunos quanto para professores. Com base nas informações obtidas através da avaliação, é possível direcionar as ações do professor no ensino e as do aluno na aprendizagem. Dessa forma, sua função vai além da simples prática de "aprovar" ou "reprovar" com base nas respostas em exames ou outras actividades avaliativas, integrando-se mais profundamente aos processos de ensino e aprendizagem.

A preocupação em somente aprovar determinada disciplina/cadeira ou aprovar em determinado exame, leva os estudantes a pular uma das componentes mais importantes do ensino que é o Aprendizagem, optando por cometer fraudes com vista a obter aprovação.

2.1.2. Fraude Académica

Segundo (Almeida, Seixas, Gama, & Peixoto, 2015), Fraude Académica é todo o ato ou omissão consciente que possa comprometer a justiça na avaliação dos desempenhos, competências e conhecimentos dos alunos.

A “cola” raramente é abordada no interior das instituições de ensino superior, quando se comenta sobre ela é de forma imatura e sem importância. A “cola” existe, mas não é discutida, não há providências para inibi-la. Parece existir um acordo tácito entre docentes e discentes, para uma prática mesquinha de irresponsabilidade social (Barbosa J. Á., 2017).

Figura 3. Um exemplo de fraude em sala de aula. Fonte: https://formacaoformadores-ccp.pt/guia-do-formador/o-formador-e-a-actividade-pedagogica/guia-da-desonestidade-academica/tecnicas-de-como-cabular

Segundo (Souza, 2016), para os professores, a "cola" é uma inimiga ousada uma vez que desafia seus métodos avaliativos, suas escolhas metodológicas, seu domínio de sala de aula e até mesmo sua presença nela. O ensino transmissivo de conteúdos, no qual, ao professor cabe apenas "passar" a informação e ao aluno captá-la e repeti-la, sendo a avaliação restrita à prova escrita, medidora, que atribui nota e classifica, mostra-se como um ambiente favorável à manifestação da cola.

O desafio é constante já que as estratégias de cola são aperfeiçoadas através do tempo, as mais antigas perdem espaço para as mais modernas e criativas. Em consequência disso, para minimizar e evitá-las, as instituições de ensino tomam algumas medidas preventivas, corretivas ou repreensivas para punir o aluno que for apanhado colando. Por outro lado, os mais variados mecanismos de controle terminam por legitimar e convidar a tal prática, porque apenas um número pequeno de alunos, comparado ao número real de "infratores", é pego colando, o que parece ser suficiente para manter a impressão de controle (KRAUSE, 1997 citado por (Souza, 2016)).

2.1.3. Técnicas de fraudes em sala de aula

O *site* (Formação de Formadores , n.d.) destaca onze diferentes técnicas de cábula cometidas em sala de aula, a destacar:

O método da camisa de mangas compridas

Na prática, o aluno utiliza os seus antebraços como papel de cábula escrevendo aí todas as informações que necessita memorizar. Sempre que pretende consultar a cábula só tem que arregaçar as mangas, enquanto o docente não está a olhar para si. Existem variantes em que o papel da cábula é colado nas pernas - embora aí a leitura seja mais difícil.

A Mesa é a melhor amiga

Há estudantes que são muito pontuais, até demasiado. São os primeiros a chegar à sala com o propósito de escrever na mesa a sua cábula. Em seguida só têm que pousar algo em cima dela: uma peça de roupa, umas folhas em branco, etc. Este método é improvável que ocorra em exames de admissão pois os estudantes só entram na sala para dar início ao exame e o estudante não sabe previamente onde irá se sentar.

Tecnologia

Hoje em dia a tecnologia coloca ao serviço do aluno que cábula um arsenal de opções. Desde calculadoras que aparentam um ser simples - mas que têm capacidade para armazenar variedade de informação. O telefone também é muito usado. O melhor mesmo é não permitir o seu uso, colocando-os sobre a secretária do formador até ao final do teste.

Por vezes a Universidade opta pelo uso de detetores de metais, mas ainda há estudantes que conseguem entrar na sala do exame com os dispositivos, colocando-os até nos sapatos.

Chapéus

Copiar na sua forma mais comum implica apenas espreitar o teste do colega do lado ou da frente, com ou sem o seu consentimento. Estudantes usam chapéus para disfarçar o ato de espreitar o exame do outro colega, embora este método seja pouco usado pois é proibido o uso de chapéus em sala de exame de admissão.

O Método Kleenex

Se alguns dos estudantes já entregaram o teste é natural que o formador os coloque em cima da sua mesa, não tendo muitas vezes o cuidado de os

colocar com a frente virada para baixo. O estudante cabulador finge tosse, necessidade de assoar e aproxima-se da mesa do docente pedindo um lenço de papel. Enquanto o docente procura, ele só tem que espreitar para um desses testes. Um método alternativo é levar a cábula escrita num dos seus lenços de papel e, ao fingir que se assoa, consultar a mesma.

Trabalho em Equipa

Desde pagar a um "*outsider*" para que faça o teste até conseguir alguém lá fora que aguarde que o formando peça para ir à casa de banho (criando assim a oportunidade para o ajudar). A vigilância é a única defesa contra este método subversivo.

A Técnica da Mochila

Este aluno escolhe normalmente os lugares mais distantes e inacessíveis da sala. Quando o docente pede (no início do exame) para guardar todos os documentos e livros, este aluno aproveita para colocar as suas notas no chão, junto à mochila ou pasta volumosa, para que não possam ser vistas pelo docente, podendo, no entanto, ser consultadas pelo estudante ao longo do teste.

Estado desesperado

Este método é semelhante ao método do chapéu e a ideia é dar a impressão que se está com dificuldades - o que normalmente é bem visto pelo docente e apela à solidariedade e compreensão do mesmo. Enquanto o formando suspira, coloca a mão na cabeça e se inclina (num gesto de desespero) tal não passa de uma boa prestação de actor, pois na realidade fica assim melhor posicionado para espreitar o teste dos colegas, escondendo com a mão o olhar.

A técnica da Pastilha Elástica

Esta técnica é engenhosa. Alguns tipos de chicletes vêm embrulhadas em papel que pode ser aproveitado para o formando colocar as suas notas escritas. Assim, em caso de desespero, este só tem de desembrulhar a pastilha certa e ler as notas escritas.

Grafites / Mural

Este método exige a “solidariedade” da turma e consiste em alguém escrever nas paredes - em cartazes afixados ou em outro lugar estratégico, fora da visão fácil do docente - informações que ajudem o aluno a cabular. Caso o docente descubra, terá dificuldade em acusar alguém, pelo que neste caso “o crime compensará”.

A Palma da Mão

Esta técnica consiste em escrever a matéria na palma da mão, sendo consultada assim que necessária durante o exame.

Murmúrios

À medida que o teste decorre, do silêncio do início, um som de fundo vai aumentando enquanto o tempo passa. São murmúrios que normalmente vindos do lado oposto onde se encontra o docente.

2.2. Fraudes mais cometidas em exames de admissão

De acordo com o questionário realizado, a forma mais comum de fraude envolve o suborno, seja de docentes, fiscais ou outros indivíduos envolvidos no processo, respondidoa por 40% dos partici[antes. Logo em seguida, o uso de "papelinhos" ou anotações é outra tática amplamente empregada, com 35,6% de respostas.

Além do suborno e dos "papelinhos", outras estratégias fraudulentas são frequentemente utilizadas. A comunicação com outros candidatos durante a prova é uma prática comum, destacando-se com 33,3% de indicações, assim como o uso de celular ou outros dispositivos eletrónicos, escolhida por 31,1% dos inqueridos. A escrita de informações no próprio corpo, embora menos comum, ainda é observada por 24,4% das inqueridos. Curiosamente, métodos como o acesso prévio às respostas ou questões e o vazamento do enunciado da prova são raramente identificados, ambos com apenas 2,2% das menções, o que sugere que as fraudes mais acessíveis e de menor risco são as mais praticadas pelos candidatos.

2.3. Inteligência artificial e Técnicas de análise de dados

2.3.1. Inteligência Artificial

Pode-se observar que não há uma concordância sobre o que realmente significa inteligência, o que torna a tarefa de definir com precisão o que é inteligência artificial, se não impossível, pelo menos extremamente desafiadora. De acordo com (Russell & Norving, 2020), as definições de IA presentes na literatura científica podem ser classificadas em quatro categorias principais:

1. Sistemas que pensam como seres humanos
2. Sistemas que pensam racionalmente
3. Sistemas que actuam como seres humanos
4. Sistemas que actuam racionalmente

Sistemas que pensam como seres humanos

Ao longo da história da Inteligência Artificial (IA), tem-se mantido forte a ideia de que a modelagem dos processos de pensamento humano pode permitir-nos replicar tais processos em sistemas computacionais. Este tem sido um dos objectivos da ciência cognitiva, um campo interdisciplinar que engloba áreas como Psicologia, Ciência da Computação, Filosofia, Linguística e Antropologia.

Sistemas que pensam racionalmente

O pensamento racional é um processo cognitivo que envolve a análise lógica e sistemática de informações para chegar a conclusões ou tomar decisões. É uma forma de pensamento que se baseia em evidências, fatos e raciocínio lógico, em oposição ao pensamento emocional ou intuitivo. O pensamento racional é considerado uma habilidade fundamental para resolver problemas complexos, tomar decisões informadas e avaliar criticamente informações. (Viva, 2023)

Busca-se explorar a abordagem da inteligência artificial sob a perspetiva das "leis do pensamento", traçando um paralelo com a lógica aristotélica e seu desenvolvimento ao longo dos séculos. A tradição logicista na IA busca desenvolver programas que simulem a inteligência humana através da aplicação de princípios lógicos, mas enfrenta desafios complexos ao tentar

traduzir o conhecimento informal e incerto para a linguagem formal da lógica, além da complexidade computacional envolvida.

Sistemas que actuam como seres humanos

(Russell & Norving, 2020)destaca nesta abordagem, o seguinte teste proposto por Alan Turing:

Suponha que temos uma pessoa, uma máquina e um interrogador. O interrogador está em uma sala separada da outra pessoa e da máquina. O objectivo do jogo é que o interrogador determine qual dos outros dois é a pessoa e qual é a máquina.

A máquina passara no teste de Turing se o interrogador, depois de fazer perguntas por escrito, não conseguir definir se as respostas vêm da pessoa ou da máquina.

Torna-se difícil construir uma máquina que passe no teste de Turing pois precisa ter as seguintes capacidades:

Processamento de linguagem natural: para permitir que ela se comunique em linguagem humana.

Representação de conhecimento: para permitir o a máquina armazene informação.

Raciocínio automatizado: permitira que a máquina dê respostas e tire novas conclusões usando as informações armazenadas.

Aprendizagem de máquina: permite que a máquina se adapte a nossos cenários e detetar novos padrões.

Existe também o teste de Turing Total, que além das capacidades acima citadas, a máquina deve ter:

Visão de computador: permitira que ela perceba os objetos.

Robótica: para a manipulação de objetos e movimentação autónoma.

Figura 4. O cenário do teste de Turing. Fonte: Autor

Sistemas que agem racionalmente

Segundo (Russell & Norving, 2020), um agente é simplesmente algo que age. Espera-se que um agente computacional possua atributos que o diferenciam de simples "programas". Entre esses atributos, estão a capacidade de operar de forma autónoma, perceber o ambiente ao seu redor, manter-se ativo por longos períodos, adaptar-se a mudanças e ser capaz de adotar metas alheias. Um agente racional é aquele que age visando alcançar o melhor resultado possível ou, em situações de incerteza, o melhor resultado esperado.

2.3.2. Ciência de dados

Segundo (Uzinski, Abreu, & de Olivera, 2020), ciência de dados (*Data science*) e Inteligência artificial (*Artificial intelligence*) podem ser consideradas como algumas das áreas da ciência mais importantes de nosso tempo.

Nos dias de hoje, grande volume de dados são gerados o tempo todo, esse volume de dado dá-se o nome de *big data*. A ciência de dados é a arte de transformar esse volume de dados em conhecimento útil. Refere-se à coleta de dados de várias fontes para fins de análise, com o objectivo de apoiar a tomada

de decisões, utilizando geralmente grandes quantidades de dados, de forma sistematizada. (Escovedo & koshiyama)

2.3.3. Aprendizagem de máquina

Com a evolução do poder computacional e das técnicas de IA, o Aprendizagem de máquina vem ganhando mais destaque, permitindo criar máquinas que aprendem de forma autónoma a partir de uma determinada amostra de treinamento.

Segundo (Monard & Baranauskas, 2005), Aprendizagem de máquina é uma área de IA cujo objectivo é o desenvolvimento de técnicas computacionais sobre o Aprendizagem bem como a construção de sistemas capazes de adquirir conhecimento de forma automática.

Ainda que AM seja uma ferramenta poderosa para a aquisição da automática de conhecimento, deve ser observado que não existe um único algoritmo que apresente o melhor desempenho para todos os problemas. Portanto, é importante compreender o poder e a limitação dos diversos algoritmos de AM utilizando alguma metodologia que permita avaliar os conceitos induzidos por esses algoritmos em determinados problemas.

O Aprendizagem de máquina pode ser categorizado em:

- Aprendizagem supervisionado;
- Aprendizagem não supervisionado; e
- Aprendizagem por reforço.

Aprendizagem Supervisionado

Segundo (Monard & Baranauskas, 2005), no Aprendizagem supervisionado, todo exemplo possui um atributo especial, o rótulo ou classe, que descreve o fenómeno de interesse, isto é, a meta que se deseja aprender e poder fazer previsões a respeito. Os rótulos são tipicamente pertencentes a um conjunto discreto (nominal) de classes {C1,C2,...,Ck} no caso de classificação ou de valores reais no caso de regressão. Cada exemplo é descrito por um conjunto de características, representadas por um vetor de valores, e pelo rótulo da classe correspondente. O objectivo do algoritmo é aprender a relação entre as

características e os rótulos, para que possa classificar corretamente novos exemplos que ainda não foram rotulados.

Quando os rótulos representam categorias distintas, como "gato" ou "cão", o problema é chamado de classificação. Se os rótulos representam valores contínuos, como a previsão do preço de uma casa, o problema é chamado de regressão.

O Aprendizagem Supervisionado é a forma mais comum de Aprendizagem de máquina, devido à sua capacidade de resolver uma ampla gama de problemas.

Aprendizagem Auto-Supervisionada / Semi-Supervisionada: se trata de uma categoria especial da Aprendizagem Supervisionada, mas com uma diferença significativa: nesse método, não há necessidade de dados previamente anotados por humanos - os mesmos podem ser gerados por meio de heurísticas, por exemplo. No caso da aprendizagem Semi-Supervisionada, a mesma visa explorar tanto os dados fornecidos de maneira rotulada bem como dados não rotulados, de maneira efetiva, a fim de melhorar os resultados obtidos (Gatelli, 2021).

Aprendizagem não supervisionado

Aprendizagem não supervisionado, também conhecido como *machine learning* não supervisionado, usa algoritmos de *machine learning* para analisar e agrupar conjuntos de dados não rotulados. Esses algoritmos descobrem padrões ocultos ou agrupamentos de dados sem a necessidade de intervenção humana. Sua capacidade de descobrir semelhanças e diferenças nas informações o torna a solução ideal para análise exploratória de dados, estratégias de vendas cruzadas, segmentação de clientes e reconhecimento de imagem. (IBM, IBM.com, 2025)

Aprendizagem por reforço

No Aprendizagem por reforço, o sistema de inteligência artificial enfrenta uma situação. O computador utiliza tentativa e erro para encontrar uma solução para o problema. Para que a máquina faça o que o programador deseja, a inteligência artificial recebe recompensas ou penalidades pelas ações que executa. Seu objetivo é maximizar a recompensa total. (DeepLearning, 2025)

2.4. Redes Neurais

Redes neurais artificiais são sistemas de computação vagamente inspirados pelas redes neurais biológicas que constituem os cérebros animais. A rede neural em si não é um algoritmo, mas a estrutura de muitos algoritmos diferentes de Aprendizagem de máquina para trabalhar juntos e processar entradas de dados complexas. Tais sistemas aprendem a executar tarefas considerando exemplos, sem serem programados com regras específicas de tarefas. Por exemplo, no reconhecimento de imagem, as redes neurais podem aprender a identificar imagens que contenham gatos analisando exemplos que tenham sido rotulados manualmente como "gato" ou "não gato" e, em seguida, usar os resultados para identificar gatos em outras imagens. (Falcão, Moreira, Santos, & Ramos, 2019)

2.5. Framework Tensorflow

Criado pela equipe do Google Brain, TensorFlow é um *framework* de código aberto desenvolvido para Python e JavaScript, que auxilia no desenvolvimento de soluções com *machine learning*. Pode ser executado sobre diversas plataformas e arquiteturas, incluido CPUs, GPUs e as recentes TPUs (*Tensor Processing Unit*). (Falcão, Moreira, Santos, & Ramos, 2019)

(ARAUJO et al. 2017, citado por (Falcão, Moreira, Santos, & Ramos, 2019)) afirma que a arquitetura do Tensorflow se divide em três partes principais, sendo elas:

- Pré-processamento dos dados;
- Construção dos modelos;
- Treinamento e estimativas do modelo criado.

2.5.1. Tensor

O nome TensorFlow é derivado diretamente da sua ideia central: o **Tensor**. No *framework*, todas as operações de computação envolvem tensores. Um tensor é um vetor ou matriz de N dimensões que representa todos os tipos de dados. Todos os valores em um tensor mantêm um tipo de dados idêntico com uma forma (*shape*) conhecida (ou parcialmente conhecida). A forma dos dados é a dimensionalidade da matriz. (Falcão, Moreira, Santos, & Ramos, 2019)

2.6. Keras

Keras é a API de alto nível da plataforma TensorFlow. Ela fornece uma interface acessível e altamente produtiva para a resolução de problemas de Aprendizagem de máquina, com foco no Aprendizagem profundo moderno. Keras abrange todas as etapas do fluxo de trabalho de Aprendizagem de máquina, desde o processamento de dados até o ajuste de hiperparâmetros e a implantação. Foi desenvolvida com foco em permitir experimentação rápida. (Tensorflow, 2025)

2.7. Visão computacional: conceitos e aplicações

2.7.1. Visão computacional

A distinção precisa entre processamento de imagens e visão computacional é ténue. Em termos gerais, o processamento de imagens pode ser definido como um processo que recebe uma imagem como entrada e produz um conjunto de valores numéricos, os quais podem ou não formar uma nova imagem. Por outro lado, a visão computacional busca replicar a capacidade humana de enxergar, utilizando também uma imagem como entrada, mas gerando como saída uma interpretação da imagem em sua totalidade ou em partes específicas.

Conforme Gonzalez citado por (Marengoni & Stringhini, 2009), o espectro que vai do processamento de imagens até a visão computacional pode ser dividido em três níveis: baixo-nível, nível-médio e alto-nível. Os processos de baixo-nível envolvem operações primitivas, tais como a redução de ruído ou melhoria no contraste de uma imagem. Os processos de nível-médio são operações do tipo segmentação (particionamento da imagem em regiões) ou classificação (reconhecimento dos objetos na imagem). Os processos de alto nível estão relacionados com as tarefas de cognição associadas com a visão humana, onde o objectivo é emular a compreensão humana, interpretando o significado da imagem e realizando tarefas cognitivas baseadas no seu conteúdo visual.

Para (Milano & Honorato), visão computacional é a ciência responsável pela visão de uma máquina, pela forma como um computador enxerga o meio à sua volta, extraindo informações significativas a partir de imagens capturadas por câmaras de vídeo, sensores, *scanners*, entre outros dispositivos. Estas

informações permitem reconhecer, manipular e pensar sobre os objetos que compõem uma imagem.

Figura 5. Veículo em imagem escura (esquerda). Após uma equalização de histograma, em nível de cinza, onde a placa do veículo pode ser lida (direita). Fonte : (Marengoni & Stringhini, 2009)

A Figura 5 ilustra a distinção entre processamento de imagens e visão computacional através de um exemplo prático. À esquerda, vemos uma imagem escura de um veículo onde a placa não é legível. À direita, a mesma imagem foi submetida a uma equalização de histograma, resultando em uma imagem mais clara onde a placa do veículo agora pode ser vista. A visão computacional entra em cena quando aplicamos um processo para identificar e isolar a placa nessa imagem aprimorada e, em seguida, reconhecer os caracteres alfanuméricos presentes nela. Essa informação extraída da placa pode então ser usada para consultar um banco de dados e obter informações sobre o veículo.

Quando se trata de imagens, temos avanços significativos já embutidos em muitos aplicativos e outros sistemas que usamos. O Facebook já reconhece objetos automaticamente para classificar suas fotos, além disso, já aponta onde estão as pessoas na imagem para você “marcar”. O mesmo ocorre com smartphones que já disparam a foto quando as pessoas estiverem sorrindo, pois conseguem reconhecer tais expressões.

Rehem e Trindade (2009) citado por (Milano & Honorato), mencionam as seguintes funcionalidades comuns na maioria dos sistemas de visão computacional:

Aquisição de Imagem: É o primeiro passo para um sistema de visão computacional. Trata-se do processo de aquisição de uma imagem ou de um conjunto de imagens a partir de sensores de câmeras, onde os pixels de cada imagem obtida indicam coordenadas de luz e propriedades físicas. A imagem pode ser bidimensional, tridimensional ou uma sequência de imagens.

Pré-processamento: Processo realizado antes de obter informações de uma imagem, de forma a aplicar métodos específicos que facilitem a identificação de um objeto, como por exemplo destaque de contornos, bordas, destaque geométricas, etc. de figuras

Extração de características: Extração de características matemáticas que compõem uma imagem, como textura, bordas, formatos, movimento.

Deteção e segmentação: Processo realizado para destacar regiões relevantes da imagem, segmentando-as para processamento posterior.

Processamento de alto nível: Processo que inclui validação da satisfação dos dados obtidos, estimativa de parâmetros sobre a imagem e classificação de objetos obtidos em diferentes categorias.

2.7.2. Aplicações da visão computacional

Para (Milano & Honorato), a visão computacional encontra aplicações em uma vasta gama de campos, abrangendo desde a **física** e a **biologia** até a **indústria** e as **forças armadas**. Para ilustrar sua versatilidade, pode-se mencionar exemplos como a identificação de terroristas em aeroportos por meio do reconhecimento facial, a deteção de tropas adversárias ou mísseis guiados em contextos militares, a análise morfológica de células em estudos biológicos, o controle de braços robóticos em linhas de montagem automotivas e em reparos submarinos, e até mesmo em competições de futebol de robôs.

Diante da crescente preocupação com a intervenção humana e suas implicações para o futuro, aplicações voltadas ao **meio ambiente** ganham cada vez mais relevância. Através da visão computacional, torna-se viável monitorar mudanças ambientais em tempo real, processando imagens de

satélite para possibilitar a tomada automática de medidas. Adicionalmente, essa tecnologia permite a análise de eventos específicos, como padrões de migração ou o confinamento de aves em situações de estresse induzidas pelo aquecimento global.

Figura 6. Visão computacional aplicada em imagens de satélites. Fonte: (Vina, 2024)

A área da **Medicina** também se beneficia significativamente da visão computacional. Dada a limitação da perceção humana em identificar certos padrões em imagens médicas e em detetar imagens com ruído ou baixo contraste, o que pode levar a interpretações distintas, o uso de recursos computacionais se mostra valioso. Esses recursos podem auxiliar no diagnóstico de diversas doenças, atuando como um suporte para evitar imprecisões ou erros. Dessa forma, funcionariam como uma segunda opinião para o médico, confirmando suspeitas ou abrindo novas perspetivas para a identificação de uma condição médica. Esses sistemas são conhecidos como Sistemas Computacionais de Apoio ao Diagnóstico (CAD), exemplos incluem sistemas para auxiliar no diagnóstico de fraturas cranianas, lesões pulmonares e mamografias. Nesses sistemas, a visão computacional é empregada para detetar, caracterizar e classificar anomalias, com base em um extenso banco de imagens e informações. Outro fator que impulsiona o uso da visão computacional é a constatação de que a análise de radiografias se torna mais precisa com a avaliação de dois radiologistas. Nesse sentido, um sistema

automatizado poderia substituir um dos radiologistas, combinando os resultados para um diagnóstico mais acurado.

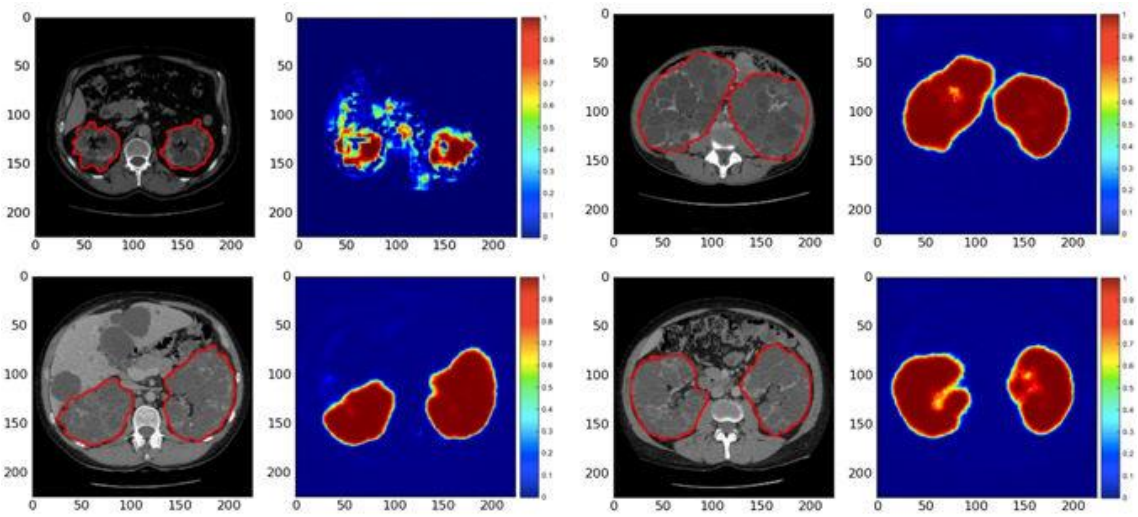


Figura 7. Visão computacional aplicada na medicina. (Fonte: (Academy, 2024))

Na **indústria**, a visão computacional encontra vasta aplicação, abrangendo desde o controle de qualidade na produção até tarefas mais especializadas, como a caracterização e classificação de minério de ferro. Sistemas de controle autônomo também se destacam, como os veículos autónomos *Remote Agent* e o *Mars Exploration* Rover da NASA.

Figura 8. Mars Exploration Rover (Fonte: (dooling, n.d.))

2.7.3. OpenCV

O OpenCV, cuja sigla representa Open Source Computer Vision Library, consiste em uma biblioteca de *software* de código aberto voltada para as áreas

de visão computacional e Aprendizagem de máquina. Sua relevância reside na vasta gama de funcionalidades que oferece para a análise de imagens e vídeos em tempo real, configurando-se como um recurso valioso para desenvolvedores e pesquisadores em múltiplos domínios.

A biblioteca está dividida em cinco grupos de funções: Processamento de imagens; Análise estrutural; Análise de movimento e rastreamento de objetos; Reconhecimento de padrões e Calibração de câmera e reconstrução 3D (Marengoni & Stringhini, 2009).

Segundo (Ribeiro, et al., 2024), as principais aplicações do OpenCv são:

Deteção e reconhecimento de rosto: o OpenCV oferece ferramentas para detetar e reconhecer rostos em imagens e vídeos, o que é útil em sistemas de segurança, autenticação biométrica e análise de emoções, entre outros.

Identificação de objetos: com algoritmos de deteção de objetos, o OpenCV pode ser usado para identificar objetos específicos em imagens ou vídeos, sendo aplicável em sistemas de vigilância, classificação de produtos e reconhecimento de padrões;

Rastreamento de objetos: a biblioteca permite o rastreamento de objeto em movimento em sequências de vídeo, útil em aplicações com monitoramento de tráfego, análise de comportamento de consumidores e navegação autónoma de veículos;

Registro e costura de imagens: o OpenCV oferece recursos para registar e unir imagens, possibilitando a criação de panoramas e mosaicos a partir de várias imagens sobrepostas;

Realidade aumentada: com o OpenCV, é possível integrar elementos virtuais em tempo real em imagens ou vídeos do mundo real, criando experiências interativas em jogos, publicidade e aplicativos de entretenimento.

2.7.4. Pré-Processamento de imagens

Para (Marengoni & Stringhini, 2009), na visão computacional, o pré-processamento de imagens é frequentemente essencial. Isso envolve ajustar o formato e o tamanho das imagens, além de filtrar ruídos que podem surgir durante a captura. Esses ruídos, que prejudicam a qualidade da imagem, podem ser causados por diversos fatores, como o tipo de sensor utilizado, a

iluminação do ambiente, as condições climáticas e a posição da câmera em relação ao objeto. É importante notar que o ruído não se limita a interferências na captura, mas também inclui qualquer elemento que dificulte a interpretação ou o reconhecimento de objetos na imagem.

A Figura a seguir mostra imagens de árvores em condições diferentes para exemplificar estes tipos de interferência.

Figura 9. Imagens de árvores obtidas em condições diferentes, topo à esquerda uma imagem "normal", topo à direita com interferência de iluminação, baixo à esquerda interferência do período do ano e baixo à direita mudança do tipo de sensor. Fonte: (Marengoni & Stringhini, 2009)

Em uma sala de exames, a iluminação deve ser uniforme e adequada, evitando sombras fortes ou reflexos que possam obscurecer detalhes importantes das imagens, evitando assim o uso de técnicas complexas para o processamento da imagem.

2.7.5. Deteção de Objetos

Objetos e Classes: Um "objeto" refere-se a qualquer entidade visual reconhecível em uma imagem, como carros, pessoas, animais, prédios, etc. Cada tipo de objeto a ser detetado é representado por uma "classe", que é uma categoria específica. A tarefa principal da deteção de objetos é detetar e localizar a presença dessas classes de objetos em uma imagem ou vídeo (Géron, 2017 citado em (Dias, Felipe, & Mafra, 2023)).

Em visão computacional, a deteção de objetos permite localizar objeitos específicos em imagens ou vídeos, utilizando algoritmos de Aprendizagem de

máquina e Aprendizagem profundo. Essa técnica busca automatizar a capacidade humana de reconhecer e localizar objetos instantaneamente, com o objectivo de replicar essa inteligência em sistemas computacionais (MathWorks, n.d.).

Diversas metodologias podem ser empregadas para essa tarefa, com destaque para as abordagens baseadas em Aprendizagem profundo, que utilizam Redes Neurais Convulsionais (CNNs). O modelo YOLO exemplifica essa categoria, demonstrando a capacidade de aprender automaticamente a detetar objetos a partir de dados visuais.

Para a implementação da deteção de objetos utilizando Aprendizagem profundo, duas estratégias principais podem ser utilizadas:

Utilização de Detetores Pré-Treinados: Essa abordagem aproveita modelos previamente treinados em extensos conjuntos de dados, permitindo a deteção de objetos comuns, como pessoas, veículos e texto, sem a necessidade de treinamento adicional. Essa opção oferece agilidade, sendo adequada para aplicações que se beneficiam da deteção de objetos genéricos.

Desenvolvimento e Treinamento de Detetores Personalizados: Para aplicações que demandam a deteção de objetos específicos ou a adaptação a cenários particulares, o treinamento de detetores personalizados é essencial. O Aprendizagem por transferência emerge como uma técnica eficaz nesse contexto, permitindo a construção de modelos a partir de redes pré-treinadas. Essa estratégia possibilita o refinamento dos modelos para atender às necessidades específicas da aplicação, oferecendo resultados mais precisos e adaptados.

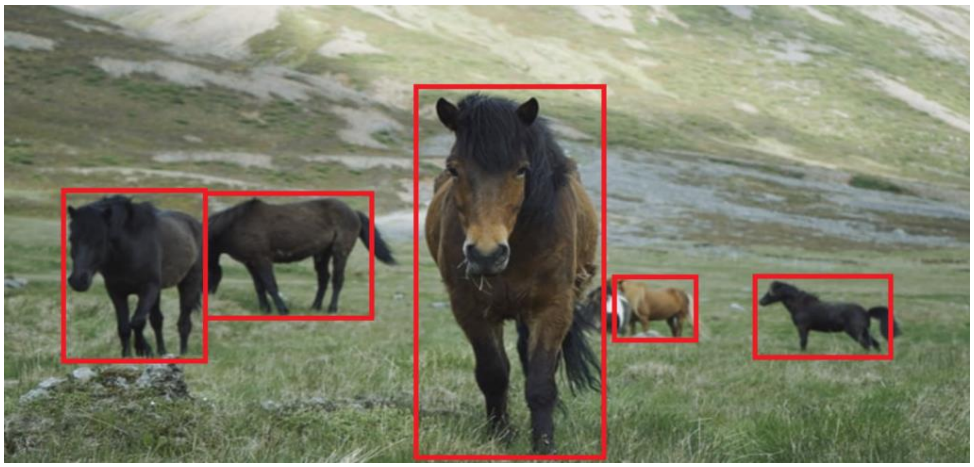


Figura 10. Deteção de cavalos. Fonte: (Tech, 2024)

2.7.6. YOLO

A deteção de objetos em tempo real emergiu como um componente crítico em inúmeras aplicações, abrangendo vários campos, como veículos autónomos, robótica, videovigilância e realidade aumentada. Entre os diferentes algoritmos de deteção de objeto, a arquitetura YOLO (*You Only Look Once*) destacou-se pelo seu notável equilíbrio entre velocidade e precisão, permitindo a identificação rápida e confiável de objeto em imagens. Desde a sua conceção, a família YOLO evoluiu através de múltiplas iterações, cada uma construindo sobre a versão anterior para abordar limitações e aprimorar o desempenho. (Terven, Esparza, & González, 2023)

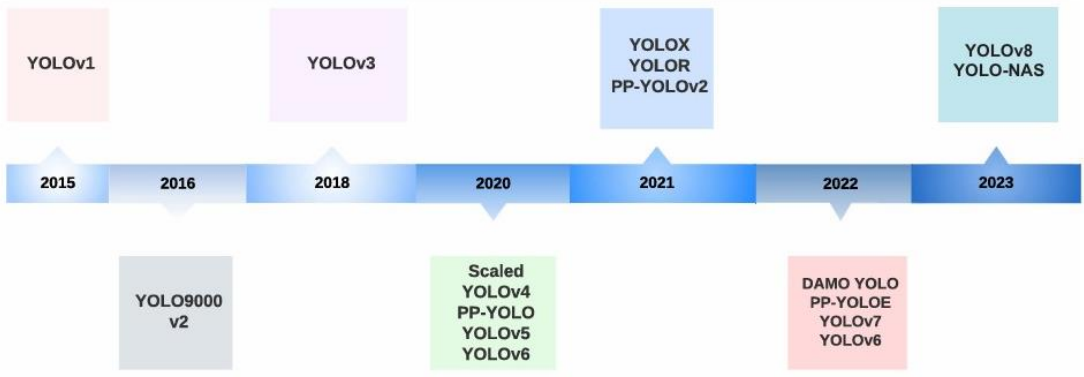


Figura 11. – Evolução do YOLO. Fonte: (Terven, Esparza, & González, 2023)

2.7.6.1. Funcionalidades do YOLO

Segundo (Boesch, 2024) O YOLO na versão v8 está disponível em cinco variantes com base no número de parâmetros: *nano*(n), *small*(s), *medium*(m), *large*(l), e *extra large*(x), podendo realizar as seguintes tarefas:

Classificação de Imagens - a classificação envolve categorizar uma imagem inteira sem localizar o objeto presente nela.

Deteção de Objetos - a deteção de objetos localiza um objeto em uma imagem desenhando caixas delimitadoras.

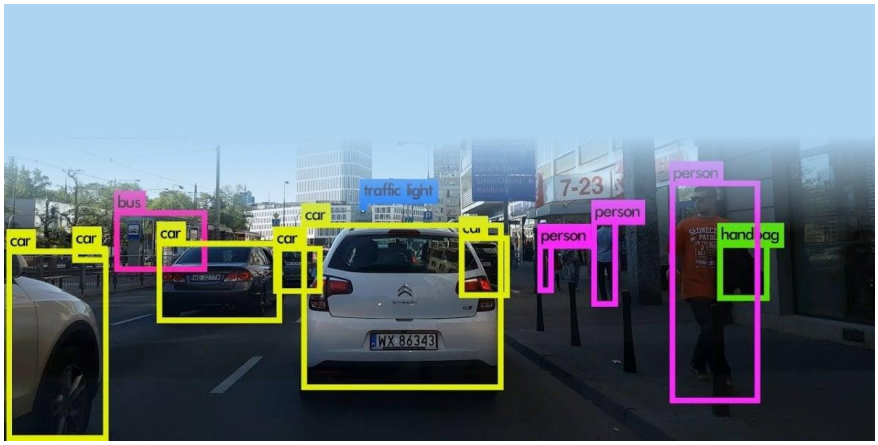


Figura 12. Deteção de objetos com YOLO. Fonte: (OPENCADD, 2019)

Segmentação de Imagens - a segmentação identifica cada pixel pertencente a um objeto. Ao contrário da deteção de objetos, a segmentação é mais precisa na localização de diferentes objetos em uma única imagem.

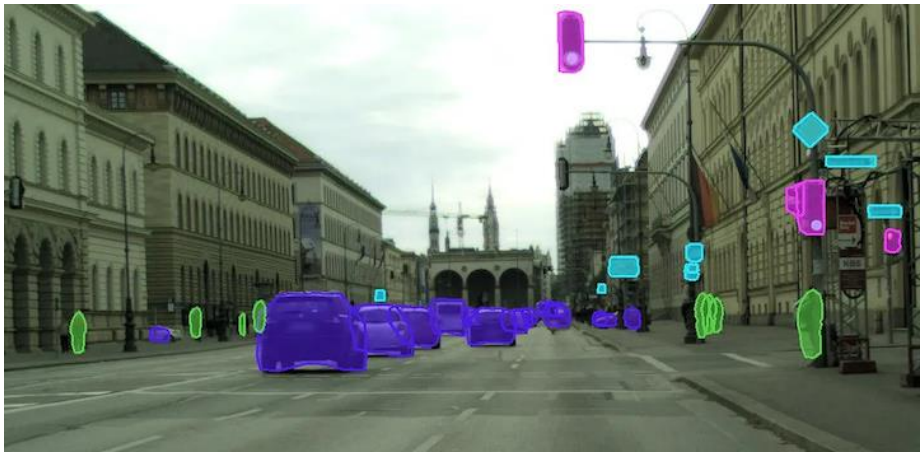


Figura 13. Segmentação de imagens com YOLO. Fonte: (Bhuyan, 2024)

3. Capítulo 3 - Desenvolvimento do Protótipo

Com base nos conhecimentos adquiridos no capítulo anterior, este capítulo é dedicado ao desenvolvimento do protótipo do sistema com vista a simular o funcionamento do sistema num cenário de realização de exames de admissão, de modo a avaliar sua eficácia na identificação de comportamentos suspeitos ou irregulares durante o processo de avaliação. Por se tratar de um sistema baseado em aprendizagem de máquina, a etapa de coleta e preparação de dados é essencial. Para garantir a robustez do modelo, recorreu-se à

plataforma Roboflow, que oferece acesso a grandes volumes de dados rotulados, facilitando o treinamento eficaz na deteção de objetos suspeitos no cenário de realização do exame.

Uma das principais razões para a escolha do YOLOv8 foi a sua capacidade de detetar automaticamente diversos objetos comuns em salas de exame que já estão disponíveis no seu modelo pré-treinado com o *dataset* COCO, como Telemóveis, laptops e pastas de costa. Além disso, o YOLOv8 também permite a análise de poses corporais, recurso importante para identificar posturas e movimentos suspeitos que possam indicar tentativa de fraude.

Contudo, como nem todos os objetos de interesse estão presentes no *dataset* COCO (como folhas de papel), foi necessário treinar um modelo para detetar novas classes específicas. Para isso, foram utilizados o TensorFlow e o Keras, bibliotecas amplamente utilizadas no desenvolvimento de modelos de aprendizagem profunda. O TensorFlow fornece alto desempenho, especialmente quando utilizado com suporte via GPU, enquanto o Keras oferece uma interface intuitiva e de alto nível, permitindo a construção, ajuste e experimentação de modelos personalizados de forma mais ágil.

3.1. Metodologia de desenvolvimento

Para o desenvolvimento do protótipo, usou-se a Metodologia CRISP-DM, que, segundo (IBM), significa Processo Padrão de Vários Segmentos de Mercados para Mineração de Dados, é uma forma comprovada pelo mercado para orientar seus esforços de mineração de dados. Esta abordagem estruturada permitiu organizar o trabalho em seis fases:

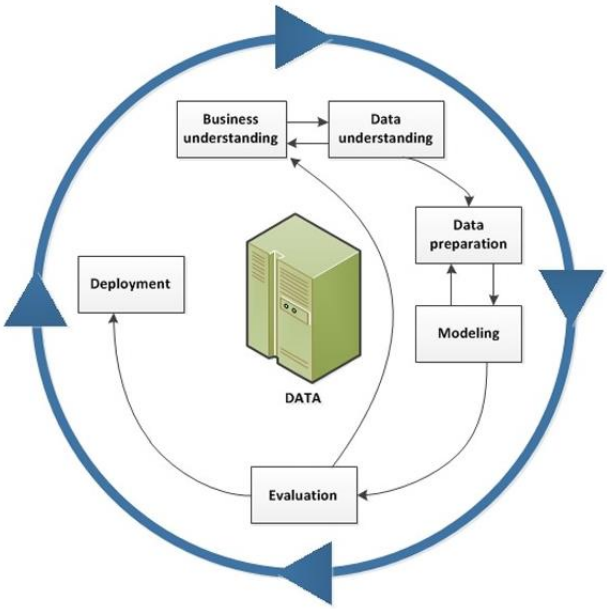


Figura 12. Metodologia CRISP-DM. Fonte: IBM.com

Compreensão do Problema – Identificação dos comportamentos e objetos que caracterizam uma fraude em contexto de exame.

Compreensão dos Dados – Análise de imagens e vídeos de simulações, com o objectivo de encontrar padrões relevantes para o problema.

Preparação dos Dados – Anotação, limpeza e organização dos dados para o treinamento do modelo, com vista a garantir qualidade e consistência.

Modelagem – Utilização do modelo YOLOv8 para deteção de objetos pré-treinados (como Telemóveis e mochilas) e das bibliotecas TensorFlow e Keras para criar um modelo capaz de detetar objetos não pré-treinados no YOLOv8

Avaliação – Testes de desempenho para verificar a eficácia do modelo na deteção de comportamentos e objetos suspeitos durante a realização dos exames.

Implantação – Simulação do sistema em um ambiente semelhante ao real de um exame de admissão para validar sua aplicação na prática.

3.2. Modelagem do sistema

Antes de iniciar o processo de conceção de um *software*, é necessário realizar uma planificação criteriosa, que envolve a compreensão clara dos objectivos do sistema, das necessidades dos usuários e dos problemas que se pretende

resolver. Na modelagem de um sistema, são definidos e detalhados os requisitos funcionais e não funcionais, as regras de negócio, bem como as principais funcionalidades que o sistema deve oferecer.
A modelagem permite prever a estrutura lógica do sistema, seu comportamento esperado e as interações entre os diversos componentes. Utilizando ferramentas e técnicas como diagramas UML (*Unified Modeling Language*), fluxogramas, casos de uso, entre outros.

3.2.1. Requisitos do sistema

Segundo (Nardi & Falbo, 2006), requisitos de *software* são sentenças que expressam as necessidades dos clientes e que condicionam a qualidade do software, ou especificações de serviços que o sistema deve prover, restrições no sistema e conhecimentos necessários para desenvolvê-lo. Eles são classificados em: **funcionais** (representam o que o sistema deve fazer, suas funções, podendo ser subdivididos em essenciais, importantes e desejáveis) e **não funcionais** (representam os atributos do sistema enquanto software constituído, o que inclui manutenção, eficiência etc).

Para a definição da ordem de prioridade dos requisitos neste trabalho, foi projetada uma classificação em três categorias: **essencial**, **importante** e **desejável**.

Essenciais - são os requisitos imprescindíveis para o funcionamento do sistema. Sem a sua implementação, o sistema simplesmente não funciona. Por isso, devem ser obrigatoriamente atendidos antes do início da operação.
Importantes - são os requisitos cuja ausência não impede o funcionamento do sistema, mas compromete sua eficiência, usabilidade ou qualidade. Embora sua implementação seja recomendada, o sistema pode ser implantado e utilizado mesmo que esses requisitos ainda não estejam completamente desenvolvidos.
Desejáveis - são os requisitos que agregam valor ao sistema, mas não enfatizam suas funcionalidades principais. O sistema pode operar satisfatoriamente sem eles.

3.2.1.1. Requisitos funcionais

Referência	Requisito	Prioridade	Descrição
RF. 01	Deteção de presença de dispositivos eletrónicos proibidos.	Essencial	O sistema deve ser capaz de identificar a presença de telefones, Relógios digitais, e outros dispositivos eletrónicos que não são permitidos durante a realização do exame de admissão.
RF. 02	Deteção de comunicação não autorizada entre candidatos.	Essencial	O sistema deve identificar padrões de comportamento que sugiram comunicação entre candidatos, como olhares prolongados e toques em outros candidatos.
RF. 03	Deteção de consulta a materiais de apoio não permitidos.	Essencial	O sistema deve ser capaz de detetar quando um candidato está consultando anotações (cábulas), livros ou outros materiais que não são permitidos durante o exame de admissão.
RF. 04	Deteção de movimentação excessiva ou suspeita.	Importante	O sistema deve identificar movimentos incomuns ou repetitivos que possam indicar tentativa de fraude, como olhar constantemente

			para os lados, mexer excessivamente a cabeça ou tentar esconder algo, gerando um alerta para análise posterior.
RF. 05	Gravação e armazenamento de evidências.	Essencial	O sistema deve gravar automaticamente vídeos ou imagens dos eventos detetados como potenciais fraudes, armazenando-os com informações relevantes como data, hora, posição do candidato na sala.
RF. 06	Geração de alertas em tempo real.	Importante	O sistema deve ser capaz de gerar alertas em tempo real para os fiscais da sala do exame quando um comportamento suspeito é detetado, permitindo uma intervenção imediata.
RF. 07	Geração de relatórios de ocorrências.	Desejável	O sistema deve ser capaz de gerar relatórios sumarizados das ocorrências de potenciais fraudes detetadas durante um exame, incluindo estatísticas e detalhes dos eventos

3.2.1.2. Requisitos não funcionais

Referência	Requisito Não Funcional	Prioridade	Descrição
RNF. 01	Desempenho e Velocidade	Essencial	O sistema deve processar o vídeo em tempo real, para garantir a deteção oportuna de atividades suspeitas. Deve manter a precisão da deteção mesmo sob carga de trabalho elevada (até 50 estudantes por sala).
RNF. 02	Precisão na deteção	Essencial	O sistema deve fornecer alta precisão na deteção de comportamentos fraudulentos (baixo índice de falsos positivos e falsos negativos).
RNF. 03	Usabilidade	Importante	A interface do sistema para os fiscais deve ser intuitiva e fácil de usar, permitindo uma visualização clara das

			câmeras e alertas. O tempo de treinamento para os fiscais deve ser minimizado.
RNF. 04	Escalabilidade	Importante	O sistema deve ser capaz de lidar com um número variável de candidatos e salas de exame, podendo ser facilmente expandido para monitorar mais locais conforme necessário.
RNF. 05	Disponibilidade	Essencial	O sistema deve estar operacional com alta disponibilidade durante os períodos de exame para garantir o monitoramento contínuo.
RNF. 06	Portabilidade	Desejável	O sistema deve ser capaz de rodar em

			diferentes tipos de hardware, oferecendo flexibilidade na escolha da infraestrutura de monitoramento.

3.2.2. Diagrama de casos de uso

Segundo (Barros, 2009), o objectivo dos casos de uso é a identificação das funcionalidades requeridas para o sistema. Assim, os casos de uso incluem-se na fase de análise de requisitos, a fase em que procuramos identificar, da melhor forma possível, o que é que o nosso sistema deve realmente ser capaz de fazer.

(Barros, 2009) aconselha conhecer as seguintes terminologias antes de desenhar o diagrama de uso:

Sistema em discussão (*system under discussion*) - sistema que se pretende entender, modelar ou desenvolver. Pode ser um pequeno programa ou um sistema constituído por que vários programas e várias máquinas e tipos de utilizador.

Ação (*action*) - algo que é executado (feito) por alguém ou por algum sistema informático. Uma unidade de comportamento.

Cenário (*Scenario*) - sequência de ações expressa sem *ifs* ou caminhos alternativos.

Actor (*actor*) - alguém ou algo que exibe um comportamento, ou seja, que executa ações. Corresponde sempre a uma entidade que está fora do sistema em discussão.

Caso de uso (*use case*) - Identificação e especificação de um conjunto de cenários de utilização do sistema em discussão.

Parte interessada (*stakeholder*) - alguém com interesse no sistema em discussão. Por exemplo, as pessoas que o utilizam, o dono do mesmo, pessoas que utilizem os resultados do sistema, outros programas.

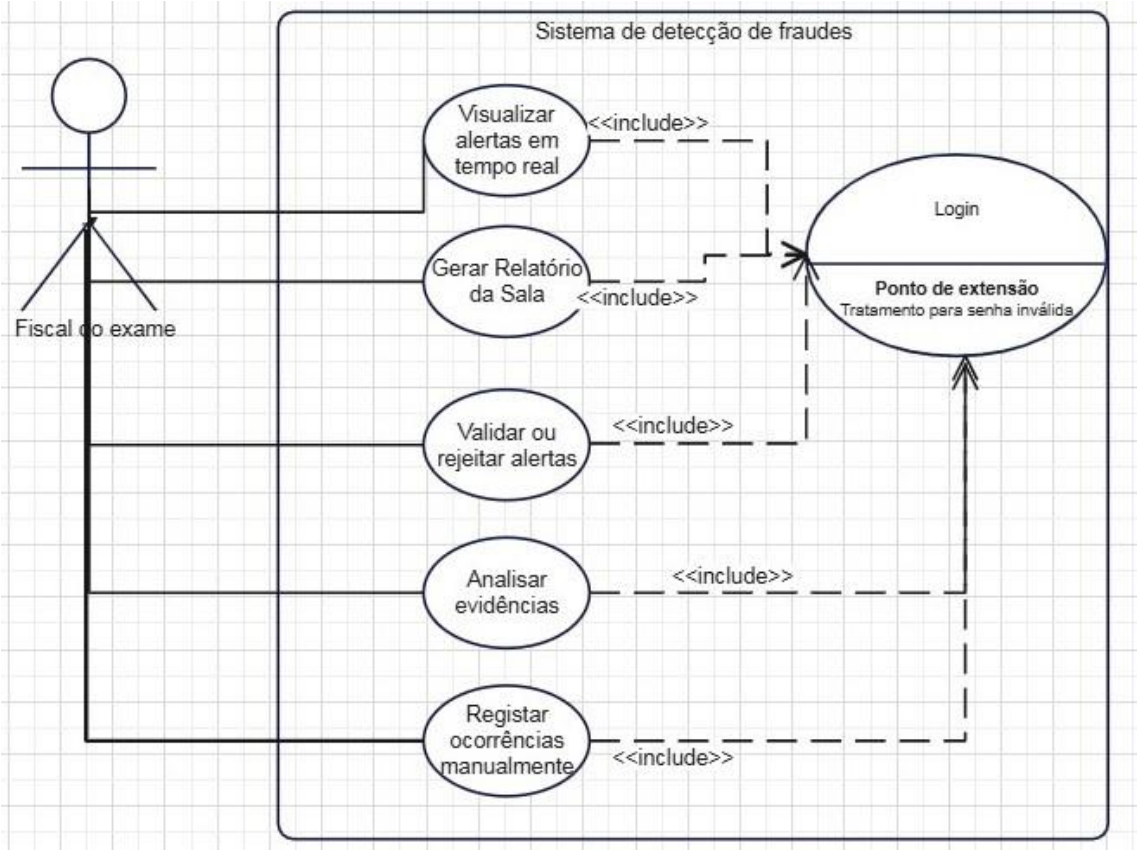


Figura 13. Diagrama de casos de uso. Fonte: Autor

Os Fiscais dos exames desempenham um papel crucial para o sistema, atuando como responsáveis pela supervisão presencial ou remota do ambiente de prova. Eles interagem diretamente com o sistema para acompanhar alertas gerados pelo sistema, validar comportamentos suspeitos detetados, registar ocorrências manualmente quando necessário, e garantir que o exame decorra de forma justa e transparente. Além disso, os fiscais podem gerar relatórios da sala de exame, comunicar falhas técnicas à equipe de suporte, e colaborar com a comissão de admissões em casos que requerem investigação mais

aprofundada. Sua actuação complementa a análise automatizada, fornecendo uma supervisão humana essencial para a eficácia e legitimidade do sistema.

3.3. Implementação do protótipo

1 – Compreensão do problema

Objectivo do sistema

O objectivo do sistema é garantir a integridade, transparência e equidade no processo de exames de admissão, por meio da deteção automática de fraudes. O sistema busca identificar comportamentos suspeitos, como cábulas, trocas de exames, uso de dispositivos eletrónicos ou interações não autorizadas entre candidatos, proporcionando uma vigilância mais eficaz, contínua e imparcial durante a realização dos exames de admissão.

Publico alvo

O público-alvo para presente trabalho é composto, principalmente, pelas instituições de ensino superior, em especial a própria UEM, que buscam garantir a transparência, integridade e equidade nos seus processos seletivos. Além disso, o sistema também se destina às comissões organizadoras de exames, às direções pedagógicas e aos profissionais responsáveis pela segurança e fiscalização durante os exames, oferecendo uma ferramenta tecnológica de apoio que complementa os métodos tradicionais de vigilância e permite uma monitoria mais eficiente e automatizada.

2 – Coleta de dados

A coleta de dados representa uma etapa bastante crucial durante o desenvolvimento de modelos de inteligência artificial pois, a escola de um bom conjunto de dados constitui para o sucesso do modelo. Foram utilizados bancos de dados obtidos da plataforma Roboflow, que forneceram imagens anotadas de elementos específicos como papéis de caderno, os quais são frequentemente associados a tentativas de fraude durante os exames. Para o reconhecimento de outros objetos relevantes, como mochilas, relógios digitais

e telefones, foi utilizado o *dataset* COCO, amplamente adotado em aplicações com o modelo YOLO.

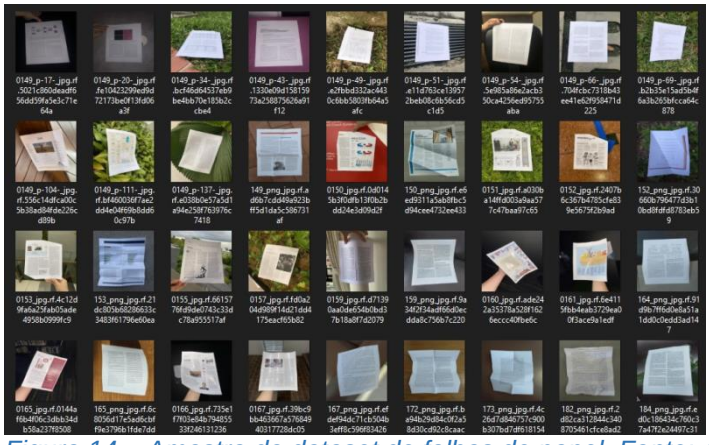


Figura 14 – Amostra do dataset de folhas de papel. Fonte: Autor

Além do uso de bases de dados públicas, também foram gravados vídeos manualmente simulando um ambiente real de exames de admissão, com o objectivo de testar o desempenho do modelo em condições mais próximas da de uma sala exame de admissão. Esses vídeos incluíram diferentes cenários e comportamentos típicos de candidatos durante uma prova, como movimentos naturais, ações suspeitas e a presença de objetos não permitidos. Essa abordagem permitiu avaliar a eficácia do sistema na deteção de fraudes em tempo real e realizar ajustes finos no modelo.

3 – Preparação dos dados

No processo de preparação dos dados para o treinamento do modelo, uma das etapas fundamentais foi o redimensionamento das imagens para o tamanho de 32x32 pixels, utilizando a biblioteca PIL (*Python Imaging Library*) conforme o código abaixo.

```
import os
from PIL import Image

input_folder = r'C:\Users\Edmildo\Desktop\DatasetPronto\Folhas'
output_folder = r'C:\Users\Edmildo\Desktop\Dataset Redimensionado\Folhas R'
size = (32, 32)
os.makedirs(output_folder, exist_ok=True)
for filename in os.listdir(input_folder):
    if filename.lower().endswith(('.png', '.jpg', '.jpeg', '.bmp', '.gif')):
        input_path = os.path.join(input_folder, filename)
        output_path = os.path.join(output_folder, filename)
```

```
    try:
        with Image.open(input_path) as img:
            img_resized = img.resize(size)
            img_resized.save(output_path)
            print(f"Imagem redimensionada: {filename}")
    except Exception as e:
        print(f"Erro ao processar {filename}: {e}")
```

Esse redimensionamento foi essencial para padronizar as dimensões de entrada do modelo, garantindo que todas as imagens tivessem o mesmo formato antes de serem utilizadas no treinamento pois imagens menores, como as de 32x32, reduzem a complexidade computacional, acelerando o tempo de processamento e treinamento.

Em seguida, cada imagem foi convertida para tons de cinza, o que reduz a complexidade dos dados, removendo informações de cor que não são essenciais para a deteção, e permitindo que o modelo foque nos padrões e formas.

```
def grayscale(img):
    return cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
```

Foi aplicada a função *equalize()*, que utiliza equalização de histograma para melhorar o contraste das imagens, destacando elementos importantes mesmo sob condições de iluminação variáveis.

```
def equalize(img):
    return cv2.equalizeHist(img)
```

Para completar a fase de pré-processamento, as imagens foram normalizadas dividindo os valores dos pixels por 255, o que padroniza a escala de intensidade entre 0 e 1, facilitando o Aprendizagem do modelo.

```
def preprocessing(img):
    img = grayscale(img)
    img = equalize(img)
    img = img / 255.0
    return img
```

4 – Modelagem

A *dashboard* do sistema é composta pelas informações importantes para deteção e visualização por parte do fiscal do exame de admissão, dentre elas:

A área de visualização da sala – onde será visualizado o cenário da sala de exame.

A área dos eventos suspeitos – onde serão armazenados vídeos com a duração de 5 segundos a partir de determinada deteção de suspeita de fraude.
Botões iniciar e terminar exame - permite ao fiscal do exame dar início e terminar a deteção de fraudes na sala do exame.

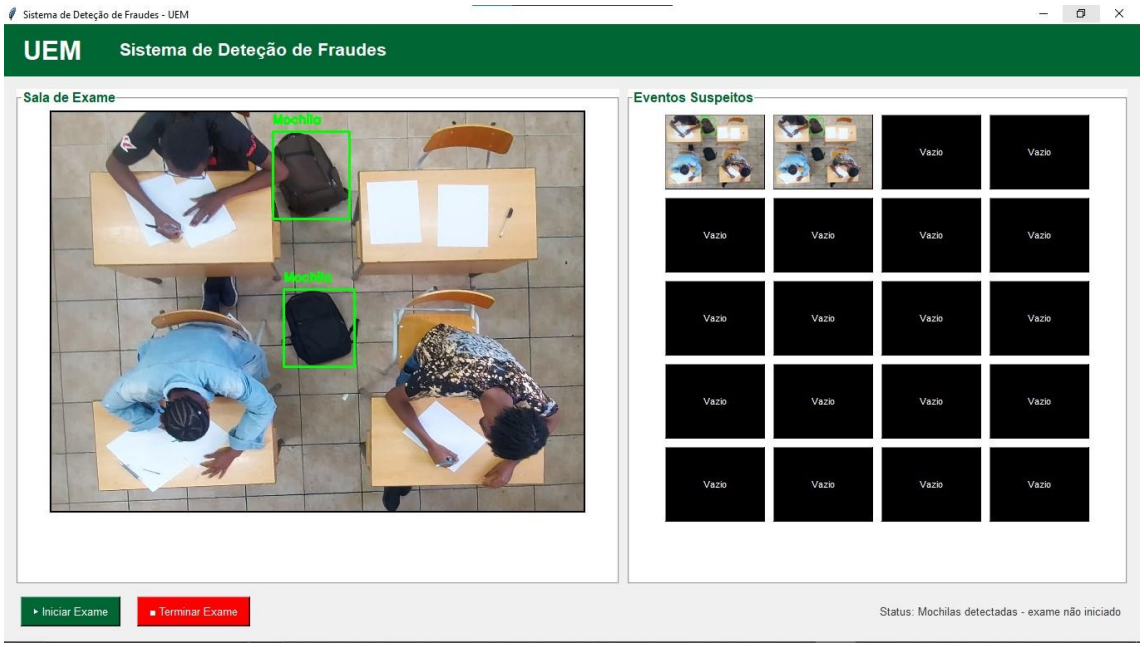


Figura 15. Dashboard do Sistema

5 - Testes

Para testar a eficiência do sistema, foram gravados vídeos simulando um exame de admissão na sala 123 da Faculdade de Engenharia. Esses vídeos, que continham diversas situações de fraude (como uso de dispositivos eletrónicos, consultas a materiais não permitidos e comunicação entre estudantes), foram então inseridos no sistema. O objectivo dessa abordagem era avaliar a capacidade do sistema em identificar e sinalizar automaticamente comportamentos considerados fraudulentos.
As deteções feitas estão ilustradas nas imagens a seguir:

O sistema, ao identificar objetos suspeitos antes do início do exame, impede o início do exame, garantindo que o ambiente esteja livre de possíveis fontes de fraude antes que o exame.

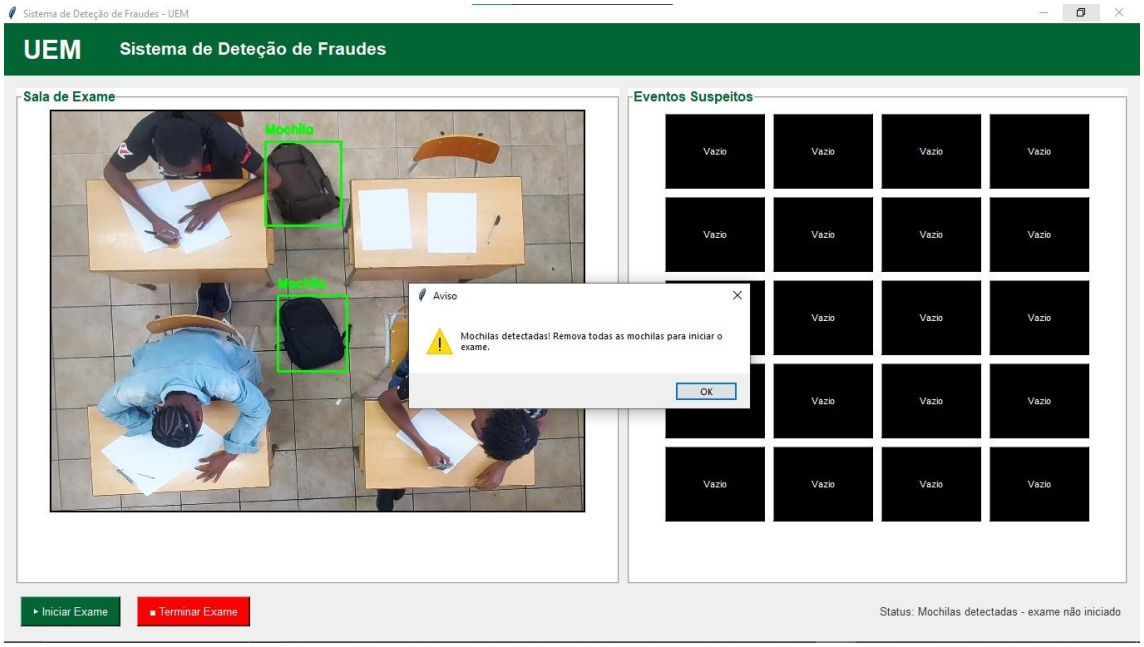


Figura 16. Aviso da impossibilidade de início do exame pois há mochilas presentes na sala do exame

Através da análise visual, o sistema consegue reconhecer padrões de movimento e foco que sugerem a leitura de materiais não autorizados, emitindo um alerta para o fiscal do exame.

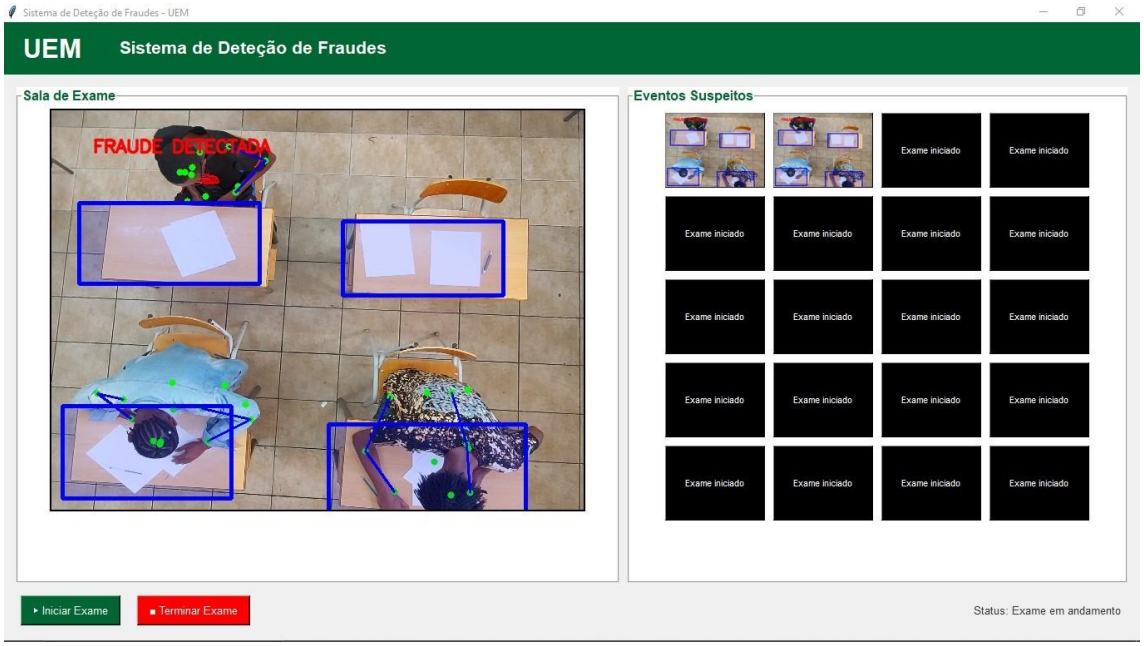


Figura 17. Deteção da consulta de "Papelinhos" durante o exame

O sistema utiliza a analise de postura para detetar interações suspeitas.

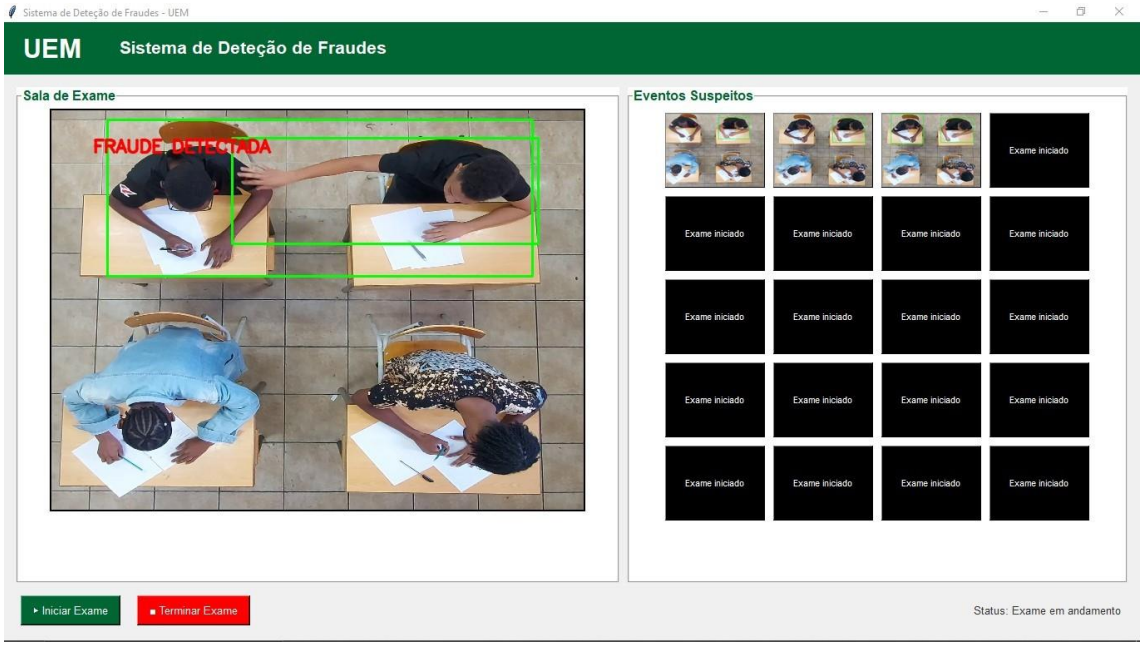


Figura 18. Deteção da comunicação entre os estudantes

O sistema faz também a deteção da troca de material entre os candidatos durante o exame. Esta é uma fraude de alta gravidade, pois pode envolver a troca de Telemóveis, calculadoras ou outros materiais com informações.

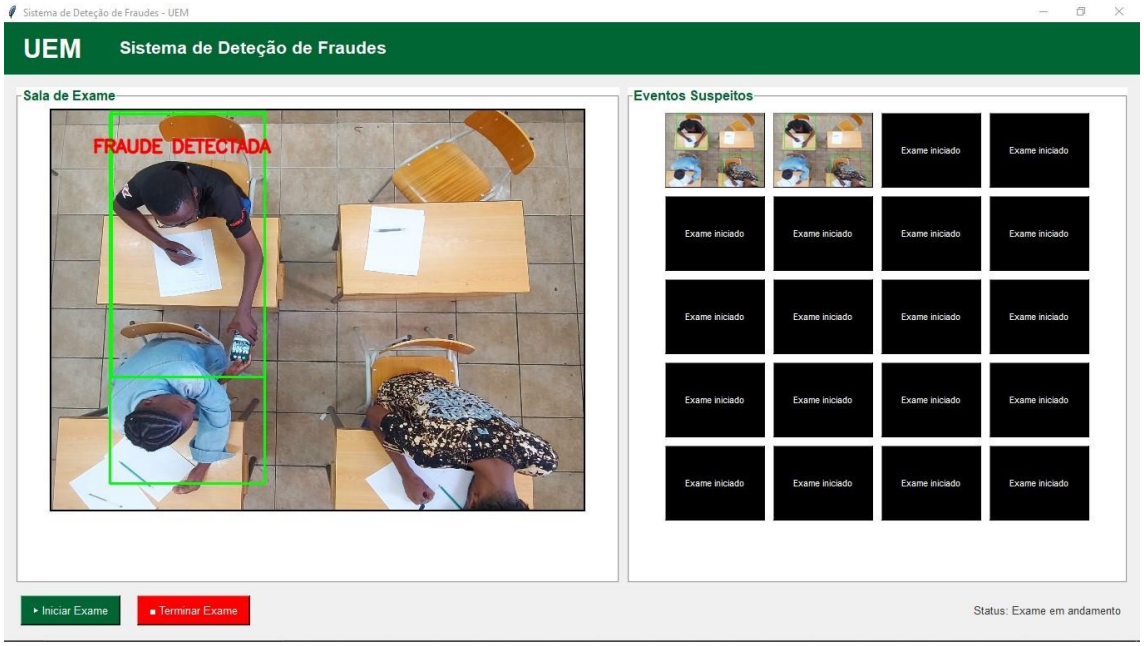


Figura 19. Deteção da troca de dispositivos entre estudantes

3.4. Discussão dos resultados

Para elaborar o trabalho, optou-se por uma metodologia de pesquisa que combinou a revisão bibliográfica e a aplicação de questionários. A pesquisa bibliográfica teve como objectivo principal a coleta de dados e informações relevantes sobre o fenómeno das fraudes académicas, abrangendo suas definições, tipologias e impactos. Complementarmente, foi desenvolvido e aplicado um questionário, visando aprofundar a compreensão sobre o estudo de caso específico, a Universidade Eduardo Mondlane, no que concerne aos motivos que levam os candidatos a cometer fraudes nos exames de admissão, bem como as modalidades de fraude mais recorrentes neste contexto.

3.4.1. Revisão Bibliográfica

A revisão bibliográfica foi essencial para embasar o estudo, trazendo conceitos centrais como fraude académica, visão computacional, análise de dados e Aprendizagem de máquina. Esses temas ajudaram a construir uma base sólida para entender como combater comportamentos fraudulentos em exames. A revisão bibliográfica detalhou o que é fraude académica, incluindo práticas de fraude mais comuns em exames.

A visão computacional, especialmente com o modelo YOLOv8, destacou-se como uma solução promissora. A revisão mostrou que o YOLO consegue detetar objetos em tempo real com alta precisão, usando modelos pré-treinados em *datasets* como o COCO para itens comuns (Telemóveis, mochilas) e permitindo treinamento personalizado para objetos específicos, como cábulas.

3.4.2. Resultados do Protótipo e Testes

O desenvolvimento e os testes do protótipo, trouxeram resultados importantes sobre o uso de visão computacional na deteção de fraudes em exames. O sistema foi projetado para atender requisitos fundamentais, como identificar dispositivos eletrónicos proibidos, comunicação não autorizada e consulta de materiais ilícitos, além de garantir desempenho em tempo real e alta precisão.

Os testes foram feitos com vídeos gravados manualmente, simulando um exame na sala 123 da Faculdade de Engenharia da UEM. O protótipo

identificou com sucesso várias fraudes, como mochilas na sala antes do exame (impedindo seu início), uso de "papelinhos", comunicação entre candidatos e troca de materiais. Esses resultados estão alinhados com o questionário aplicado, que apontou "papelinhos", comunicação entre candidatos e uso de dispositivos eletrónicos como métodos comuns de fraude.

4. Capítulo 4 - Considerações finais

4.1. Conclusão

Depois de uma longa e profunda investigação, que teve como objetivo central utilizar técnicas de análise de dados e visão computacional para desenvolver um sistema de deteção de actividades suspeitas durante exames de admissão, foi possível constatar o papel fundamental da inteligência artificial e do Aprendizagem de máquina no combate a fraudes académicas. A pesquisa demonstrou que a integração de modelos como o YOLOv8, aliada ao uso de TensorFlow e Keras para treinamento personalizado, oferece uma solução eficaz para monitorar comportamentos fraudulentos em tempo real durante a realização dos exames de admissão.

Considerando as questões levantadas na formulação do problema, verificou-se que a visão computacional, combinada com técnicas de análise de dados, é capaz de identificar padrões de fraude com alta precisão, tais como o uso de dispositivos eletrónicos, comunicação não autorizada entre candidatos e consulta a materiais proibidos. O protótipo desenvolvido comprovou sua eficácia em testes simulados, detetando situações de fraude com sucesso e gerando alertas para intervenção imediata.

O objectivo geral foi plenamente atingido, pois o sistema proposto demonstrou capacidade de automatizar a deteção de actividades suspeitas em exames de admissão, utilizando visão computacional e Aprendizagem de máquina.

Os objectivos específicos foram também devidamente alcançados:
Identificação das principais fraudes: O estudo mapeou as práticas mais comuns, como uso de "papelinhos", dispositivos eletrónicos e comunicação entre candidatos, validando-as através de questionários.
Comparação de técnicas de análise de dados: Foram exploradas abordagens como YOLOv8 para deteção de objetos e TensorFlow junto com o Keras para treinamento de modelos personalizados.
Desenvolvimento do sistema protótipo: O dashboard implementado permitiu a visualização imediata de alertas de fraude e armazenamento de evidências.

Além disso, a pesquisa evidenciou que a aplicação de tecnologias de IA na educação superior não só aumenta a transparência nos processos avaliativos, como também reduz a dependência de métodos manuais de fiscalização, que são frequentemente insuficientes diante da criatividade dos infratores. A solução proposta mostrou-se adaptável a diferentes contextos, podendo ser expandida para outras instituições que enfrentam desafios semelhantes.

Por fim, destaca-se que a implementação deste sistema representa um avanço significativo na garantia da integridade académica, alinhando-se às necessidades de instituições como a UEM. Futuros trabalhos podem explorar a integração de técnicas avançadas de análise de postura corporal e processamento de linguagem natural para ampliar ainda mais a capacidade de deteção, consolidando a visão computacional como uma aliada indispensável na promoção de avaliações justas e confiáveis.

4.2. Limitações da pesquisa

Um dos principais desafios enfrentados foi a ausência de uma Unidade de Processamento Gráfico (GPU) dedicada ao processamento dos vídeos coletados. A visão computacional, especialmente em tarefas como deteção de objetos, reconhecimento de padrões e análise de comportamento em tempo real, exige alta capacidade computacional para lidar com grandes volumes de dados de vídeo. A falta de uma GPU resultou em um processamento significativamente mais lento, uma vez que as operações foram realizadas exclusivamente em Unidades de Processamento Central (CPUs). Essa limitação impactou a eficiência do treinamento e a execução dos modelos de Aprendizagem de máquina, prolongando o tempo necessário para processar e analisar os vídeos.

Apesar dessas limitações, estratégias como a otimização de algoritmos e a redução do tamanho das imagens foram empregadas para mitigar os impactos da ausência de uma GPU. No entanto, recomenda-se que, em pesquisas futuras, sejam utilizados recursos computacionais mais robustos, como GPUs de alto desempenho, para melhorar a eficiência do processamento e permitir a

implementação de modelos mais avançados. Essas melhorias seriam cruciais para tornar o sistema mais escalável e aplicável em contextos reais de monitoramento de exames.

5. Bibliografia

5.1. Referências bibliográficas

(s.d.). Obtido em 22 de Agosto de 2024, de Formação de Formadores : https://formacaoformadores-ccp.pt/guia-do-formador/o-formador-e-a-actividade-pedagogica/guia-da-desonestidade-academica/tecnicas-de-como-cabular

(18 de Dezembro de 2023). Obtido em 29 de Agosto de 2024, de Espaço Mente Viva: https://espacomenteviva.com.br/glossario/o-que-e-pensamento-racional/

Academy, D. S. (12 de Março de 2024). *dsacademy*. Obtido em 20 de Abril de 2025, de dsacademy.com.br: https://blog.dsacademy.com.br/segmentacao-de-imagens-medicas-com-deep-learning/

Almeida, F., Seixas, A., Gama, P., & Peixoto, P. (2015). *A Fraude Academica no Ensino Superior em Portugal: Um estudo sobre a ética dos alunos portugueses.* Portugal: Universidade de Coimbra.

Arruda, V. (s.d.). Obtido em 27 de Agosto de 2024, de Vanderlei Arruda: ttps://vanderleiarruda.wordpress.com/2012/04/10/pensando-de-forma-humana-a-modelagem-cognitiva/

Barbosa, E. B. (s.d.). *"COLA" EM SALA DE AULA: A TAXIONOMIA É O ANTÍDOTO.* Universidade Federal do Amazonas (UFAM), Brasil.

Barbosa, F. d. (2020). *Inteligência Artificial no Contexto do Serviço Público.* Brasilia, Brasil: Enap - Escola Nacional de Administração Pública.

Barbosa, J. Á. (2017). *As práticas de "cola" na Universidade e sua relação com os processos de Ensino, Aprendizagem e Avaliação.* Coimbra.

Barros, J. P. (2009). *Casos de Uso e Respectivos Diagramas.* Instituto Politécnico de Beja, Escola Superior de Tecnologia e Gestão.

Bhuyan, Z. (20 de Fevereiro de 2024). *Medium*. Obtido em 6 de Junho de 2025, de Medium: https://zubinbhuyan.medium.com/effortless-coco-annotation-to-yolo-segmentation-14b4c7f893b9

Boesch, G. (18 de Dezembro de 2024). *Viso.ai*. Obtido em 6 de Maio de 2025, de Viso.ai: https://viso.ai/deep-learning/yolov8-guide/

databricks. (2024). *databricks*. Obtido em 5 de Junho de 2025, de databricks.com: https://www.databricks.com/br/glossary/what-is-dataset

Dias, R. L., Felipe, d. A., & Mafra, S. B. (2023). *Comparação de Modelos YOLOv5 e YOLOv8paraDetecção de Objetos em Áreas Rurais Usando Transferência de Aprendizagem.* Instituto Nacional de Telecomunicações- Inatel. Brazil: Inatel.

dooling, D. (s.d.). *Britannica*. Obtido em 26 de Abril de 2025, de britannica: https://www.britannica.com/topic/Mars-Exploration-Rover

Escovedo, T., & koshiyama, A. (s.d.). *Introdução a Data Science: Algoritmos de Machine Learning e metódos de análise.* Casa do Código.

Fleck, L., Tavares, M. H., Eyng, E., Helmann, A., Andrade, C., & de Moares, M. (2016). *Redes Neurais Artificiais: Princíoios Ba'sicos.* Universidade Tecnológica Federal do Paraná . Revista Eletrônica Científica Inovação e Tecnologia.

Gatelli, L. C. (2021). *Sistema de monitoramento, contagem e classificação de fluxo de veículos usando Redes Neurais Convolucionais.* Universidade Federal do Rio Grande do Sul, Engenharia Elétrica, Porto Alegre.

Gatti, B. A. (2003). *O Professor e a aAvaliação em Sala de Aula.* Universidade Católica de São Paulo – PUC-SP, Departamento de Pesquisas Educacionais, São Paulo.

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social* (6 ed.). São Paulo: Atlas.

IBM. (s.d.). *Guia do IBM SPSS Modeler CRISP-DM.*

Marengoni, M., & Stringhini, D. (2009). *Tutorial: Introdução à Visão Computacional usando OpenCV* (Vol. XVI). Universidade Presbiteriana Mackenzie: RITA.

MathWorks. (s.d.). *MathWorks*. Obtido em 13 de Abril de 2025, de Mathworks.com: https://www.mathworks.com/discovery/object-detection.html

Milano, D. d., & Honorato, L. B. (s.d.). *Visão Computacional.* Universidade Estadual de Campinas, São Paulo.

Monard, M. C., & Baranauskas, J. A. (2005). Conceitos sobre Aprendizagem de M´aquina. Em S. O. Rezende, *Sistemas Inteligentes: Fundamentos e Aplicações* (pp. 39-56). Barueri-SP: Manole.

Mussi, R. F., Mussi, L. M., Assunção, E. T., & Nunes, C. P. (8 de Agosto de 2019). Pesquisa Quantitativa e/ou Qualitativa: distanciamentos, aproximações e possibilidades. Rio de Janero.

Nardi, J. C., & Falbo, R. d. (2006). *Uma Ontologia de Requisitos de Software.* Universidade Federal do Espírito Santo, Vitória - ES - Brasil .

Novikobas, A. C., & Malari Maia, L. B. (2020). *Conceito de Inteligência e a Teoria das Inteligências Múltiplas.*

OPENCADD. (4 de Julho de 2019). *OPENCADD*. Obtido em 6 de Junho de 2025, de OPENCADD: https://www.opencadd.com.br/blog/yolo-you-only-look-once-deteccao-de-objetos-em-tempo-real-com-deep-learning

Pereira, S. d. (s.d.). *Introducao a Inteligencia Arti cial.* Universidade de São Paulo.

Ribeiro, H. M., Picanço, A. R., Carr, C. N., Sanos, D. E., Filho, D. R., & de Almeida, T. C. (2024). *Aplicação do OpenCV utilizando técnicas de visão computacional e segmentação de imagens para reconhecimento de colônias bacterianas em análises microbiológicas de qualidade de água.* Universidade do Estado do Pará (UEPA). Brasil: Revista Caderno Pedagógico.

Russell, S., & Norving, P. (2020). *Artificial Intelligence: A Modern Approach* (4 ed.). Pearson.

Significados. (s.d.). Obtido em 26 de Agosto de 2023, de https://www.significados.com.br/inteligencia/

Souza, J. A. (2016). *Prova com Cola: uma conjectura.* Encontro Brasileiro de Pós-Graduação em Educação Matemática, Curítiba.

Standard Encycopedia of Philosophy. (s.d.). Obtido em 28 de Março de 2025, de https://plato.stanford.edu/entries/turing-test/

Tech, D. (2024). *Didática Tech*. Obtido em 13 de Abril de 2025, de didatica.tech: https://didatica.tech/deteccao-de-objetos/

Terven, J., Esparza, D. M., & González, J. A. (2023). *A Comprehensive Review of YOLO Architectures in Computer Vision: from YOLOv1 to YOLOv8 and YOLO-NAS.* MDPI.

uem.co.mz. (s.d.). Obtido em 03 de Setembro de 2024, de uem.co.mz: https://uem.mz/index.php/faculdade-de-engenharia/

Uzinski, J. C., Abreu, C. C., & de Olivera, B. R. (2020). *Aplicações de Inteligência Artificial e Ciênca de Dados.* Brasil: Pantanal Editora.

Vina, A. (27 de Dezembro de 2024). *Ultralytics*. Obtido em 12 de Março de 2025, de Ultralytics.com: https://www.ultralytics.com/pt/blog/using-computer-vision-to-analyse-satellite-imagery

Viva, E. M. (2023). *espacomenteviva*. Obtido em 29 de Agosto de 2024, de espacomenteviva.com.br: https://espacomenteviva.com.br/glossario/o-que-e-pensamento-racional/

Anexos

Anexo 1 – Resultado do questionário

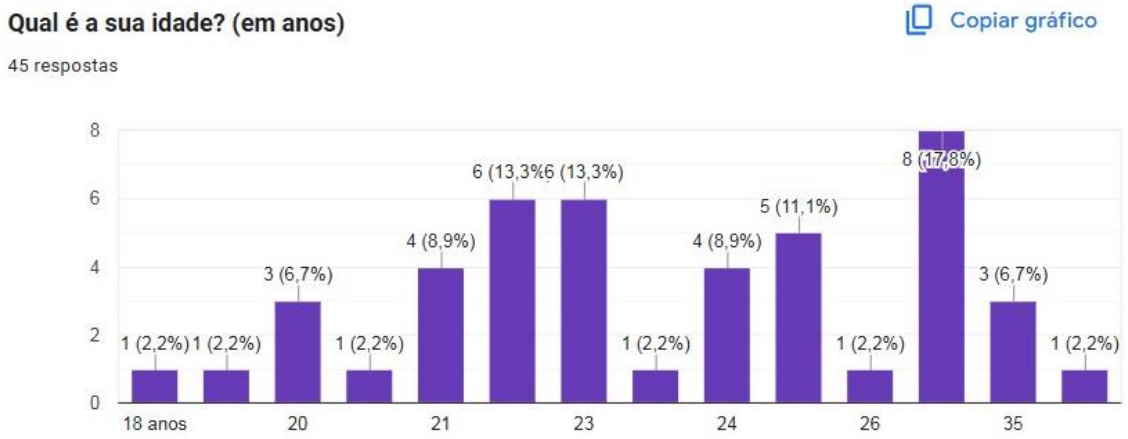


Figura A1 – 1. Faixa etária dos inquiridos

Foram inquiridos 45 participantes, dos quais cerca de 71% pertencem à faixa etária de 18 a 25 anos, 26,7% têm entre 26 e 35 anos, e 2,2% possuem mais de 35 anos.

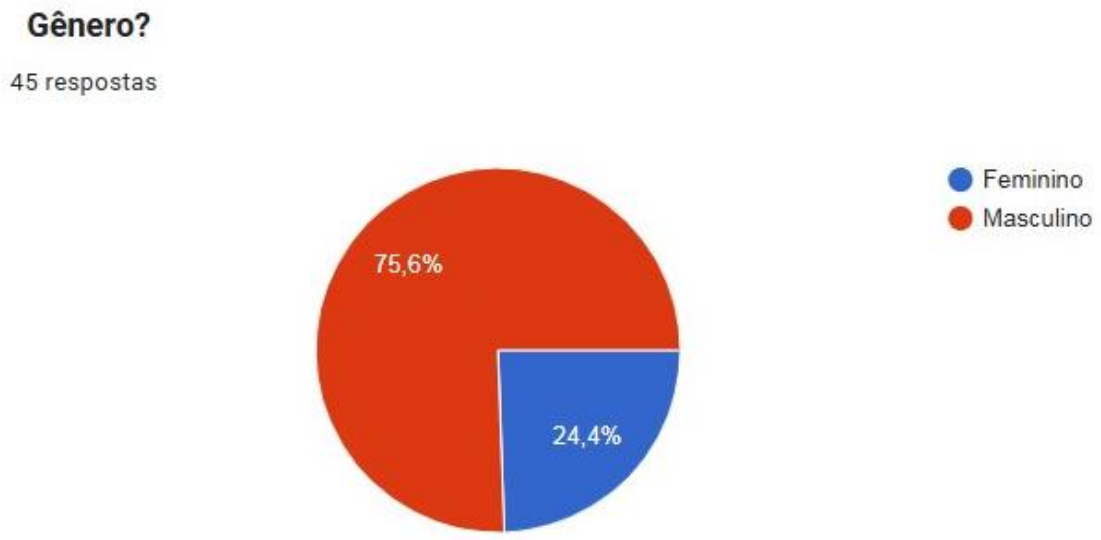


Figura A1 – 2. Género dos inqueridos

Em relação ao género dos participantes, 75,6% são do género masculino, enquanto 24,4% são do género feminino.

Figura A1 – 3. Nível universitário dos inqueridos

Quanto ao ano de frequência universitária, a maioria, 37,8%, encontra-se no 5º ano, seguido por 20% no 4º ano, 13,3% no 3º ano, 11,1% no 1º ano, e 8,9% tanto no 2º quanto no 6º ano. Isso indica que a maior parte dos participantes está em fases avançadas da graduação, o que pode refletir uma maior experiência e consciência sobre os processos de admissão e as práticas de fraude.

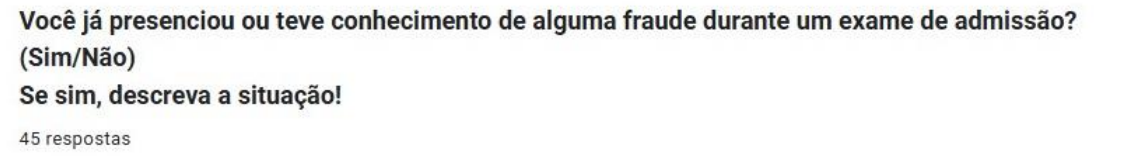


Figura A1 – 4. Conhecimento dos inquiridos sobre alguma ocorrência de fraude em sala de exame

Uma parte significativa relatou situações suspeitas ou confirmadas de irregularidades. Aproximadamente metade respondeu "Sim", descrevendo práticas como o uso de aparelhos eletrónicos (Telemóveis, "bombinhas"), cábula escrita em papel, comunicação entre candidatos, troca de identidade (uma irmã fazendo prova pela outra), recebimento prévio ou durante o exame das respostas e até rumores não confirmados. A outra metade declarou não ter presenciado ou tido conhecimento de fraudes.

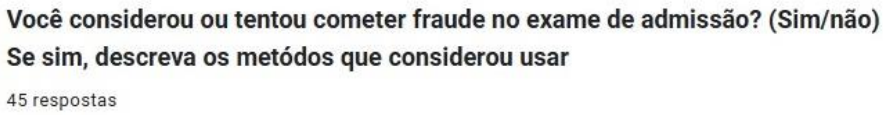


Figura A1 – 5. Informação sobre a prática de fraude por parte dos inqueridos

A grande maioria afirmou que não cometeu nem considerou cometer fraude, expressando posicionamentos firmes contra essa prática, inclusive com frases como "nunca faria algo igual". No entanto, houve ao menos dois relatos que admitem práticas fraudulentas em outras formas de avaliação, como levar folhas com exercícios resolvidos ou trocar informações com colegas.

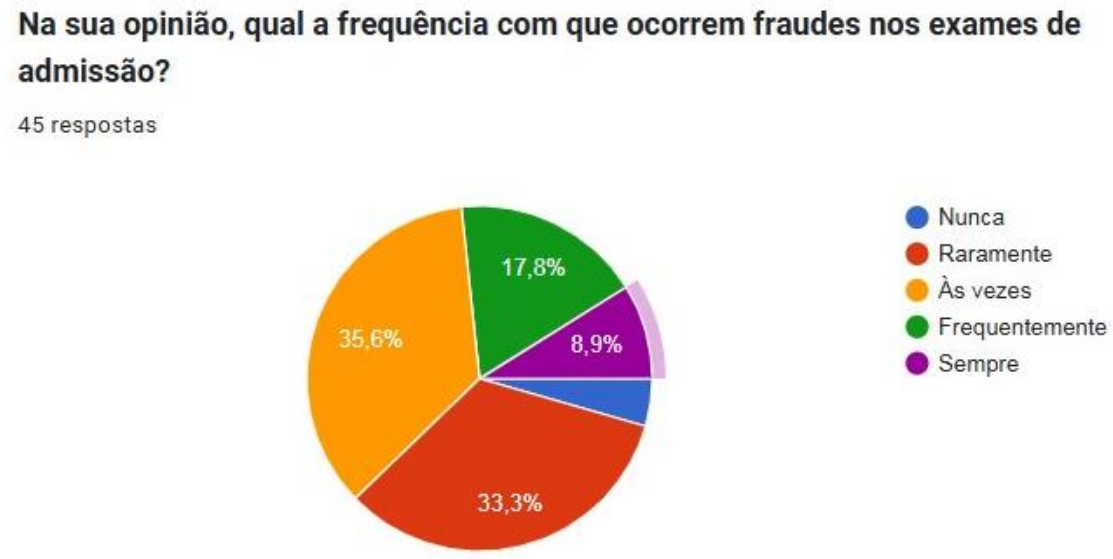


Figura A1 – 6. Frequência de ocorrência das fraudes académicas

A perceção dos participantes sobre a frequência de fraudes em exames de admissão mostra que a maioria acredita que essas práticas ocorrem com alguma regularidade: 35,6% disseram “Às vezes” e 33,3% “Raramente”, o que somado representa quase 70% dos respondentes. 17,8% afirmaram que fraudes ocorrem “Frequentemente”, enquanto 8,9% acreditam que “Sempre” ocorrem e uma pequena de 4,4% parcela considera que “Nunca” ocorrem.

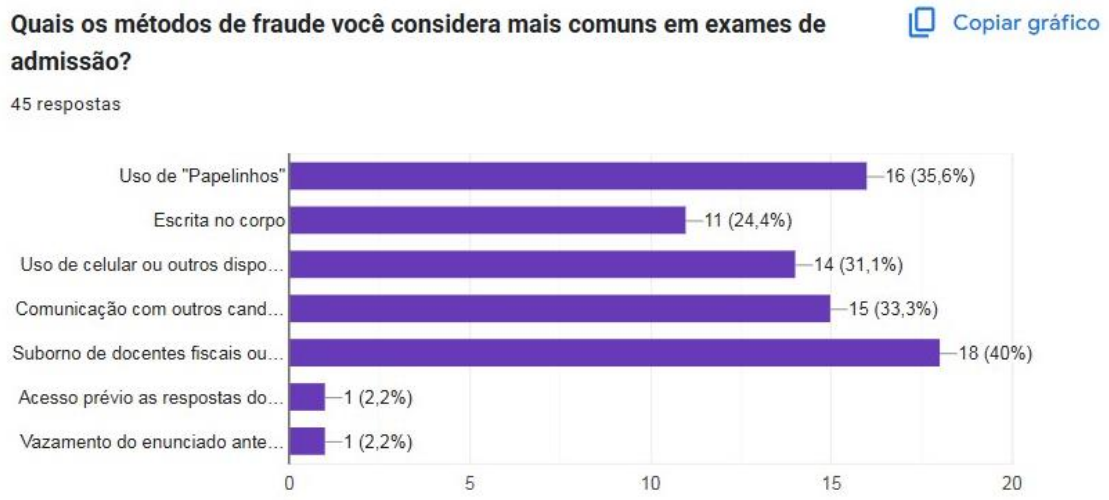


Figura A1 – 7. Métodos de fraudes mais comuns em salas de exame

Os métodos de fraude considerados mais comuns em exames de admissão foram principalmente o suborno de docentes, fiscais ou outros envolvidos (40%) e o uso de "papelinhos" (35,6%). Também se destacam a comunicação com outros candidatos (33,3%) e o uso de celular ou dispositivos eletrónicos (31,1%), seguidos pela escrita no corpo (24,4%). Métodos menos citados foram acesso prévio às respostas ou questões e vazamento do enunciado antes da prova, ambos com apenas 2,2% das respostas.

Figura A1 – 8. Método de fraude mais difícil de ser detetado

Sobre o método de fraude mais difícil de ser detetado, predomina o suborno de docentes, fiscais ou outros envolvidos como o mais discreto e complexo de identificar, sendo citado de forma recorrente. Em seguida, destacam-se métodos como a escrita no corpo, o uso de “papelinhos”, aparelhos eletrónicos (como telefones) e a comunicação entre candidatos. Houve também menções ao acesso prévio às respostas ou exames, além de algumas pessoas que disseram não saber ou não ter opinião formada.

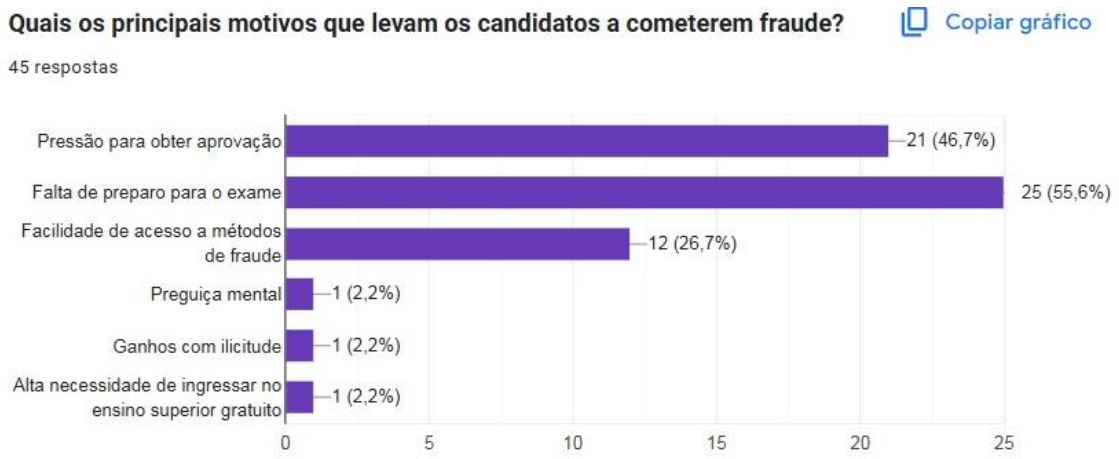


Figura A1 – 9. Motivos que levam os candidatos a cometerem fraude

Os principais motivos apontados para que candidatos cometam fraudes em exames de admissão são, em primeiro lugar, a falta de preparo para o exame (55,6%) e, em seguida, a pressão para obter aprovação (46,7%). A facilidade de acesso a métodos de fraude também foi citada por 26,7% dos respondentes. Outras razões foram mencionadas de forma isolada, como preguiça mental, ganhos com ilicitude e a alta necessidade de ingressar no ensino superior gratuito, cada uma com 2,2%.

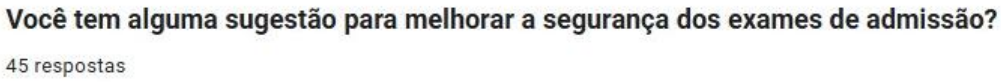
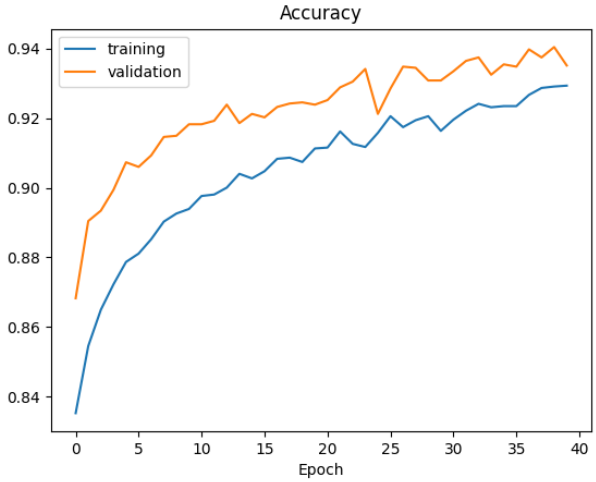


Figura A1 – 10. Sugestões para melhoria da segurança dos exames de admissão

Muitos participantes destacaram o uso de tecnologias, como câmeras de vigilância, sistemas de visão computacional, autenticação biométrica e exames eletrónicos ou multimídia. Houve também recomendações para maior rigor na fiscalização, como revistas físicas nos candidatos, controle mais severo por parte dos fiscais e supervisores, além de presença de pessoal da gestão superior das instituições. Outros sugeriram melhorias estruturais, como a redução do número de candidatos por sala e a elaboração tardia dos exames para evitar vazamentos. Também foram mencionadas abordagens educativas, como conscientização sobre as consequências da fraude e melhoria na qualidade do ensino básico e secundário, a fim de reduzir a necessidade de recorrer a métodos fraudulentos.

Anexo 2 – Acurácia e Perda após o treinamento do modelo



Figuras A2 – 1. Acurácia após o treinamento do modelo

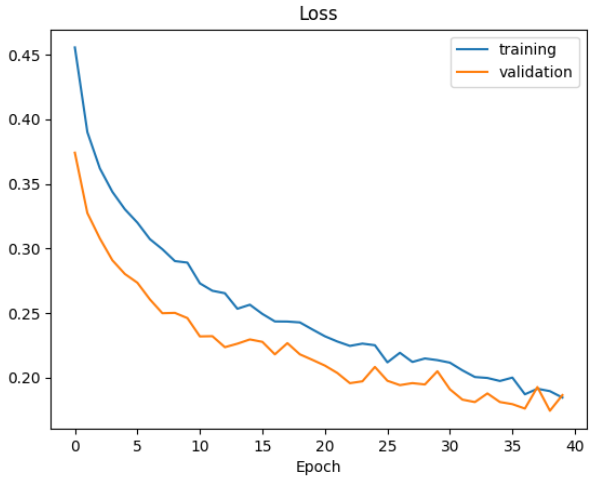


Figura A2 – 2. Perda após o treinamento do modelo

Anexo 3 – Elementos pertencentes ao *dataset* COCO

person	fire hydrant	elephant	skis	wine glass	broccoli	dining table	toaster
bicycle	stop sign	bear	snowboard	cup	carrot	toilet	sink
car	parking meter	zebra	sports ball	fork	hot dog	tv	refrigerator
motorcycle	bench	giraffe	kite	knife	pizza	laptop	book
airplane	bird	backpack	baseball bat	spoon	donut	mouse	clock
bus	cat	umbrella	baseball glove	bowl	cake	remote	vase
train	dog	handbag	skateboard	banana	chair	keyboard	scissors
truck	horse	tie	surfboard	apple	couch	cell phone	teddy bear
boat	sheep	suitcase	tennis racket	sandwich	potted plant	microwave	hair drier
traffic light	cow	frisbee	bottle	orange	bed	oven	toothbrush

Figura A3 – 1. Elementos pertencentes ao dataset COCO